ШУМЕНСКИ УНИВЕРСИТЕТ
"ЕПИСКОП К. ПРЕСЛАВСКИ"
ФАКУЛТЕТ ПО МАТЕМАТИКА
И ИНФОРМАТИКА
ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

KONSTANTIN PRESLAVSKY
UNIVERSITY OF SHUMEN - BULGARIA
FACULTY OF MATHEMATICS
AND COMPUTER SCIENCE
FACULTY OF TECHNICAL SCIENCE

МАТТЕХ 2018

СБОРНИК НАУЧНИ ТРУДОВЕ

Том 2, част 1

Информационни, технически и икономически проблеми на системите за сигурност

Студентска секция

MATTEX 2018

CONFERENCE PROCEEDINGS

Volume 2, part 1

Information, Technical and Economical Problems of Security Systems

Student's Section

УНИВЕРСИТЕТСКО ИЗДАТЕЛСТВО
"ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ"

ШУМЕНСКИ УНИВЕРСИТЕТ „ЕПИСКОП К. ПРЕСЛАВСКИ“
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
FACULTY OF TECHNICAL SCIENCE

МАТТЕХ 2018

СБОРНИК НАУЧНИ ТРУДОВЕ

MATTEX 2018

CONFERENCE PROCEEDINGS

Том 2, част 1

Информационни, технически и икономически проблеми на системите за сигурност

Студентска секция

Volume 2, part 1

Information, Technical and Economical Problems of Security Systems

Student’s Section

Том 2, част 2

Комуникационна и компютърна техника и технологии

Геодезия, фотограметрия и картография

Общо инженерство, технически системи и логистика

Volume 2, part 2

Communication and Computer Technologies

Geodesy, Cartography and Cadastre

General Engineering, Technical Systems and Logistics

Ш У М Е Н
2018

Настоящият сборник съдържа научни доклади, изнесени на проведената през октомври 2018 година в Шуменския университет научна конференция с международно участие MATTEX 2018 с резултатите от научните изследвания на преподаватели, докторанти, специалисти и студенти от Шуменския университет, други учебни заведения, фирми и организации. Конференцията беше частично финансирана от Фонд Научни Изследвания с договор ДПМНФ01/23-31.08.2018г., от проект РД-08-146/08.02.2018 на Шуменски университет и от дарение на Пашабахче България ЕАД, гр. Търговище.

Всички доклади, публикувани в сборника, са рецензирани.

This volume contains the reports presented on the Scientific Conference with international participation MATTEX 2018 held at Konstantin Preslavsky University of Shumen in October 2018. The reports contain the results of the research of lecturers, PhD students, specialists and undergraduate students at Konstantin Preslavsky University of Shumen, other Higher Education Institutions, companies and research organizations. The conference was partially supported by the Scientific Research Fund under contract DPMNF01/23-31.08.2018г., project RD-08-146/08.02.2018 of Shumen University and Paşabahçe Bulgaria, Targovishte.

All papers published in this volume have been reviewed.

EDITORIAL BOARD:

Corr. Mem. Prof. DSc Petar Getsov – Bulgaria
Prof. DSc Andrey Ivanov Andreev - Bulgaria
Prof. DSc Borislav Yordanov Bedzhev - Bulgaria
Prof. DSc Garo Mardirosian - Bulgaria
Prof. DSc Krzysztof Szczypiorski - Poland
Prof. DSc Mihail Petkov Iliev - Bulgaria
Prof. Dr. Alen Sarkisyan - France
Prof. Dr. Evgeni Petrov Manev - Bulgaria
Prof. Dr. Yuriy Ivanov Dachev - Bulgaria
Assoc. Prof. Dr. Andrey Iliev Bogdanov - Bulgaria
Assoc. Prof. Dr. Chavdar Nikolaev Minchev - Bulgaria
Assoc. Prof. Dr. Hristo Atanasov Hristov - Bulgaria
Assoc. Prof. Dr. Janis Kaminskis - Latvia
Assoc. Prof. Dr. Tihomir Spirdonov Trifonov – Bulgaria
Assoc. Prof. Dr. Voldemars Karklins - Latvia
Assoc. Prof. Dr. Petar Krasenov Boyanov - Bulgaria

© Университетско издателство "Епископ Константин Преславски"
Konstantin Preslavsky University Press

ISSN: 1314-3921

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 3 - 10 Problems of Security Systems

HUMANITARIAN ASPECTS OF PROTECTION OF INFORMATION

IVO V. VELIKOV

ABSTRACT: *With the increase in the scope and the increasingly dynamic development of information systems, in practice in all spheres of social activities, with the penetration or at least approaching the information society, information becomes a basic commodity and value of this society.*

KEYWORDS: *Information, Security.*

ХУМАНИТАРНИ АСПЕКТИ НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА

ИВО В. ВЕЛИКОВ

АБСТРАКТ: *С нарастването на обхвата и все по-динамичното развитие на информационните системи, на практика във всички сфери на обществени дейности, с навлизането или поне приближаването към информационно общество, информацията се превръща в основна стока и ценност на това общество.*

1. Въведение

С нарастването на обхвата и все по-динамичното развитие на информационните системи, на практика във всички сфери на обществени дейности, с навлизането или поне приближаването към информационно общество, информацията се превръща в основна стока и ценност на това общество.

Темата за нормативната основа и човешките ресурси при защитата на информацията придобива все повече значение, защото от една страна хората използват технологиите по различни начини, от друга – динамичното развитие на технологиите неминуемо налага нови образци организационно поведение и променя качествено административните процедури и механизми.

Имаме удоволствието в горния смисъл да коментираме един изключително актуален проблем.

Доколкото в правния мир не изпреварваме, но и не изоставаме от европейските и световни тенденции – имаме си ЗЗКИ и ДКСИ, ЗЗЛД и КЗЛД, ЗДОИ и платформа за ДОИ към администрацията на МС (чл.15), т.е. имаме навсякъде закон плюс една структура с централни правомощия, която от една страна да осигурява изпълнението на законите като контролен орган, от друга да спомага за реализирането на правата на гражданите.

Доколкото по горната тема сме писали и преподавали достатъчно години, втората страна на хуманитарните аспекти на защитата на информацията смятаме за по-интересна, по-бурно развиваща се и за съжаление – и с някои негативни тенденции у нас.

2. Изложение

Връзката на човешкия фактор с информационната сигурност е проблем, стар колкото и света, но днес той е особено злободневен. Ако се вгледаме в технологиите за защита на информацията, веднага ще забележим, че на пазара се предлагат достатъчно чисто

технологични – софтуерни, хардуерни и организационни решения. Някои от тях наистина са много прецизни, разбира се – и скъпи. Но дори и да имаме най-скъпите технологии, най-прецизните и сложни системи, с базите данни работят хора, които могат да бъдат използвани от конкуренцията и противника много по-вероятно и често, отколкото да се преодоляват многобройните защити. И без да изпадаме в някаква технологична абсолютизация, технологиите днес се развиват толкова бързо, че след шест месеца или една година нашата ултрамодерна и скъпа технологична защита вече ще е достатъчно позната или достатъчно пъти компрометирана. Освен това, парадоксално, но факт – технологиите за декодиране се развиват по-бързо от технологиите за кодиране на информацията. Така един опитен нарушител, и при най-скъпи технологии за защита ще има нужда от няколко минути или десетки минути, за да преодолее защитата, организирана само на базата на технологията.

Така човешките ресурси, които на пазара на труда са достатъчно оскъдни като качество, особено в областта на информационните технологии, и които само с добросъвестното си и ангажирано поведение на работното място биха допринесли неимоверно за качеството на информационната сигурност, са вероятно най-важният елемент на тази динамична система – защитата на информацията.

Очевидно е, че и колегите преди мен и след мен, участници в тази научна конференция са се насочили абсолютно резонно в такава насока на разсъждение.

Реално е да се мисли, че защитата на информацията има няколко напълно самостоятелни аспекта, които бихме характеризирали по следния начин:

- Технологичен аспект. Мястото и ролята на информационните технологии, но не само – и на организацията по тяхното прилагане и използване. Тази високо специализирана дейност обаче се предлага от много специалисти и информационни структури;

- Нормативен аспект – ЗЗКИ, ЗЗЛД, ЗДОИ. Както у нас, така и в международен план, към настоящия момент имаме тези три закона, приети България в началото на хилядолетието – в периода 2000-2002 г.. В тях сравнително успешно е реципиран чужд опит – ЕС, НАТО и на някои конкретни страни-членки на тези организации. При ЗКИ и ЗЛД имаме и съответните държавни структури, отговорни за цялостната политика по защита на конкретните видове информация – Държавната комисия по сигурността на информацията и Комисията по защита на лични данни. Нещо повече – чрез двата закона се въвеждат специални лица, отговорни повече или по-малко за защитата на данните – Служител по сигурността на информацията при ЗЗКИ и длъжностно Лице по защита на личните данни по ЗЗЛД. При ЗДОИ няма такъв орган (ако изключим т.нар. „платформа“ в МС), но информацията, която се регламентира чрез този нормативен акт е жизнено важна за социума, така че имаме множество НПО, които се интересуват от спазването на нормите на закона. Така се изгражда актуалната система за защита на видовете данни – във всяка една от областите имаме достатъчно пространни и подробни норми, една сложна и динамична система, която се превръща в ангажимент на държавата, местната власт, частните структури, чуждестранните субекти в нашата страна, НПО и др.

- Човешки (хуманитарен) аспект – тема на дискусията.

Ненапразно оставихме накрая хуманитарният аспект на проблема по защитата на информацията. Той ще бъде основната тема на последващото изложение. Той е тема и на една нова презентация в обучението на ССИ от ДКСИ, с която обръщаме внимание на заплахата от разузнавателно проникване в системата за защита на информацията и противодействието на т.нар. „инсайдър“ – вътрешен човек на атакуваната система.

Какви могат да бъдат загубите от подобно проникване или преодоляване на защитата на информацията:

- Пари;
- Имущество;
- Пропуснати ползи;
- Разходи за защита и издирване;
- Разходи за дела;
- Губи се репутация и клиенти;
- Нелоялна конкуренция;
- Загуба от неплатени данъци.

С горното изброяване просто се опитваме не да обхванем всички видове загуби, а просто да подскажем, че те могат да бъдат безкрайно различни и ние дори често пъти нямаме представа какво може да понесе нашата организация като загуба.

И въпреки, че съзнаваме важността на проблема за опазване на информацията, организациите не съумяват да противодействат достатъчно ефективно. Дори имаме примери на атаки срещу цели държави, като например Естония и Италия в средата на първото десетилетие на този век. Трябва ни доста развинтено въображение какво би се получило, ако успее кибератака срещу ЕСГРАОН, НАП, митници и няколко министерства или съдебната власт. Причините за сравнително закъснелите реакции и сравнителната безпомощност срещу такива атаки дори на мощни организации и държави са следните (отново без претенции за пълна изчерпателност):

- Различна подготовка на човешкия фактор, осигуряващ информационната сигурност (това е активна и съзнателна дейност, искаме целия потенциал на човешкия ресурс, но понякога той толкова просто си не може да се справи);
- Различия в теорията и законодателствата на страните;
- В над 80% от случаите имаме „вътрешен човек“ (инсайдър) според службите за сигурност;
- Не навсякъде информационната сигурност е с висок приоритет;
- Нарушенията са също различни – неправомерен достъп, случайни или нарочни изменения, унищожавания, разкривания на съдържание, излъчвания, бедствия и аварии също могат да са заплаха и др.
- Динамиката в развитието на технологиите (декодирането се развива по-бързо, както споменахме по-горе).

В допълнение към казаното до момента – имаме още доста причини, които да са важни за изграждането на една комплексна политика за информационна сигурност (хора, средства, техника и т.н.), дори и да имаме желанието за такова усилие:

- Самата дейност е сложна дейност – нуждаем се от експерти, те да бъдат обединени в успешни екипи, техника, организация на работа;
- Индивидуална и колективна отговорност на човешкия фактор;
- Анализи на риска и заплахите;
- Сигурност на персонала;
- Сигурност на физическите обекти;
- Безопасност на мрежите;
- Компютърна сигурност.

Цялата многопосочност на усилията пречи на съсредоточаването в определена насока и организациите често изпускат някакви елементи в системата си за информационна сигурност. Тук веднага бихме привели пример с една високо технологична компания като „Хюлет Пакард“. Неотдавна в среща със специалист по

корпоративна сигурност на компанията се оказа, че процедурите им са толкова добре разписани, че самият той отговаря за около 15 държави в Централна и Източна Европа и когато има пробив или компрометиране на системата за информационна сигурност, обикновено са му достатъчни 2-3 дни, преглед на определени процедури и действия, след което неминуемо ще бъде открита причината за проблема (т.е. процедурата или протокола, който е нарушен). Така става очевидно, че проблемът е в човека като индивидуален елемент, не толкова в технологията, процедурата, проверката или обучението на персонала.

Споменахме системата за информационна сигурност вече няколко пъти. С това понятие просто искаме да подчертаем, че се изискват наистина многопосочни усилия от всички служители на организациите, за да имаме изпълнение на изискванията за надеждност, гъвкавост и оперативност на системата. Сред изискванията към системата даваме приоритет на такива отношения на работните места и в самото ръководство като:

- Мотивиран персонал;
- Квалифициран персонал;
- Ясни и точни процедури и механизми за работа;
- Процедури за проверка и защита на информационната сигурност;
- Процедури за работа при кризи или заплаха за информационната сигурност;
- Резервиране на базите данни.

Разбира се, че всяка организация трябва да приспособи всички тези отношения към собствената си среда, но и да открие допълнителни такива, които биха й дали възможност да развива системата си за информационна сигурност. Тук няма рутина, нито някакви особени правила или подходи към реалната ситуация в колективите. На теория по всеки от изброените елементи има достатъчно написани книги, правила, системи и процедури, но често те са неприложими за конкретна организация, сфера, регион или дейност.

Поредната класификация на изисквания към системата за информационна сигурност още веднъж идва да покаже стойността на човешкия фактор в нея. В следствие на това, първата и може би наистина кадрова политика на една организация е да си създаде едно многофункционално звено за информационна сигурност. Като казваме това, не означава, че една фирма с пет човека персонал трябва да включи всички тях в това звено, или да назначава нови хора, които да се занимават само с такава дейност. Това, разбира се, най-често не е възможно и е наивно да се мисли, че такава структура някога ще си го позволи. Говорим обаче за едни или двама от тези пет, най-способните ИТ-специалисти, които да поемат ангажимент и за този вид политика. Ясно е, че в службите за сигурност, държавните ведомства и др. големи организации винаги може да има дирекция „Сигурност“, „Информационна сигурност“, или просто звено в дирекция „Човешки ресурси“, които да имат отношение към защитата на информацията. Твърде вероятно е с приемането на новия регламент 679/ 2016 г. на ЕС за защита на личните данни да се подходи по аналогичен начин – „ударът“ да бъде поет от тези структури. Това е нормален вариант. Много по-сложно е да се защити информацията (в случая на примера – личните данни) от магазинче или ресторант в Смолян, от автосервиз или селскостопански производител, където такива структури в организацията няма, а и подобни кадри традиционно не достигат. Тогава наистина е добре просто едно лице да бъде определено за отговорно, да се подготви, обучи и въведе като длъжностно лице, но да има такова без споделена отговорност.

Тогава неговите усилия ще трябва да се насочат към:

- Разработване и внедряване политика, процедури и правила за информационна сигурност;

- Разработване и провеждане на програми за обучение на персонала;
- Различни функционални отговорности – анализ на риска, управление на риска, планове за информационна сигурност, мерки за информационна сигурност за всяка работна единица, периодични преценки на състоянието на системата и т.н.

Звучи сложно и претенциозно, но всъщност може да са просто една страничка с важни съвети и правила, с които това лице да покаже на служителите и работниците, че трябва да се съобразяват с изнасянето на информация.

Към подобни лица сме в състояние да направим един куп препоръки:

- Проверка на външните лица и персонала;
- Контрол върху длъжностните лица;
- Разделение на отдели и служби (ЗЗКИ дава отлични примери как трябва това да стане), на компютри от хора, които не работят с тази техника;
- Да е ясно отговорността за работните места, дейностите и процесите (да няма споделена отговорност);
- Максимум информация само на определени минимален брой служители;
- На отговорни длъжности – само проверени лица;
- Развитие на система за поощряване, признание и възможност за развитие на персонала;
- Рекламата, стандартизираният брифинг, връзките с клиенти, какво да споделяме открито –проблемът е изключително валиден за частните структури, които трябва да бъдат внимателни в своята откритост и реклама, защото колкото повече се знае за тях, толкова по-уязвими от конкуренти стават (проблем за мярата в стремежа към популярност);
- Правила за използване на данните (софтуер за регистрация на влизанията – кой, кога до кои бази данни, по каква причина, имал ли е право и т.н.);
- Ясна управленска структура (целеви групи);
- При възникнали кризи и конфликти – ротация на работните места.

Трябва да се има предвид, че емиграцията на експерти по информационни технологии няма да спре и непрекъснато ще губим такива. Това положение е проблем дори за високотехнологични и по-състоятелни държави и фирми от Западна Европа – САЩ, Китай и др. страни продължават да източват добрите специалисти. У нас тази тенденция е очевидна също. В такъв случай как да се запълни празнината след тях и как може да се реагира адекватно?

Многофункционалното звено, което препоръчахме е сред тези реакции. Добре е да бъдат привличани експерти от службите за сигурност и обществен ред. В известен смисъл те са сред специалистите, които могат да заменят или да подпомогнат останалите ИТ-експерти в противодействието на различни атаки към информационната сигурност. На пазара на труда все още се намират такива експерти. Освен всичко друго, тяхното умение за работа с хора, за анализ на риска, оценка на информацията и вземане на решение, особено бързи и интуитивни решения при кризи е също от полза на организацията. Всъщност, към всички служители в организациите и най-вече на специалистите по информационна сигурност препоръчваме:

- Необходимо е на първо място системата за информационна сигурност да се изпълни като блок схема по функционално-структурен (имаме функции – кой ще ги изпълнява) или структурно-функционален (има структура - кои са й функциите) подход;
- След това в последователност изграждането на системата да започне по схемата: анализ на риска (заплахите) – оценка на нашата среда и уязвимост – вземане на решение за системата – планиране на мероприятия и видовете сигурност – разпределение на

задачите (за техническите мероприятия може да се намерят външни изпълнители) – органи и система за контрол над информационната сигурност – планиране на действия при кризи и кризисни ситуации.

Така без да имаме достатъчен брой квалифицирани кадри, имаме достатъчно добре осведомени служители относно изграждането на една система за информационна сигурност на организацията.

Разузнавателна заплаха

Съвсем накратко по този специфичен проблем на защитата на информацията:

Разузнавателната дейност на специализирани държавни органи и големи корпорации представлява най-голяма заплаха в сравнение с дейността на други организации и групи. Основна движеща сила и обект на разузнавателната дейност е човекът. Човекът разузнава и е разузнаван! За разузнаващия човек е важно да направим едно важно разграничение – разграничението между разузнавач и агент. И двамата са „щпиони“, но:

– Разузнавачът е кадрови служител на разузнавателна структура, държавна, корпоративна или друга.

– Агентът е вербувано от разузнавач лице за изпълнение на разузнавателни задачи в интерес на разузнавателната структура, в която разузнавачът е служител.

Разузнавателната заплаха произтича от всяко действие, с което разузнаващият се стреми да допринесе за изпълнението на двете основни разузнавателни задачи – събирането на представляваща интерес информация или/и оказването на влияние върху нечие поведение, върху вземането на решения.

За решаване на поставените задачи, по правило разузнавачите и агентите използват, особено при първоначален контакт, някакво прикритие. Пред нас те могат да се появят като дипломати, журналисти, учени, експерти в различни области, активисти от обществени организации, представители на фирми и всякакви други. Ролята, в която излизат пред нас, е тяхното удобно прикритие, което им е необходимо, за да не ни отблъснат при първоначален контакт.

Разузнавателните служби по света се занимават с различни видове разузнавателна дейност: шпионаж, саботаж (проваляне на нечия дейност), диверсия (провал на част от дейността за отвличане на вниманието на противника и нанасяне на основния удар срещу него на друго място). Провеждат се и т.нар. хибридни операции – съчетание на мека и твърда сила, комбиниране на информационни операции за влияние и употреба на физическа сила (от военни и полувоенни формирования, от престъпни групи и др.). В арсенала на разузнавателните служби влиза също използването на корупцията, маргинализирани социални групи, екстремистки и терористични движения и пр.

Разузнавателниятподход за привличане към сътрудничество обхваща поне пет основни етапа: проучване, набелязване, изучаване, подбор и привличане към сътрудничество.

Технологията на привличането към сътрудничество включва:

- първоначални неангажиращи контакти,
- зачестяващи срещи,
- установяване на трайни отношения,
- проява на разбиране към проявените от кандидата за вербуване желания и интереси, предпочитания и убеждения,
- изразяване на разбиране и подкрепа, подпомагане във вземането на трудни решения,
- предложение за сътрудничество.

За да вербува, вербовчикът трябва да се превърне в истински приятел на вербувания! Без лицемерие! Ето тук е ключето на разузнавателното майсторство, границата, която разделя и свързва чисто човешките отношения с разузнавателните задачи.

Има и по-груб вариант. Служителят, който е обект на разузнавателен подход, да открие, че този, с когото развива приятелски отношения, разполага с компрометираща информация. В даден момент компроматът обикновено се поднася заедно с обещание за подкрепа, за избягване на отрицателните последици, т.е. отново с проява на „приятелско“ отношение. Практиката показва, че т.нар. „вербовка на компрооснова“ не е надеждна основа за трайно сътрудничество. Всяко лице, подложено на натиск чрез компромат, иска да се избави от този натиск и от компромата, от който е зависимо. За да продължи сътрудничеството на компрооснова, е необходим постоянен натиск, постоянна принуда за все по-компрометиращи действия, така че нито за миг да не може да се откаже сътрудничество. Затова много често разузнавателните служби използват членове на организирани престъпни групи за проникване в средата, от която имат интерес и в която могат да реализират своите цели. Престъпниците са удобни за компрометиране. Но може и да не знаем, че са престъпници. Разузнавателните служби използват корупцията и пороците на хората, за да ги манипулират и да оказват натиск.

Предложението за сътрудничество идва след продължителен период на вече установени отношения. Когато е отправено пряко, тогава имаме т.нар. пряк подход. Предложението е от името на разузнаващата структура – служба или корпорация.

Другият подход е т.нар. подход под чужд флаг. Предложението се прави от името на т.нар. прикритие, структура, различна от разузнавателната: медия, обществена организация, академична общност или нещо подобно, под благовиден и приемлив предлог. Зад тази структура-прикритие, която по правило е със съвсем законна дейност, стои чуждата разузнавателна структура. В даден момент разузнавателната структура може да реши, че прикритието не ѝ е нужно и да разкрие истинския характер на сътрудничеството.

Друг подход е непрекият подход. Открива се благовиден предлог и се установява някакъв общ интерес. Общ интерес между служителя, който е обект на разузнавателен подход, и разузнавача, чиито истински цели служителят не познава. В общуването помежду им двамата „откриват“ общия интерес.

3. Заключение

Разузнавателната заплаха може да бъде разпозната и рискът от нея – предотвратен. Затова трябва да имаме предвид, че този, който се стреми да ни привлече към сътрудничество, обикновено:

1. Проявява силен интерес към нас.
2. Стреми се да ни бъде приятел.
3. Винаги проявява разбиране.
4. Обикновено търси повод за нови срещи с нас.
5. Организира „случайни“ срещи с нас, дори само „онлайн“.
6. Знае за нас повече от нормалното.
7. Проявява силен интерес към наши познати.
8. Проявява интерес извън заявения.

Ако разпознаем или дори само се усъмним, че ние или наши познати са обект на разузнавателен подход, трябва да съобщим на компетентните органи. Няма място за притеснение, ако споделим тази информация. По-добре да сгрешим, отколкото да се окажем прави!

Към кого да се обърнем? Към контраразузнаването – Държавна агенция „Национална сигурност“ (ДАНС). Ако нямаме контакт с ДАНС, можем да се обърнем към служителя по сигурността на информацията, който трябва да информира ДАНС. Можем да потърсим контакт и с друга служба за сигурност или обществен ред, към всеки орган, който може да сигнализира или помогне да споделим подозренията си.

ЛИТЕРАТУРА:

[1] Закон за достъп до обществена информация.

[2] Закон за защита на класифицираната информация.

[3] Закон за защита на личните данни.

[4] Гюров, Румен, Овладяване на риска, С., Авангард Прима, 2018 г.

[5] Домозетов, Христо, Микрокомпютри, човек, информационна сигурност, с., Ел Ге, 1996 г.

Име на автора: проф. д-р инж. Иво Великов Великов
Месторабота: Член на ДКСИ и професор във Висше училище по сигурност и икономика – Пловдив
E-mail: manoflight@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 11 - 16 Problems of Security Systems

A VIEW ON THE PROCEDURES FOR IMPLEMENTATION OF SPECIAL INVESTIGATION MEANS IN THE FEDERAL REPUBLIC OF GERMANY

ILIN A. SAVOV

ABSTRACT: *This report addresses some of the procedures for the application of special intelligence tools in the Federal Republic of Germany. The rules regarding the authorization, use and control of the operating methods by the respective state bodies are specified. The new operational tool, the so called "raster search". On the basis of the review of the German legislation on the use of special intelligence means, conclusions are made.*

KEYWORDS: *Special investigation means, data retention, raster search, undercover officer, Federal Republic of Germany.*

ЕДИН ПОГЛЕД ВЪРХУ ПРОЦЕДУРИТЕ ПО ПРИЛАГАНЕ НА СПЕЦИАЛНИ РАЗУЗНАВАТЕЛНИ СРЕДСТВА ВЪВ ФЕДЕРАЛНА РЕПУБЛИКА ГЕРМАНИЯ

ИЛИН А. САВОВ

АБСТРАКТ: *В настоящия доклад се разглеждат някои от процедурите по прилагане на специални разузнавателни средства във Федерална република Германия. Посочени са правилата по отношение на разрешение, използване и контрол на оперативните способи от съответните държавни органи. Анализиран е новият оперативен способ т.нар. растерно търсене. Въз основа на направеният преглед на германското законодателство във връзка с използването на специални разузнавателни средства са направени изводи.*

1. Въведение

Федерална република Германия се явява водеща страна в Европейския съюз както в икономическо, така, по мнението на практически всички анализатори, и в политическо отношение. Поради това ще разгледаме основните правни принципи, върху които се изгражда използването на оперативните способи при разследване на престъпления, в това число, придобиване на информация чрез тези, които в нашето законодателство са наречени „специални разузнавателни средства“. Тези въпроси достатъчно пълно са разработени в Наказателно процесуалния кодекс, раздел VIII[1] „Следствени действия“ (Strafprocessordnong Abschnitt 8 - Ermittlungsmaßnahmen) на ФРГ, Закона за телекомуникациите[2] и някои други нормативни актове.

В доклада няма да разглеждаме всички следствени действия, а само тези оперативно-технически способи, които съответстват на нашия ЗСРС. В немския НПК подробно са описани способите, за разкриването на какви престъпления могат да се прилагат и кои органи дават разрешения за тяхното прилагане.

[1] Strafprozeßordnung (StPO) - Наказателно-процесуален кодекс в редакцията му, публикувана на 7 април 1987 г. (I, стр. 1074, 1319), последна промяна на 30 октомври 2017 г. (I, стр. 3346) .

[2] Telekommunikationsgesetz (TKG) – Закон за телекомуникациите от 22 юни 2004г. (BGBl. I S. 1190), последна промяна от 30 октомври 2017 г. (BGBl I стр. 3618).

2. Изложение

Разрешението за контрол на телекомуникациите се насочва само срещу обвиняемия или срещу лица, които въз основа на определени факти се предполага, че получават или съобщават на обвиняемия конкретни или последващи съобщения или че обвиняемият използва своята система за връзка или информация.

По силата на разрешението всяко лице, което предоставя или участва в предоставянето на телекомуникационни услуги[3], съгласно § 152 от Закона за съдебната власт осигурява тези мерки[4] за Съда, прокуратурата и разследващите лица на полицейските служби. Има все пак някои допълнителни изисквания съгласно Закона за телекомуникациите и Наредбата за наблюдение на телекомуникациите.

При осъществяване на контрола трябва технически да се гарантира това, че:

1. могат да бъдат наблюдавани и записвани само:

а) текущи телекомуникации, или

б) съдържанието и обстоятелствата на съобщението, които биха могли да бъдат наблюдавани и записани по време на настоящия процес на предаване в обществената далекосъобщителна мрежа от датата на разрешението;

2. са направени само промени в системата на информационните технологии, които са от съществено значение за събирането на данни, и

3. промените, направени при завършването на мярката, доколкото това е технически възможно, автоматично се отменят.

Има изисквания за протоколиране при всяко използване на техническото оборудване за целите на наблюдението.

Подслушването на помещения може да бъде насочено срещу обвиняемия и да се извършва само в дома на обвиняемия [7]. В домовете на други лица мярката е допустима само ако въз основа на определени факти може да се приеме, че това е възможно, например:

1. обвиняемият, посочен в разрешението, пребивава там и:

2. прилагането на способа само в жилището на обвиняемия не ще доведе до разследване на обстоятелствата по делото или до установяване местоположението на друг обвиняем на същото наказателно производство.

Извън пределите на жилищата изказвания[5], направени непублично, могат да се подслушват и записват [7] с помощта на технически средства[6] също без знанието на лица, към които се прилага мярката, ако на основание на конкретни факти съществува подозрение, определеното лице е извършило престъпно деяние, посочено § 100а (абз.2)[7], в качеството на изпълнител или съучастник, явяващо се тежко също в конкретния случай, или опит за такова престъпно деяние, ако опита се явява процесуално наказуем и разследването на обстоятелствата по делото или установяване местонахождението на

[3] Всяка организация, оказваща услуги в сферата на телекомуникациите, в това число, извън публичните мрежи, т.е. така също вътре в предприятия и учреждения в рамките на интранета, е длъжна да предостави достъп съгласно абзац 3 (изр.1) в съчетание с § 110 (абз.1, изр. 6) от Закона за телекомуникациите.

[4] Съгласно § 110 от Закона за телекомуникации допълнителни мерки (например, предоставяне на технически устройства и осъществяване на организационни мерки) са длъжни да предприемат само организации, предлагащи своите услуги на широката публика, при което някои от тях са изключени съгласно § 3 (абз. 2) на Постановлението за контрол на телекомуникациите.

[5] Получаване на информация за действията на контролираното лице извън жилищата не е възможно без наблюдение и проследяване.

[6] Това положение се прилага само при подслушване с помощта на технически средства, но не и при послушване без използване на технически средства, както случайно, така и запланирано.

[7] Списък на престъпленията, за които е допустимо да се осъществява наблюдение на телекомуникациите.

обвиняемия по друг способ не би имало шансове за успех или би било съществено затруднено.

Мярката може да се прилага само към обвиняемия. Разрешението за прилагане на мярката по отношение на други лица[8] може да бъде издадено, само ако на основание на конкретни факти съществува предположение, че те са в контакт с обвиняемия или такъв контакт ще бъде установен, прилагането на мярката ще доведе до установяване на обстоятелства по делото или местонахождението на обвиняемия и установяването по друг способ не би имало шансове за успех или би било съществено затруднено.

Прилагането на мярката се разрешава също, даже ако е неизбежно, че ще бъдат засегнати трети лица.

Процедурата по прилагане на този способ в основни линии е същата, както описаната в § 100е за другите оперативно-технически способи, свързани с послушването.

Когато това е необходимо за разследване на факти или определянето на местоположението на обвиняем, изисканите данни, събрани на основание §§ 95 и 111 от Закона за телекомуникациите, се предоставят от телекомуникационната организация, предоставяща или участваща в телекомуникационните услуги (съгласно § 113 параграф 1, изречение 1 от Закона за телекомуникациите). Отнася се за искане на информация до данни, чрез защитен достъп до терминали или на устройства за съхранение, като се използват пространствено разделени терминали, съгласно § 113 параграф 1, изречение 2 от Закона за телекомуникациите. Информацията може да се изисква само ако законовите изисквания за използване на данните са налице.

Информацията за трафичните данни може също така да изпрати към определен интернет-адрес, както се разрешава от § 113 (абз. 1, изр. 3) и § 113с (абз. 1, т. 3) от Закона за телекомуникации.

Искане на информация за трафичните данни до съда може да бъде изпратено само от прокуратура. В случаите на непосредствена опасност, разпореждането може да бъде издадено от прокурора или упълномощен от него служител от разследващия персонал съгласно § 152 от Закона за съдебната система. В този случай, обаче, съдебно решение трябва да бъде поискано незабавно. Горните изисквания не се прилагат, ако засегнатите от искането за информация вече го имат или са запознати или ако използването на данните вече е разрешено с решение на съда.

Засегнатото лице се уведомява доколкото е възможно и възможно най-скоро за разкриването на данните за трафика. Уведомяването се извършва дотолкова, доколкото това не противоречи на целта на разследването. Уведомяването не се извършва, ако то противоречи на първостепенните интереси на трети страни или на самото засегнато лице. Ако уведомяването е отложено, то причините трябва да се запишат.

При наличие на искане за информация за данните от трафика организацията, която предоставя или участва в предоставянето на телекомуникационни услуги, предава необходимата информация незабавно [7].

Ако съществува подозрение, основано на конкретни факти, за това, че определено лице в качеството на изпълнител или съучастник е извършило престъпно действие, явяващо се значително също в конкретния случай, особено, престъпно деяние, посочено в § 100а абз. 2 или опит за такова деяние, явяващо се значително също в конкретния случай, ако опита се оказва процесуално наказуем[9] или е подготвило такова деяние посредством

[8] Съгласно § 148 от НПК на ФРГ прилагането на тази мярка към защитника е забранено. Ограничения съгласно § 160а от НПК на ФРГ действат и към други носители на професионална тайна. По отношение на роднини ограничения не са постановени.

[9] Наказуемостта на опита е определена в §§ 23 ал. 1 от НК на ФРГ.

друго престъпно действие, то с помощта на технически средства[10] могат да бъдат установени:

1. Номера на прибора на мобилния телефон[11] и номера на неговата карта[12] , а също
2. Местонахождението на мобилния телефон,

ако това е необходимо за разследване обстоятелствата по делото или установяване местонахождението на обвиняемия.

В рамките на прилагане на такива мерки е допустимо да се събират лични данни на трети лица само ако по технически причини това е неизбежно за достигане на посочените по-горе цели. Тези данни могат да се използват само за сравнение с цел установяване на търсения номер на прибора или SIM - картата и трябва да бъдат незабавно унищожени с завършване прилагането на мерките.

§ 100a (абз. 3)[13] и § 100e (абз. 1, изр. 1 ÷ 3[14], абз. 3, изр. 1[15] и абз. 5, изр. 1[16]) се прилагат mutatis mutandis. Поръчката е ограничена до максимум шест месеца. Необходимо е удължаване с продължителност не повече от шест месеца при условие, че продължават да се прилагат условията, посочени в началото на този способ.

Един от способите, който няма аналог в българското законодателство, е така нареченото ***растерно търсене***. То се използва както в наказателния процес (§§ 98a, 98b, 98c), така и в превантивната дейност на полицията на основание административното право на провинциите за установяване кръга на потенциално заподозрени. Става дума не за издирване, а за компютърно търсене в базите данни на лица, които изпълняват определени критерии (например: мъж, възраст 20 – 30 години, жител на Мюнхен,, блондин, притежател на Фолксваген Голф, левичар). В превантивната дейност на полицията този метод се използва основно в борбата с тероризма и организираната престъпност.

Същността на този способ представлява най-често автоматизирано сравняване на данни, събрани извън наказателния процес и не за неговите цели. Те указват характерните белези (Pruefungsmerkmale) на евентуалния извършител на разследваното престъпление, които се сравняват с тези на други лица, за да се установят лицата извън подозрение или лицата, притежават някои от характерните белези на извършителя и са свързани с по-нататъшното разследване.

---

[10] За установяване на данните може да бъде използван така наречения пеленгатор IMSI (IMSI catcher). Тази мярка се отличава от мерките съгласно § 100g с това, че в случаите на § 100i данните, с които разполагат органите на наказателното преследване са недостатъчни, за да се осъществи нито подслушване съгласно § 100a, нито за получаване на информация за връзките съгласно § 100g. Затова с помощта на конкретно техническо устройство първоначално се установява номера на прибора и/или сим-картата и доколкото съществува непосредствена връзка, също местонахождението на прибора. Някои модификации на пеленгатора IMSI да се подслушват разговорите, обаче тази модификация може да се използва само в съответствие с изискванията на § 100a.

[11] Има се предвид идентификационния номер на прибора IMEI (International Mobile Equipment Identity).

[12] Има се предвид идентификатора на абоната IMSI (International Mobile Subscriber Identity) , явяващ се индивидуален и известен само на телекомуникационния оператор.

[13] § 100a (3) Заповедта се насочва само срещу обвиняемия или срещу лица, които въз основа на определени факти се предполага, че получават или съобщават на обвиняемия конкретни или последващи съобщения или че обвиняемият използва тяхната система за връзка.

[14] § 100e (1) Мерките по § 100a могат да бъдат разпореждани от съда само по искане на прокурора. В случай на непосредствена опасност заповедта може да бъде взета и от прокурора. Освен ако разпореждането на прокуратурата не бъде потвърдено от съда в рамките на три работни дни, то престава да бъде ефективно.

[15] § 100e (3) Заповедта се изготвя в писмена форма.

[16] § 100e (5) Ако условията на заповедта вече не съществуват, мерките, взети въз основа на заповедта, се прекратяват незабавно.

Процедура за разследване при растерно търсене.

За разследването с компютър разрешението се издава от съдията. В изключителни случаи при необходимост от незабавни действия разпореждане може да бъде дадено от прокурора, който е длъжен незабавно да уведоми съдията. Ако до три дни последният не потвърди, разпореждането губи силата си. Разрешението се предоставя в писмена форма. В него трябва да са посочени лицата или организациите, които са длъжни да дадат данните, и данните трябва да бъдат ограничени с признаци, необходими в конкретния случай. Предаването на данните, използването на които е ограничено със специални федерални[17] или на провинциите правни актове, не може да бъде назначено.

Ако данните са предадени на носители на данни, тези данни трябва да бъдат върнати веднага след приключване на съгласуването. Личните данни, прехвърлени на други носители, трябва незабавно да бъдат заличени веднага щом вече не са необходими за наказателни производства.

След завършване прилагането на мерките по § 98а е необходимо да се уведоми държавния орган, в компетенциите на който се отнася съблюдаването на положенията за защита на личните данни, съхранявани от държавните органи.

За разследване на престъпно деяние или за установяване местонахождението на лица, обявени за издирване във връзка с наказателно производство, личните данни от материалите за наказателно производство могат автоматично да се сравняват с други данни, запазени във връзка с наказателно преследване или с изпълнение на наказания за извършени престъпления или с предотвратяване извършването на нови престъпления.

Служителите под прикритие могат да бъдат използвани за разследване на престъпления, ако има достатъчно фактически доказателства, че дадено престъпление е от съществено значение[18]:

1. В сферата на нелегалната търговия с наркотични вещества или оръжие, фалшифициране на пари или подправяне на платежни средства.
2. В областта на защитата на държавата (§§ 74а, 120 от Закона за съдебната власт),
3. Във вид на занятие или нееднократно вследствие на особена склонност.
4. Организирани от член на банда или друга престъпна организация.

За разкриване на престъпни деяния служителите под прикритие могат да се използват също, ако на основание на конкретни факти е установена опасност от рецидив. Използването на служителите под прикритие е допустимо също, ако разкриването по друг способ би било невъзможно или съществено затруднено. За разкриване на престъпления служителите под прикритие могат да се използват също, ако това е целесъобразно във връзка с особеното значение на деянието и други мерки не биха имали шансове за успех.

Служителите под прикритие са държавни служители на полицейска служба, водещи разследване под друга самоличност, създадена за тях за продължително време (легенда). Те имат право да участват в правоотношения под легендата.

Ако това е необходимо за създаване и съхранение на легендата, могат да се създават, изменят и използват съответните документи.

От гореизложеното могат да се направят някои основни изводи:

- Наказателно-процесуалния кодекс на ФРГ подробно регламентира условията, които правят допустимо прилагането на всеки един оперативен способ.

---

[17] Например, съгласно положения в Данъчния кодекс [Abgabeordnung}; § 39 от Закона за пощите [Postgesetz]; § 35 от Социалния кодекс I [Sozialgesetzbuch I]; § 67 и последващите от Социалния кодекс X [Sozialgesetzbuch X]; § 88 от закона за телекомуникациите [Telekommunikationgesetz].

[18] Дословно: престъпно деяние, имащо важно значение (Straftat von erheblicher Bedeutung). Законодателят използва това ограничение за съблюдаване на принципа за съразмерност.

- Изброяват се изчерпателно престъпленията за всеки способ, които правят възможно неговото използване.
- Процедурите по отношение на получаването на разрешение, прилагане, използване на събраните данни и прекратяване, както и начините за контрол на федерално ниво и на ниво провинции също са детайлизирани за всяка приложена мярка.
- За разлика от нашата страна някои от способите могат да се използват при престъпления със средна тежест, дори при превантивната дейност на полицейските органи.

3. Заключение

Структурите в сферата на сигурността на Федерална Република Германия са натоварени със специални правомощия, които се характеризират с необходимостта от висок професионализъм, наличие на специфични умения и компетентности и не на последно място - с работа в условия на конспирация и невъзможност за публично огласяване на дейността. От своя страна държавните органи са ангажирани да променят и допълват всички нормативни актове, свързани със защита на националната сигурност и борбата срещу тежката организирана престъпност, които да отговарят на съвременните предизвикателства и опасности.

ЛИТЕРАТУРА:

[1] Закон за специалните разузнавателни средства.

[2] Закон за противодействие на тероризма.

[3] Strafprozeßordnung (StPO) - Наказателно-процесуален кодекс в редакцията му, публикувана на 7 април 1987 г. (I, стр. 1074, 1319), последна промяна на 30 октомври 2017 г. (I, стр. 3346).

[4] Telekommunikationsgesetz (TKG) – Закон за телекомуникациите от 22 юни 2004г. (BGBl. I S. 1190), последна промяна от 30 октомври 2017 г. (BGBl I стр. 3618).

[5] Abgabeordnung - Данъчния кодекс на Федерална Република Германия.

[6] Postgesetz - Закона за пощите на Федерална Република Германия.

[7] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 386-391.

Име на автора: проф. д-р Илин Александров Савов
Месторабота: Ректор на Висше училище по сигурност и икономика - Пловдив
E-mail: ilin_savov@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 17 - 22 Problems of Security Systems

GENERAL ORGANIZATIONAL SECURITY THEORY

EVGENI P. MANEV

ABSTRACT: *The article argues that general security theory can be generated even some authors do not share such an idea. The evidences obtained by applying the methodology of scientific approach based on objective facts and laws driving establishment and development of social organization regarded as a complicated system that have to ensure its functions and normal existence.*

KEYWORDS: *Theory, security, organization.*

ОБЩА ТЕОРИЯ НА СИГУРНОСТТА НА ОРГАНИЗАЦИЯТА

ЕВГЕНИ П. МАНЕВ

АБСТРАКТ: *В темата се доказва, че може да се генерира обща теория за сигурността на организацията противно на твърденията на някои автори. Доказателствата следват методологията на научния подход и се основават на обективните закономерности, по които се самоорганизира и развива сложната система на социалната организация, за да осигури изпълнение на необходимите организационни функции и нейното нормално съществуване.*

1. Въведение

Темата за сигурността на организацията и на личността съществува толкова време колкото съществуват и те. Тя се изучава от древността до наши дни и ще се изучава докато човечеството съществува поради своята динамична същност. Има изобилие от литература за обяснение на същността и съдържанието на основни понятия в сигурността, както и анализи на сигурността. Не са редки случаите когато тези основни понятия са в противоположни посоки. Тези факти показват, че няма единно разбиране. Една от причините за това е, че в повечето случаи анализите се базират на лични мнения и конкретен емпиричен опит на авторите, които рядко се опират на изводи, базирани на закономерности на процесите и явленията в социалната организация – колектив, корпорация, държава, регионална или глобалната система.

2. Изложение

Някои автори изразяват мнението, че сигурността не е наука, тя е изкуство и практика, с което е трудно да се съгласим от научна гледна точка. Такъв подход означава, че научните теории за обясняване на сигурността нямат място в реалния бит на човека. Следователно те са лаически. Ако това е така, не би следвало такива теории да намират място във висшите учебни заведения, които се занимават с научни знания.

Настоящият доклад има за цел да обоснове някои основни белези на научната теория за изучаване на сигурността на социалната организация[1]. За целта е създадена хипотезата, че известни научни теории могат да се интерпретират и чрез прилагане на научния подход

[1] По-нататък в текста за краткост ще се използва понятието организация в смисъл социална организация.

и методология е възможно да се да се създаде самостоятелната научна дисциплина – обща теория за сигурността.

За да се обоснове общата теория на сигурността трябва да се докаже, че тя отговаря на общоприетите изисквания за отделна научна теория. На следващ етап да се даде определение на понятието сигурност, да се изясни неговата същност и съдържание, да се дефинира основната роля и основните функции на сигурността. Да се определят критериите за таксономия на нивата на сигурност в организацията. Трябва да се докаже, че тези теоретични постановки са общовалидни за всяка организация.

Знанието за сигурността се е формирало като част от знанието за света в границите на една самостоятелна сфера, обикновено наричана за краткост "сигурност", което от научна гледна точка не е коректно поради непълнотата си, но в практиката се използва с презумпцията за означаване на *сигурност на социалната организация*.

От своето ниво и теоретичност сигурността има свой отделен обект и предмет на изследване, които я отличава от останалите науки.

Обектът на изследване на научната дисциплина „Сигурност" е същността (т.е. закономерностите), съдържанието, формите и динамиката на състоянието на *текущото функциониране* на организацията спрямо нейното *нормално (проектно, планово) функциониране*[2] с цел постигане на поставените организационни цели, в условията на външната и вътрешна среда.

Предметът на изследване на научната дисциплина "Сигурност" е същността (закономерностите), съдържанието и формите на процесите и явленията предизвикващи рискове и заплахи за *нормалното (проектното, планово) функциониране на организацията* и пребиваване и работа на хората в нея, които ако не се смекчат или избегнат, биха я отклонили от нейната проектна (планова) функционалност, с което биха застрашили частично или напълно постигането на организационните цели или съществуването на организацията, т. е. биха създали по-ниско ниво на сигурност за самата организация и нейните членове.

Сигурност изучава същността (т.е. закономерностите), съдържанието и динамиката на състоянието на *нивото на функциониране на организацията*[3] в съответствие с поставените цели, в условията на външната и вътрешна среда, възникване и развитие на процеси, явления и феномени, които могат да създадат рискове и заплахи за плановото функциониране на организацията, при което неизбежно се налага целенасочена управленска организационна и техническа дейност за запазване или възстановяване на същото.

Теорията на научната дисциплина „Сигурност" изучава същността, съдържанието, формите и характеристиките на рисковете и заплахите за организацията от гледна точка на нейното нормално функциониране както и същността, съдържанието, формите, начините и средствата за борба с тях. „Сигурността" изучава най-общите закономерности и съдържание на функциониране на организацията като динамично нейно състояние от гледна точка постигане на нейните цели в планираните срокове, с използване на планираните за използване ресурси, с цел получаване на необходимите количествени и

[2] Под планово функциониране на организацията се разбира текущо функциониране, което отговаря на проектното – съгласно плана (проекта) на организационно-функционално-архитектурния модел на организацията, създаден за постигане на нейните цели.

[3] Под ниво на функциониране на организацията се разбира степента в която текущото функциониране отговаря на проектното – съгласно плана за организационно-функционално-архитектурния модел на организацията за постигане на нейните цели.

качествени показатели на произведения продукт[4]. На тази база във функционален аспект науката за сигурност се разбира, отъждествява и представя в рамките на научната дисциплина "Сигурност".

Общата теория на сигурността доказва изискванията към съдържанието на определението за понятието сигурност (не дава единно определение на понятието *сигурност, дефинира основната роля и функции на сигурността в организацията, които са общо валидни за всяка организация.* Решаване на проблема с определението в науката е от фундаментално значение за нейното развитие. В общата теория на сигурността е използвана аналитично обоснованата концепция за извеждане на най-важните (основни) изисквания за съдържанието на определението з сигурност на организацията[5].

От методологична гледна точка е подбран многодисциплинарен инструментариум за изследване на сигурността. За решаване на поставената задача е целесъобразно и методически правилно е научният подход да се прилага през цялото време на изследванията. На следващо място са подбрани подходящи теории и техните методи, които са използвани като инструментариум за анализите. Следвайки тази логика, общата теория за сигурността използва знанията и методите на три основни сфери от научното знание: изучаването на организацията като сложна социална система, принципния концептуален функционален-организационно-архитектурен модел на организацията и теорията на организационната култура. Тези теории се интерпретират през призмата на основните социални закони, които се отразяват и развиват в законите на организационното и държавно строителство през националната култура и културния код[6].

Другият принципен концептуален подход е хипотезата са равновесната точка на функциониране на системата, която е доказана в теорията на системите и е изведен законът, че „всяка система се стреми към равновесната си точка на функциониране". На тази база се доказва, че изкуствените организации трябва да се планират така, че да работят в планов режим в равновесната точка на системата –организация. Този подход решава няколко важни въпроса:

- Задължава прилагане на функционален подход при изучаване и планиране на организацията.
- Задължава планирането на организационното функциониране да става в равновесната точка, т.е. в точката в която системата постига своите цели по възможно на-добрия начин.
- В тази точка системата има най-високо ниво на сигурност (хипотеза, която е доказана в общата теория на сигурността).

В рамките на научната дисциплина "Сигурност" като производни учебни дисциплини се представят „Национална сигурност", "Международна сигурност", "Глобална сигурност", "Икономическа сигурност", "Демографска сигурност" "Военна сигурност" и др. Тъй като това са тясно определени съставни области в обхвата на общото понятие сигурност, удачно е те да се наричат аспекти на сигурността – направления за нейното изучаване, които имат общ предмет, но обясняват различни страни, процеси и закономерности от този общ предмет. Основанията за това са, че сигурността не може да се разглежда извън рамките на социалната организация, поради

[4] Тук под понятието *продукт* се разбира материален или нематериален резултат, получен в следствие функционирането на организацията за постигане на планираните количествени и качествени показатели.
[5] Манев, Е., Доклад на тема: „Определение за сигурност – организационнокултурен подход", НК с международно участие на тема: „Право и интернет" (панел „Проблеми на сигурността"), 21 и 22.05.2016 г., БСУ.
[6] Пак там.

което е правилно научната дисциплина, имаща предмета на общата теория на сигурността на социалната организация да се нарича "Сигурност на организацията" или както е прието за краткост "Сигурност", но с тази презумпция. Социалната организацията разбирана в този смисъл, като абстрактно събирателно понятие на общност от хора, се отнася както за държавата, така и за международните организации в даден определен смисъл – политически, икономически, социален и т.н. Понятието сигурност се експлоатира интензивно в ежедневието на хората от векове. По своето съдържание то е толкова всеобхватно колкото самия бит на хората, така че едва ли има област на живота, в която да не се употребява, да не се отнася и да не е натоварено с обща и специфична същност и съдържание. То присъства в ежедневните ни отношения с останалите хора в обществото, при пътуването за работа, при използването на съвременните средства за електронна комуникация, бизнес, услуги и къде ли не още. Всичко това се случва и възприема индивидуално от човека или групово в социалната среда. Това обуславя неговото богато съдържание, универсалност, но не изключва и неговата специфична натовареност с конкретно съдържание и степен (ниво на сигурност).

Целта на изследванията на научната дисциплина "Сигурност" е изучаване и създаване на специализирани, научни знания за рисковете и заплахите за социалните организации за тяхното проектно функциониране и постигане на проектните им цели, изучаването им и на тази основа предлагане на начини за тяхното преодоляване или избягване. За постигането на тази цел, научната дисциплина *"Сигурност" решава следните по-важни задачи:*

- Създава научни теоретични и приложни знания на общата теория за сигурността на организацията;
- Генерира научни теоретични и приложни знания на останалите дялове от теорията за сигурността като: знания за структурите за организационно и политическо управление; *аспектите на сигурността* (политически, икономически, демографски и др.); секторите на сигурността (стопански, промишлен, енергиен, отбрана и др.); знания за *функционално-структурната сигурност* (на отделни важни (стратегически) обекти и структури; стратегически енергийни възли и централи, комуникационни възли (пристанища, сухопътни, морски и въздушни възли, енергийни, водни и други важни за сигурността обекти). Изучава сигурността на функциите на системите, от гледна точка на осигуряване постигането на целите на организацията.
- На базата на създадените знания за функционално-структурната сигурност се предписват мерки за нейната същност и съдържание за поддържане на необходимото ниво за нормалното функциониране на организацията разглеждан като сложна социална система. На следващо по-ниско ниво идват *обектовата сигурност* – сигурността на относително самостоятелните обекти изпълняващи самостоятелни задачи в обхвата на дадена функция. На това ниво вместо за сигурност, е по-правилно да се изследват безопасните условия на труд и надеждност на техническите системи.
- Създава научната теория и практика на важни раздели като: „Национална сигурност", „Международна (регионална и глобална) сигурност".
- Създава научните теоретични и приложни знания, които са база за разработване на основни документи на държавата като Конституцията и законите, Стратегията за национална сигурност, Националната военна (отбранителна) стратегия, концепции, доктрини, и др.

Сигурността има смисъл да се разглежда само в контекста на социалната организация. Извън социалната организация не съществува „абстрактна” сигурност. Поставен въпросът за сигурността води след себе си много други важни въпроси като: Каква сигурност? Колко сигурност? Сигурност за кого? Сигурност къде и кога? Сигурност как и на каква цена, с какви ресурси? С какви критерии и как да се измерва сигурността? и др. Всички тези въпроси кореспондират с една или друга социална организация и отделния човек, в качеството му на неин *основен* градивен елемент, който не може да съществува извън нея. Посочените дотук най-общо предмет, цел и задачи на научната „Сигурност” обосновават нейния интегрален характер. Това означава, че изучаването на сигурността не е по силите на отделна наука, а следва да се ползват знанията и инструментариума на много науки, в обхват, обем и съдържание необходими за постигане целите на необходимата сигурност на организацията. Това не означава, че науката “Сигурност”, няма и не може да има специфичен инструментариум за изследвания. Например, специфични инструменти са измерване степента на сигурност в социалните групи (организации), сравнителен анализ на баланса на ресурсите на организациите – човешки, териториални, материални, финансови, военните и др.

Общата теория за сигурността на организацията се опира на някои общи фундаментални науки като философия, култура, теории на системите, организационни теории, психология, социология, политология, кибернетика и др.

Следователно понятието сигурност има два аспекта – широк и тесен. В широк смисъл (аспект) сигурността следва да се разглежда като общо понятие за обозначаване на определено състояние на стабилност и предсказуемост на дадена сложна социална система, а в тесен (специализиран) смисъл (аспект) тя се отнася към специфични съставни подсистеми от системата от по-висш порядък (например системите икономическа, политическа, военна, социална и т. н., които са рекурсивни системи от системата за национална сигурност (система от по-висш порядък), която е подсистема на държавата, разглеждана като социална организация. В науката важно място заема подреждането на използваните понятия в дадена научна област. В общата теория на сигурността, понятието *сигурност* е родово понятие, а *аспектите на сигурността са видови понятия*. За тази цел и по-голяма яснота в общата теория на сигурността са въведени понятията: сигурност в широк смисъл – *„сигурност-ш”,* понятието сигурност в тесен смисъл – *„сигурност-т”.* Поради това същността и съдържанието на категорията „*сигурност-ш“*, отнасящо се до сигурността в широкия смисъл, се разкриват с инструментариума на фундаменталните теоретични знания, като се използва мултидисциплинарният подход от обществените науки като философия, социология, култура, системните теории, етика, естетика и други, докато същността и съдържанието на „*сигурността-т“*, отнасяща се до сигурността в тесен, смисъл се разкриват с инструментариума на частните науки в дадено конкретно научно направление например за политическия аспект на сигурността – държавознание, политология, право и др., за икономическия аспект на сигурността – икономическите науки, за военния аспект – военните науки и т.н.

Понятието сигурност в широк смисъл е познато в науката за сигурността, като неговото съдържание включва изучаването както на общите теоретични закономерности така и нейните съставни компоненти, наричани аспекти като политически, икономически, военни, етнографски, екологически и др. Възприемането на сигурността, като общи теоретични постановки и възгледи, които са общовалидни и за всеки един от нейните аспекти следва, да се разглежда като ***обща теория на сигурността***, която разкрива нейните закономерности, същност и съдържание. Това е, което следва да разбираме и наричаме *сигурност в широкия смисъл на това понятие*. Само тази обща теория на

сигурността не е достатъчна, за да се изведат конкретни, полезни изводи и препоръки за практиката. Освен общотеоретичните знания за сигурността са необходими и специфични знания за отделните аспекти на сигурността в организацията. Тези знания също са от общ характер както знанията от общата теория на сигурността, но са от по тясна и вече по-специализирана област от научното знание. Изучаването на аспектите на дадена система за сигурност също предполага използването на мултидисциплинарния подход, но за разлика от общата теория на сигурността тук се използват знания от научните дисциплини в съответната конкретна научна област. Например за изучаването на икономическия аспект на сигурността се използват научните дисциплини в обхвата на икономическите науки, във военния аспект на сигурността се използват военните науки, в политическия аспект на сигурността се използват знанията на политическите науки и т.н. Съдържанието на знанията в обхвата на аспектите на сигурността освен, че има по-тясно специализиран характер спрямо знанията за общата теория за сигурността съдържат и конкретни специализирани знания в дадената област – икономическа, политическа, военна и т.н.

Изучаването на даден аспект на сигурността също не е достатъчно, за да се опознаят в най-големи подробности и детайли всички фактори, явления и закономерности влияещи върху нея. Задълбочаването на познанието може да се постигне, като се слезе на още по-детайлно, по-ниско ниво на изучаване на конкретните системни елементи – на нивото на отделна научна дисциплина от "пакета" научни дисциплини изучаващи дадения аспект на сигурността. На това конкретно и детайлно ниво на изучаване на сигурността, обикновено се говори за надеждност на техническите системи за безотказна работа и безопасни условия на труд при социалните системи вместо за сигурност.

3. Заключение

В заключение, общата теория на сигурността дава основите за нейното изучаване и научно обяснение. Поради ограничения в обема на докладите тук не се разглеждат доказателствата за основната роля и формите на нейното проявление в организацията, за основните и производни функции на сигурността в организацията. Също не се разглеждат и обосновките за използваните сфери на организационни-функционално-архитектурния модел на организацията във връзка с науката за културата и организационнокултурния модел и системните теории интерпретирани за изучаване на сигурността.

Използването на тези групи теоретични знания в комплекс дават основание за синтезиране на общата теория за сигурността за разкриване на нейните общовалидни закономерности, съдържание, роля и функции. Това открива пътя за по-дълбоко навлизане в проблемите на сигурността, нейното опознаване, планиране, организиране и управление с по-висока степен на научно обоснована достоверност и повишаване на ефективността на използваните ресурси.

ЛИТЕРАТУРА:

[1] Манев, Е. Глобална, регионална и национална сигурност, Софттрейд, С., 2012.

[2] Манев, Е. Организационна култура: същност, съдържание, измерване, ВИ, С. 2007.

[3] Манев, Е., Доклад на тема: „Определение за сигурност – организационнокултурен подход“, НК с международно участие на тема: „Право и интернет“ (панел „Проблеми на сигурността“), 21 и 22.05.2016 г., БСУ.

Име на автора: проф. д-р Евгени П. Манев
Месторабота: Университета по библиотекознание и информационни технологии (УниБИТ), София
E-mail: evgeni_manev@yahoo.com

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 23 - 33 Problems of Security Systems

IMPLEMENTATION OF THE FOOTPRINTING AND RECONNAISSANCE CYBER ATTACKS AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS

PETAR KR. BOYANOV, HRISTO A. HRISTOV

ABSTRACT: *In this paper implementation of the footprinting and reconnaissance cyber-attacks against the government agencies, private organizations and academic institutions is made.*

KEYWORDS: *Footprinting, Government agencies, Information Security, Modern cyber-attacks, Reconnaissance, Software vulnerability, Threat.*

ПРИЛОЖЕНИЕ НА КИБЕРАТАКИТЕ ЗА ПОЛУЧАВАНЕ НА ИНФОРМАЦИОННИ ОТПЕЧАТЪЦИ И ПРИЛАГАНЕ НА РАЗУЗНАВАТЕЛНИ ТЕХНИКИ В ПРАВИТЕЛСТВЕНИ АГЕНЦИИ, ЧАСТНИ ОРГАНИЗАЦИИ И АКАДЕМИЧНИ ИНСТИТУЦИИ*

ПЕТЪР КР. БОЯНОВ, ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *В тази статия са извършени научни експерименти и изследвания относно начините на приложение на кибератаките за получаване на информационни отпечатъци и прилагане на разузнавателни техники срещу правителствени агенции, частни организации и академични институции.*

1. Въведение

В тази статия кибератаките представляват използване на злонамерени софтуерни инструменти от киберпрестъпниците с цел намиране и експлоатиране на уязвимост в сканираната компютърна машина жертва на служителя от организацията.

Киберпрестъпникът може да бъде служител от същата организация, в която работи, софтуерен програмист, работещ в друга организация, обикновен потребител, високо квалифициран агент от разузнавателна служба или терорист [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [24], [25], [26].

Киберсигурността представлява общ набор от препоръки и решения, необходими за изграждането на защитни механизми срещу съвременните видове кибератаки.

Последиците след извършена дадена кибератака могат да доведат до пълен срив и блокиране на хардуерните и софтуерните компоненти на компютърната машина на служителя или всички компютърни машини в организацията [32], [33]. По този начин дадената организация жертва ще претърпи изключително сериозни финансови загуби. Ако уязвимостите и слабостите не бъдат открити от служителите по сигурността, тогава е възможно и пълно закриване (фалиране) на организацията [1], [2], [3], [7], [8], [9], [10], [11], [13], [15], [16], [24], [27], [28], [29], [30], [31].

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

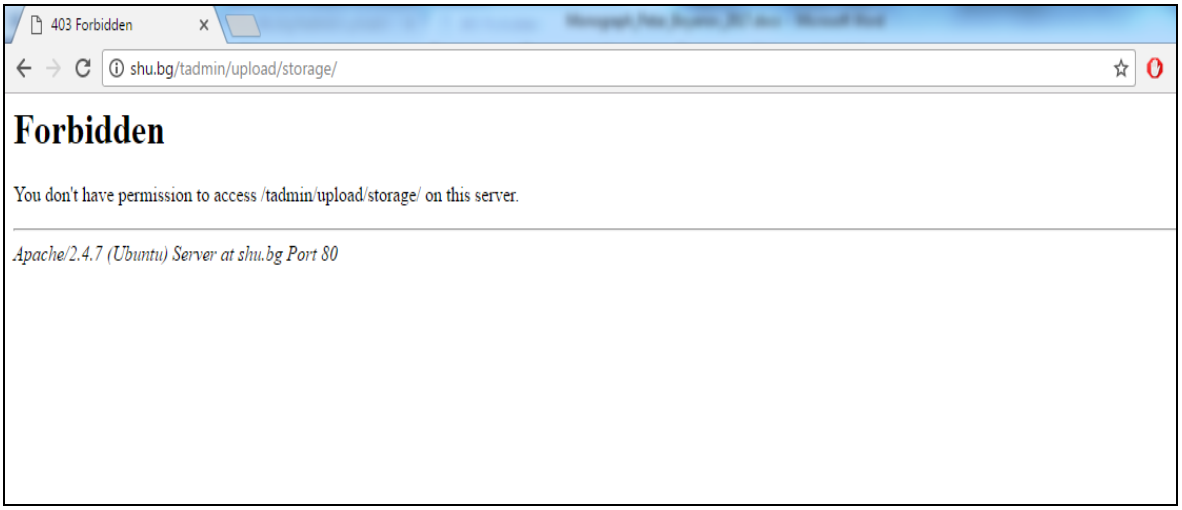
2. Изложение

Получаването на информационни отпечатъци от дадена държавна или частна организация се осъществя чрез следните начини [1], [2], [3], [4], [5], [6], [9], [12], [14], [15], [17], [21], [24], [25], [26], [27], [28], [29], [30]:

- Събиране на информация чрез публични безплатни или отворени източници.
- Активно събиране на информация.
- Анонимното събиране на информация.
- Псевдоанонимно събиране на информация.
- Събиране на информация от календара на организацията.

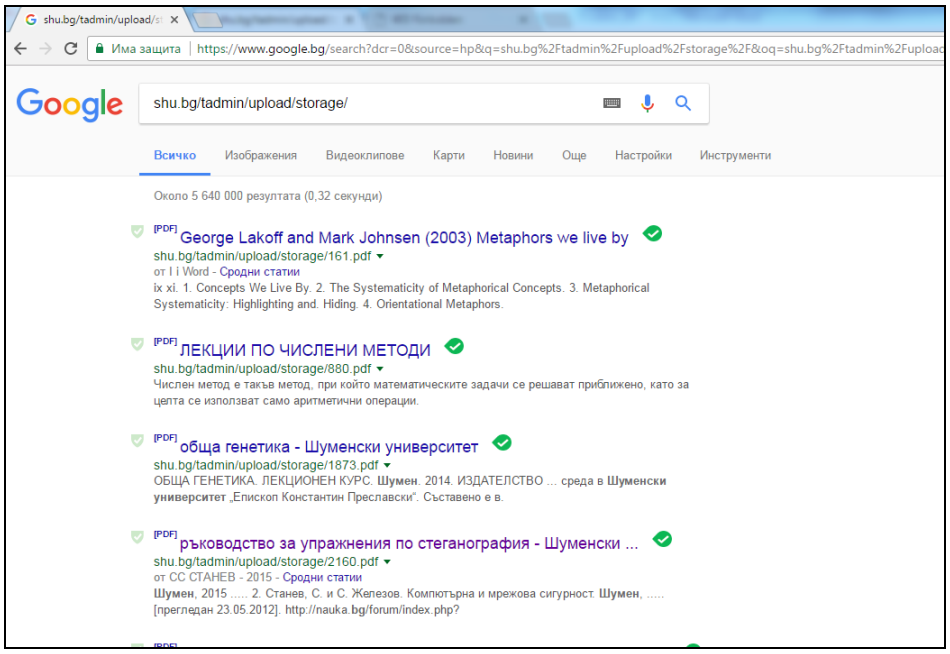
Събиране на информация чрез публични безплатни или отворени източници или средства представлява един от най-лесните начини, с които киберпрестъпникът да получи важна информация за организацията жертва [32], [33]. Типични примери за публични безплатни източници на информация са телевизията, социалните мрежи (Facebook, Messenger, LinkedIn, Instagram, Twitter, Pinterest, MySpace, Skype, Viber, Whatsapp, Google+) в интернет пространството, уеб блогове, онлайн уеб вестници и др. По този начин не се изисква по никакъв начин директен контакт и кореспонденция със съответната организация жертва [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17]. Ако бъдат използвани тези публични източници, тогава киберпрестъпникът ще може да получи информация за публичните логически мрежови IPv4 и IPv6 адреси, версията на инсталираните операционни системи в организацията, специализирания инсталиран софтуер на уеб сървъра [18], използван от организацията жертва, използваните услуги от протоколите TCP и UDP за всяка една операционна система на служител, механизмите за контрол на достъпа, цялата система на инфраструктура и налични системи за откриване и предотвратяване на неоторизирани прониквания [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [18], [19], [20], [22], [23], [25], [26], [27], [28].

Благодарение на кибератаката за получаване на информационни отпечатъци чрез търсещи машини се разкри, че достъпът до следния уеб линк „shu.bg/tadmin/upload/storage/“ е забранен. Това е показано на фиг. 1. Но в същото време ако този адрес бъде написан в търсещото поле на Google, тогава излиза дълъг списък с учебни материали, които не трябва да бъдат с отворен достъп! Това е показано на фиг. 2.

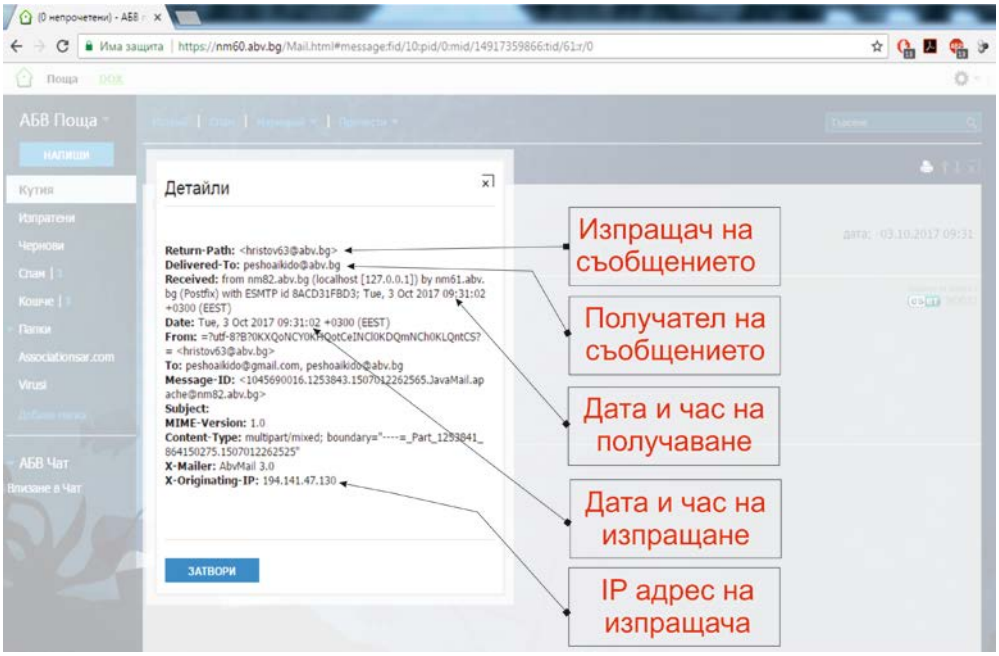


Фиг. 1. достъпът до следния уеб линк „shu.bg/tadmin/upload/storage/“ е забранен.

<u>Кибератаката за получаване на информационни отпечатъци чрез електронни съобщения</u> се използва главно от киберпрестъпниците за получаване на информация от заглавната част на електронните съобщения, проследяване на кореспонденции с електронни съобщения чрез специални софтуерни програми [32], [33]. На фиг. 3 е показан пример за получаване на информация от заглавната част на електронно съобщение [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [22], [23]. В практиката едни от най-използваните софтуерни инструменти за проследяване на електронни съобщения са MSGTAG, GetNotify, WhoReadMe, Pointofmail, Zendio, Read Notify и др.



Фиг. 2. Открити учебни материали, които не трябва да бъдат с отворен достъп



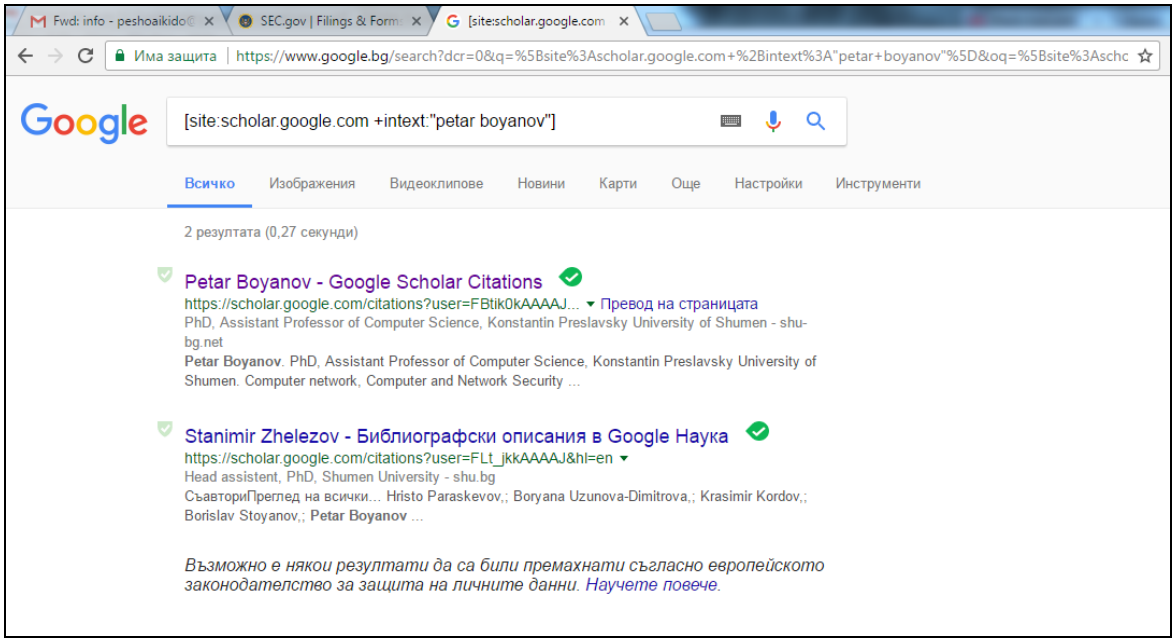
Фиг. 3. Информация от заглавната част на електронно съобщение.

<u>Кибератаката за получаване на информационни отпечатъци чрез конкурентно разузнаване</u> представлява процес на събиране и анализиране на информация за

определена организация жертва чрез използване на интернет пространството. Главната цел на тази атака е да се установи с какво се занимават другите организации и как те представят своите услуги и продукти. Източниците, които се използват да бъде извършвано конкурентното разузнаване, са патенти и търговски марки, месечни или годишни отчети, конференции, симпозиуми, конгреси, вестници, продуктови каталози, дистрибутори, агенти, доставчици [32], [33] уеб сайтове на компаниите, дигитални бази данни, търсещи машини и интернет [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17]. На фиг. 4 е показана една от най-известните бази данни - EDGAR, която е собственост на Американската Комисия по ценните книжа и борсите U.S. Securities and Exchange Commission (SEC). Тази база данни предоставя безплатна информация за дадената компания и по този начин злонамереният извършител може легално да получи това, от което има нужда за осъществяване на реалната кибератака [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [21], [25], [26], [27], [28], [29], [30].

Фиг. 4. База данни EDGAR на Американската комисия по ценните книжа

<u>Кибератаката за получаване на информационни отпечатъци чрез компанията Google</u> е насочена главно за откриване на уеб сайтове, които са изключително уязвими на многобройни експлойти. Извършването на тази атака се постига чрез използването на специални оператори със стрингове (знаци) и заявки, с които се намира точно конкретна информация за избраната жертва. На фиг. 5 е показано използването на само два оператора - "site:" и "intext". Ако примерно злонамереният извършител иска да намери информация за лицето "petar boyanov" в международната дигитална база данни за научни изследователи и преподаватели - Google Scholar, тогава за тази цел трябва да бъде изписано в търсещата машина Google следният текст: [site:scholar.google.com +intext:"petar boyanov"]. По този начин може да бъде търсена информация и за служители, работещи в определена организация или компания [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17].

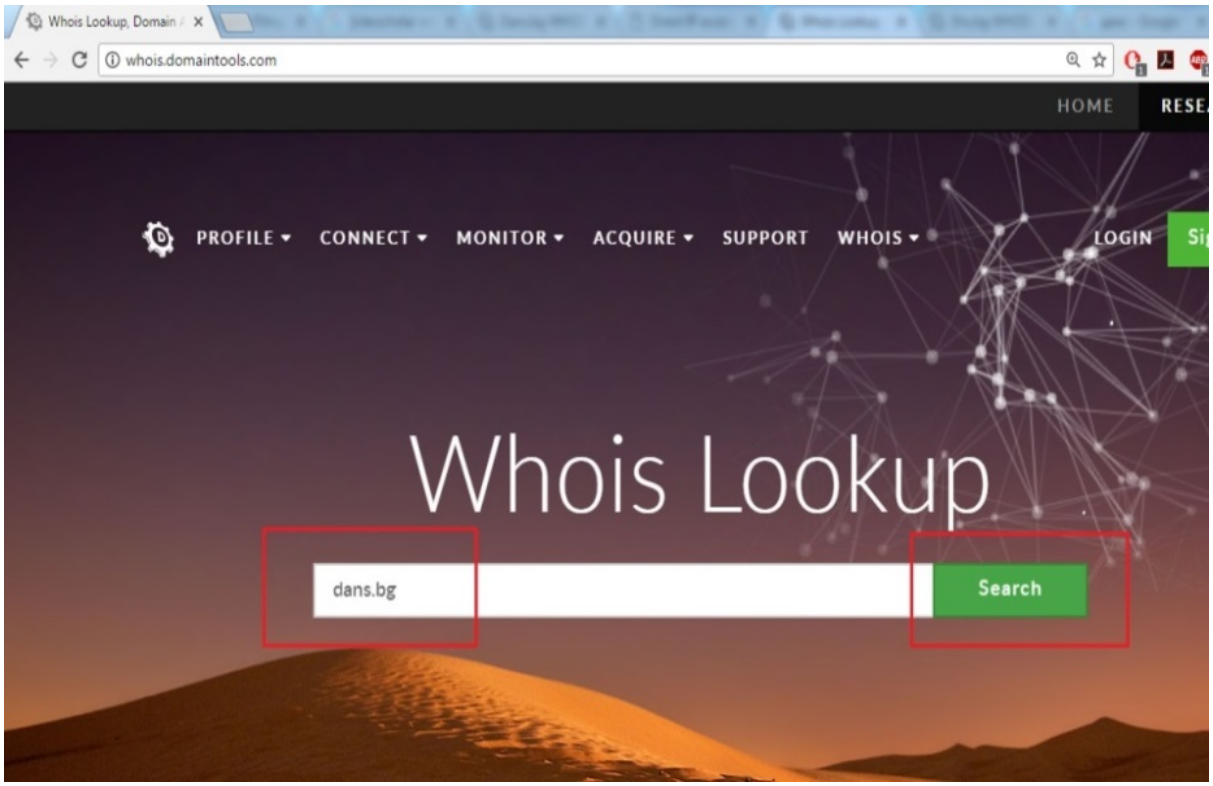


Фиг. 5. Търсене на информация само по два оператора

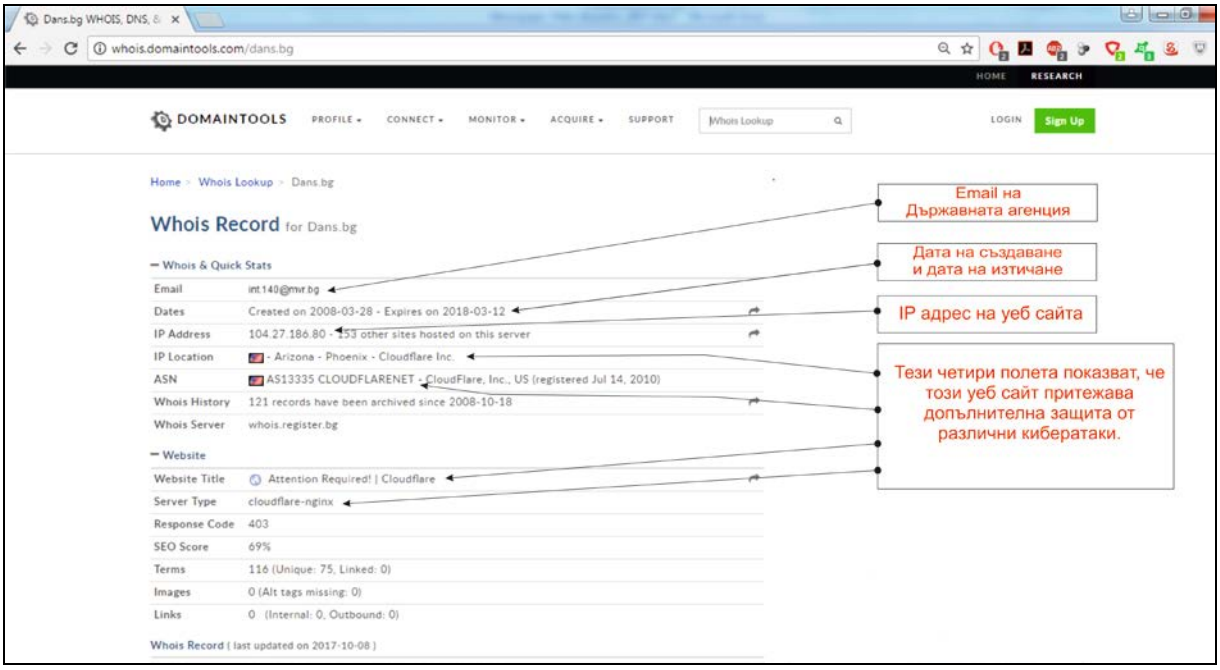
<u>Кибератаката за получаване на информационни отпечатъци чрез базите данни на Регионалните интернет регистри</u> представлява начин за получаване на важна информация за домейна на организацията чрез протокола WHOIS. Чрез този протокол атакуващият хост изпраща WHOIS заявка към LOOKUP таблицата на определен WHOIS сървър с името на уеб сайта и домейна на организацията [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [18], [21]. Един от най-известните WHOIS сървъри в целия свят е уеб адрес - http://whois.domaintools.com. Ако примерно злонамереният хост иска да получи повече информация за уеб сайта и домейна на Държавна агенция „Национална сигурност” в Република България - www.dans.bg, тогава е необходимо да се напише само "dans.bg" в полето „Whois Lookup”, като това е показано на фиг. 6.

Резултатът след написването на домейна е показан на фиг. 7 и фиг. 8. Информацията, която се предостави от базата данни на сървърите, е следната [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17]:

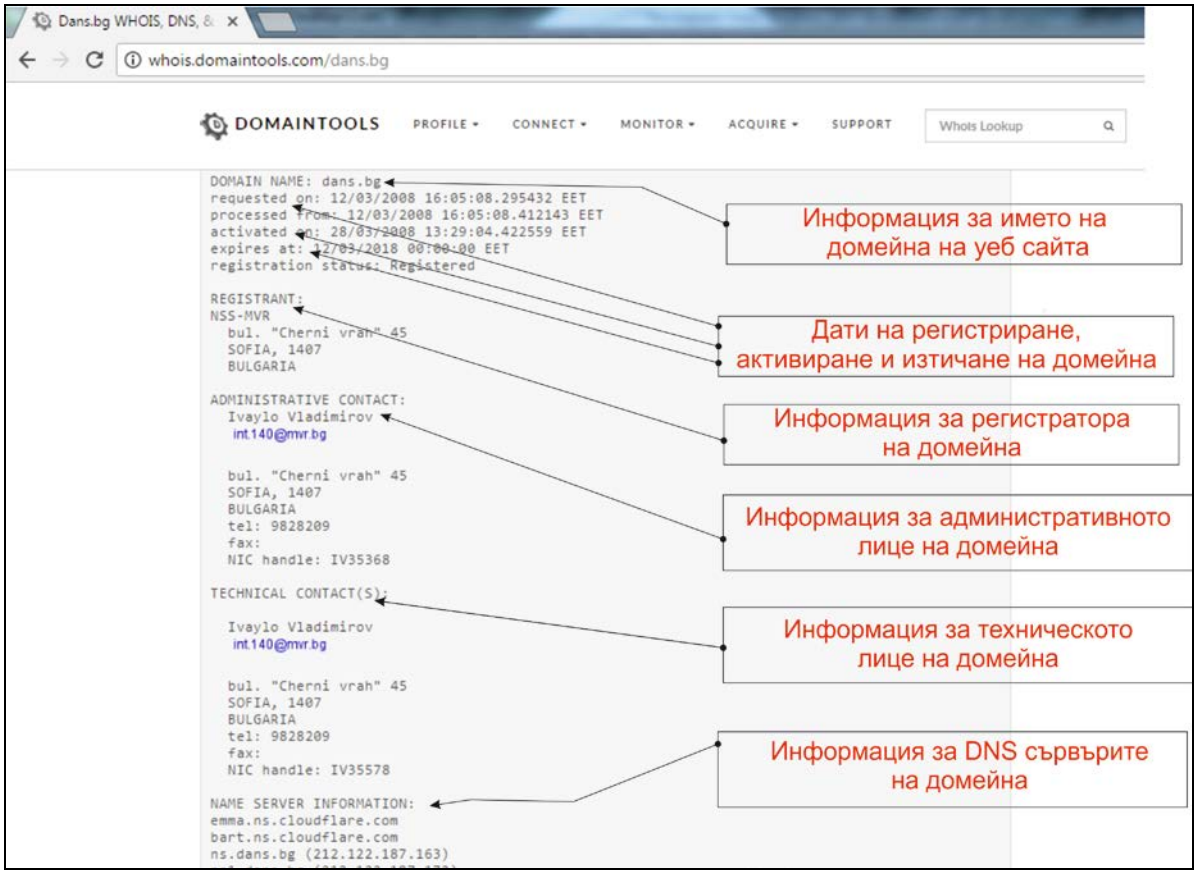
- Показано е името на домейна - dans.bg.
- Показани са датите на регистриране, активиране и изтичане на домейна.
- Показан е публичният IPv4 адрес за директен достъп до уеб сайт на dans.bg - 104.27.186.80.
- Установи се, че уеб сайтът dans.bg разполага със сериозна допълнителна защита от различни видове кибератаки. Уеб платформата, която е използвана за защита на сайта, е собственост на Американската компания Cloudflare, Inc.
- Показана е информация за името на регистратора на домейна - NSS-MVR, както и неговият адрес - bul. "Cherni vrah" 45, SOFIA, 1407, BULGARIA.
- Установи се, че административното лице за контакт е "Ivaylo Vladimirov" с email: int.140@mvr.bg.
- Установи се, че техническото лице за контакт е "Ivaylo Vladimirov" с email: int.140@mvr.bg и телефон: 9828209.
- Установи се, че DNS сървърите на домейна са emma.ns.cloudflare.com, bart.ns.cloudflare.com, ns.dans.bg (212.122.187.163) и ns1.dans.bg (212.122.187.172).



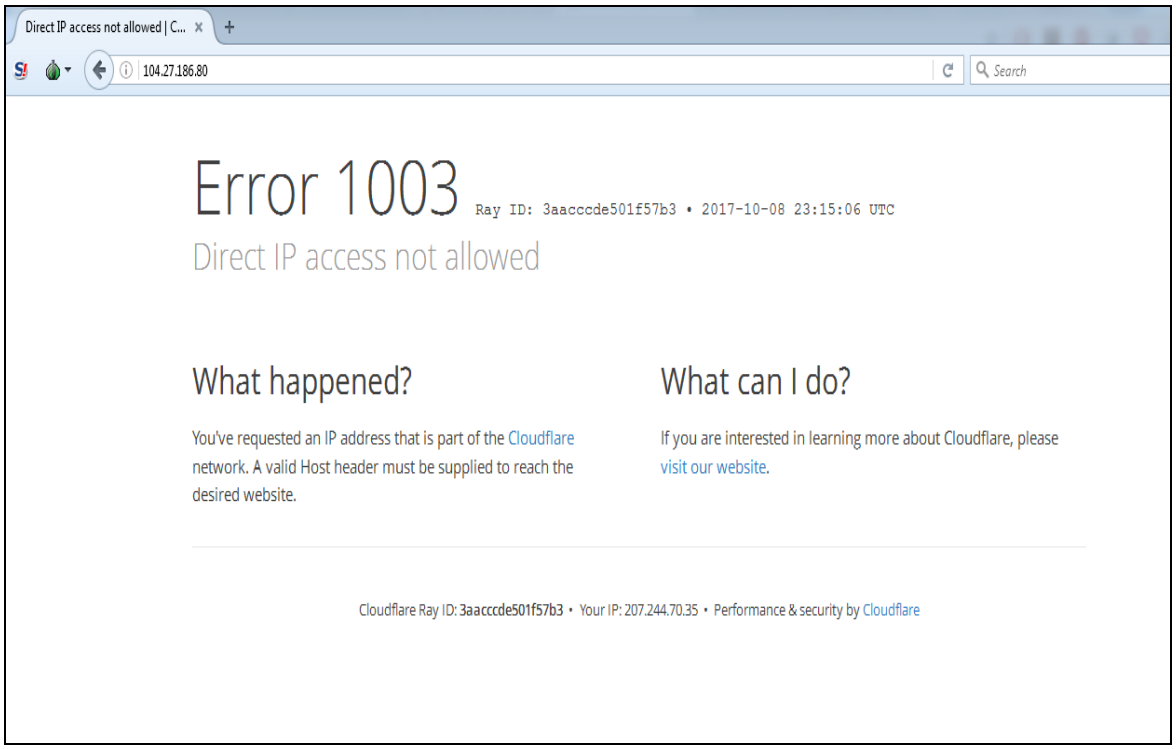
Фиг. 6. Правене на Whois заявка за домейна "dans.bg"



Фиг. 7. Показване на първата част от получения запис за домейна "dans.bg"



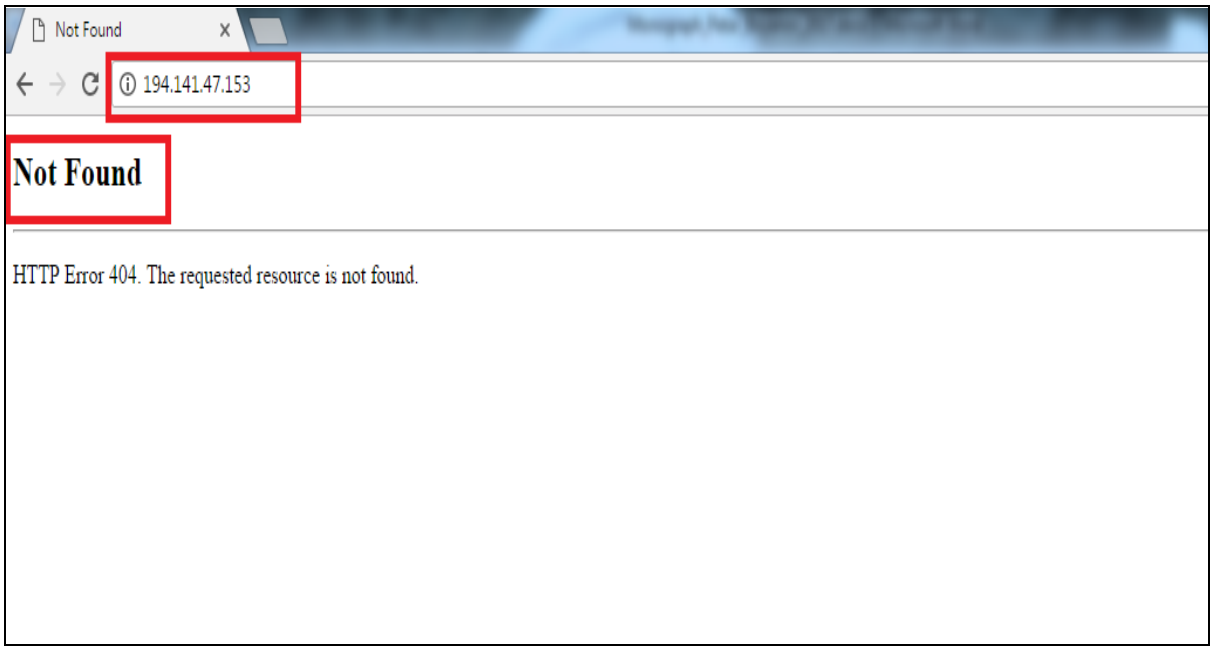
Фиг. 8. Показване на втората част от получения запис за домейна "dans.bg"



Фиг. 9. Директният достъп до уеб сайта "dans.bg" е забранен

От фиг. 9 се установи, че ако даден злонамерен извършител се опита да осъществи директен достъп на уеб сайта на Държавна агенция „Национална сигурност” в Република България, ще бъде спрян. Причината за това е, че публичният IPv4 адрес 104.27.186.80 на домейна е защитен да бъде директно достъпван. Най-отдолу е изписано, че идентифицирано събитие за достъп до домейна е "Cloudflare Ray ID: 3aacccde501f57b3", а IPv4 адресът на киберпрестъпника е "IP: 207.244.70.35". Трябва да се знае, че този адрес на престъпника може да не бъде неговият истински адрес, а всъщност да бъде фалшив!

На фиг. 10 е показано, че и директният достъп с публичния IP адрес на сайта на Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“ е също забранен. Публичният IPv4 адрес на уеб сайта на Факултета по технически науки е 194.141.47.153, името на уеб сайта е ftn.shu.bg [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [21]. При този случай е използвана ръчна настройка за защита от специалната конфигурация от менюта на уеб сървъра, в който се хоства този уеб сайт. Докато на фиг. 9 се използва цяла специална уеб платформа, която играе ролята на защитен филтър от различни уеб посегателства [1], [2], [3], [4], [5], [8], [9], [10], [11], [14], [15], [17], [32], [33].



Фиг. 10. Забранен директен достъп на публичния IP адрес на уеб сайта ftn.shu.bg

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да предприемат и направят следните защитни действия като:

- Задължително принуждаване и задължаване на потребителите (служителите) на АИС/М да не разгласят конфиденциална информация на трети лица. Това може да се осъществи чрез подписване на специални вътрешни протоколи, с което да се гарантира, че няма да изнесат никаква информация на киберпрестъпници или организации конкуренти.
- Затваряне или блокиране на всички ненужни мрежови портове в компютърните машини на служителите чрез хибридна изградена защитна стена.
- Задължително преглеждане каква информация ще бъде качена на официалния уеб сайт.
- Задължително ограничаване или блокиране на достъпа на търсещите машини от кеширане на уеб страницата на организацията или компанията.
- Конфигуриране на специални настройки в маршрутизаторите и комутаторите, че да могат да отхвърлят всякакви разузнавателни мрежови пакети и заявки.

ЛИТЕРАТУРА:

[1] Ташева, Ж., Боянов П., Сравнителен анализ на злонамерени уеб-базирани атаки, Научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при Националният военен университет „Васил Левски”, гр. Шумен, България, ISBN 978-954-9681-49-9, 6 - 7 Юни 2013, с. 178-183.

[2] Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol.3, 2013, pp. 114-124.

[3] Allen, L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing, Birmingham, UK, May 2012, ISBN 978-1-84951-774-4, pp. 414

[4] Bodmer, S., Kilger, M., Carpenter, Gr., Jones, J., Reverse Deception: Organized Cyber Threat Counter-Exploitation, McGraw-Hill Education, 2012, ISBN: 978-0-07-177250-1, pp. 465.

[5] Gorodetski, V., Kotenko, I., Attacks against computer network: formal grammar-based framework and simulation tool, Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, ISBN: 978-3-540-00020-4, pp. 219-238.

[6] Gragido, W., Pirc, J., Cybercrime and espionage: An analysis of subversive multi-vector threats, Syngress, 2011, ISBN: 978-1-59749-613-1, pp. 270.

[7] Grubb, L. S., Cuéllar, L., Survey of network weapons part 1: weapons for profiling, Journal of Computing Sciences in Colleges, vol.19, issue 4, 2004, ISSN: 1937-4771, pp. 314-320.

[8] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[9] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3, 2014, pp. 104-111.

[10] Hristov, Hr., A modern survey on problems of business organization’s security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[11] Hristov, Hr., Civil Control under security sector, Annual of Konstantin Preslavsky University of Shumen, Shumen, 2016, Vol. VI E, Faculty of Technical Sciences, ISSN 1311-834X, pp.161-173.

[12] Kahya-Özyirmidokuz, E., Gezer, A., Ciflikli, C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, ISBN: 978-1-61208-242-4, pp.18 – 23.

[13] Kaur, R., Singh, G. Analysing, Port Scanning Tools and Security Techniques, International Journal of Electrical Electronics & Computer Science Engineering, Volume 1, Issue 5, October 2014, ISSN : 2348 2273, pp. 58 – 64.

[14] Meyers, C., Powers, S., Faissol, D., Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 22.

[15] Meyers C., Powers S., Faissol D., Probabilistic Characterization of Adversary Behavior in Cyber Security, No. LLNL-TR-419023, Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 52.

[16] Shimeall, T. J., Spring, J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[17] Simmons, C., Shiva, S., Dasgupta, D., Wu, Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA ’14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[18] Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., Educational simulation the local area network of academic departments with securely configured FTP server, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.

[19] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[20] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference “Technics. Techologies. Education. Safety ’18”, Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[21] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[22] Fetfov O., Tonev V. Bedzhev B. “Information Encryption with Combination Generator”, CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[23] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[24] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[25] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.

[26] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[27] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[28] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[29] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[30] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[31] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security" № 1(3)-2013 УДК 004 (056.5+413.5).

[32] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[33] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност", ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

Име на автора: доц. д-р инж. Петър Красенов Боянов
Месторабота: Шуменски университет „Епископ Константин Преславски", Факултет по технически науки, Катедра „Управление на системите за сигурност"
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com, petar.boyanov@shu.bg
Име на съавтора: доц. д-р инж. Христо Атанасов Христов
Месторабота: Шуменски университет „Епископ Константин Преславски", Факултет по технически науки, Началник на катедра „Управление на системите за сигурност"
E-mail: h.a.hristov@shu.bg, hristov63@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 34 - 41 Problems of Security Systems

IMPLEMENTATION OF INFORMATION SYSTEM CYBER ATTACKS AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS

PETAR KR. BOYANOV, HRISTO A. HRISTOV

ABSTRACT: *In this paper implementation of information system cyber-attacks against the government agencies, private organizations and academic institutions is made.*

KEYWORDS: *Footprinting, Government agencies, Information Security, Modern cyber-attacks, Reconnaissance, Software vulnerability, System, Threat.*

ПРИЛОЖЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМНИ КИБЕРАТАКИ СРЕЩУ ПРАВИТЕЛСТВЕНИ АГЕНЦИИ, ЧАСТНИ ОРГАНИЗАЦИИ И АКАДЕМИЧНИ ИНСТИТУЦИИ*

ПЕТЪР КР. БОЯНОВ, ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *В тази статия са извършени научни експерименти и изследвания относно начините на приложение на информационните системни кибератаки срещу правителствени агенции, частни организации и академични институции.*

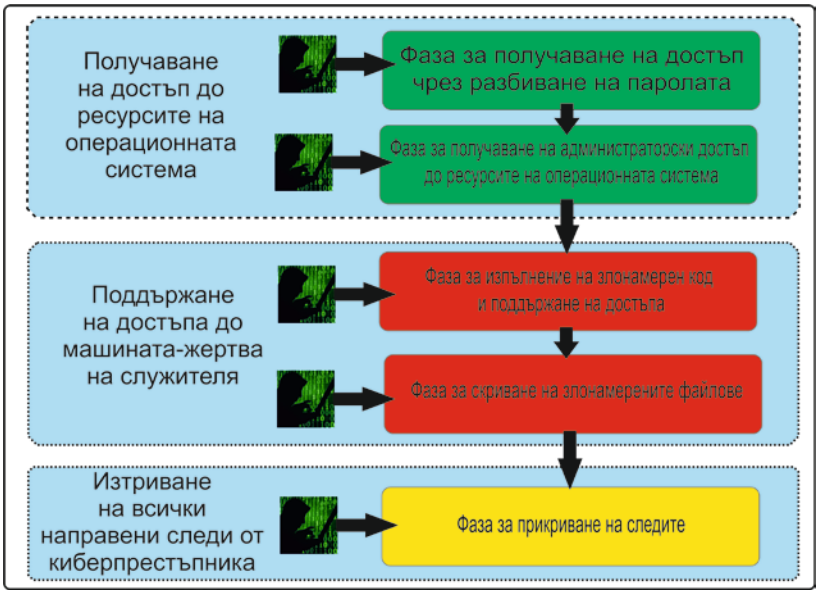
1. Въведение

В тази статия информационните системни кибератаки представляват съвкупност от специални злонамерени софтуерни програми, които се използват за осигуряване на неоторизиран достъп до ресурсите на машината жертва на служителя от държавната или частната организация [1], [2], [3], [5], [6], [8].

Успешното извършване на определена кибератака към машината жертва на служителя от дадена организация е свързано с изпълнението на основните фази на кибератаките [32], [33]. Фазите на извършване на кибератака са:

- Разузнавателна фаза;
- Сканираща фаза;
- Фаза за получаване на достъп чрез разбиване на паролата;
- Фаза за получаване на администраторски достъп до ресурсите на операционната система;
- Фаза за изпълнение на злонамерен код и поддържане на достъпа;
- Фаза за скриване на злонамерените файлове;
- Фаза за прикриване на следите. Всичко това е показано на фиг. 1.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

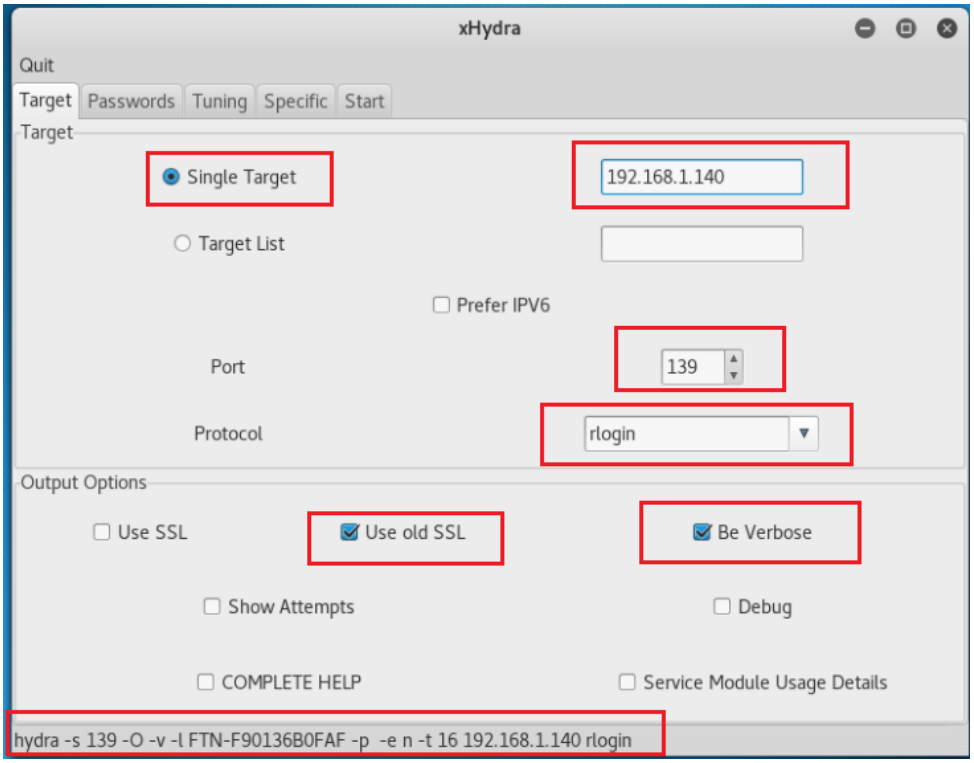


Фиг. 1. Фазите на извършване на кибератака

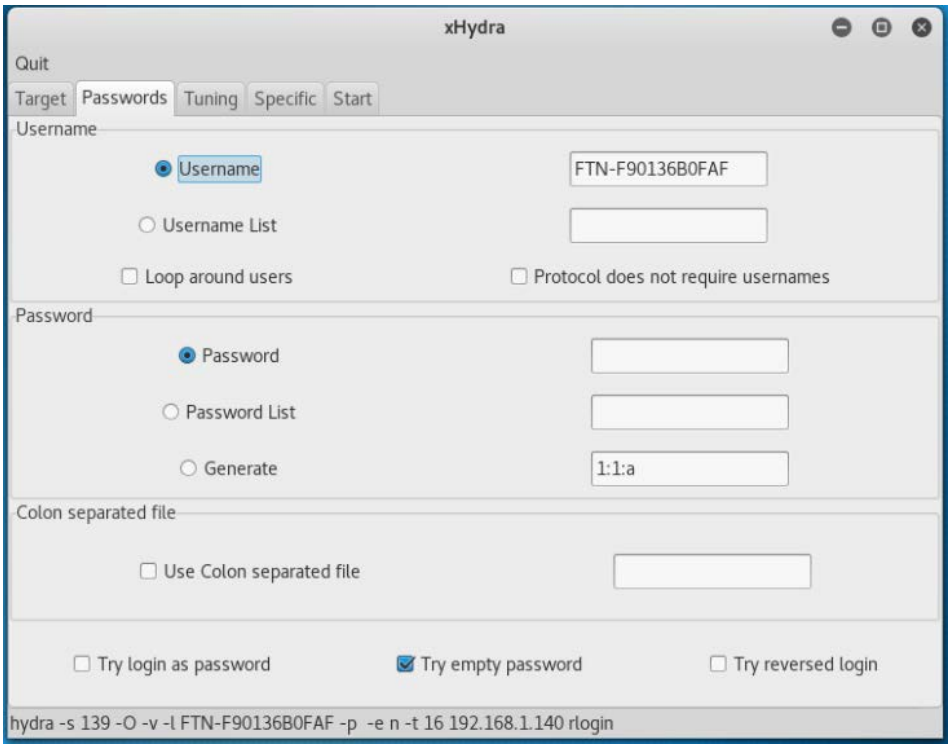
2. Изложение

Кибератаки за разбиване на пароли. Те от своя страна се разделят на няколко вида като [1], [2], [3], [4], [7], [9], [11], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31]:

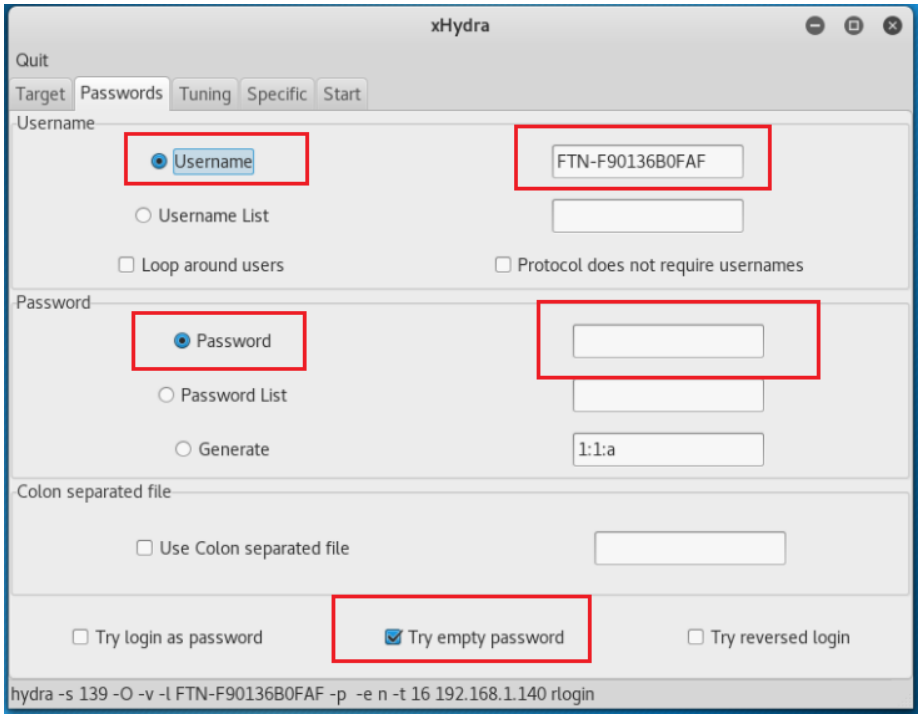
- Кибератаки, използващи файлове от речници на различни езици. За тези атаки е характерно, че киберпрестъпникът прави няколко файла от речници на различни говорими езици с цел по-ефективното разбиване на паролата.
- Кибератаки, използващи груба сила за отгатване на паролата. За тези атаки е характерно, че киберпрестъпникът прави файл, съдържащ всякакви възможни комбинации от думи, цифри и символи.
- Сричкови кибератаки за отгатване на паролата. При тях злонамереният извършител използва различни срички, записани в файл.
- Кибератаки, използващи пароли по подразбиране. Пример за пароли по подразбиране са потребителското име да бъде "admin" и паролата също да бъде "admin".
- Кибератаки с ръчно отгатване на паролата. При тези атаки извършителят на случаен принцип се опитва да отгатне паролата на своята жертва. Но трябва да се знае, че преди това киберизвършителят е получил по някакъв начин повече информация за използваната парола на своята жертва.
- Хибридни кибератаки. Те са съвкупност от всички споменати по-горе атаки.



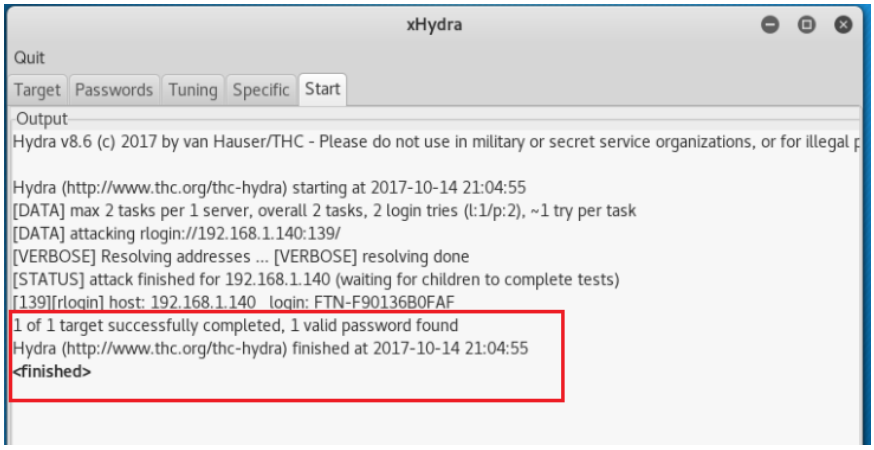
Фиг. 2. Настройка на конфигурационните параметри на програмата xHydra в Linux базирана операционна система



Фиг. 3. Настройка на конфигурационните параметри на програмата xHydra в Linux базирана операционна система



Фиг. 4. Настройка на конфигурационните параметри на програмата xHydra в Linux базирана операционна система



Фиг. 5. Получени резултати от програмата

Софтуерната програма за разбиване на пароли, която е използвана, е xHydra v8.6 © 2017 by van Hause/THC. Конфигурационните параметри на програмата са съответно [1], [2], [10], [11], [12], [18], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]:

- Избор за единична жертва с IP адрес - 192.168.1.140.
- Мрежов порт за достъп - 139.
- Протокол за достъп - rlogin.
- Избор за детайлно описание на резултатите.
- Избор за използване на стария стил на SSL протокола.
- Избрано потребителско име - FTN-F90136B0FAF. Това потребителско име е получено чрез сканиращи мрежови кибератаки.
- Не е сложена парола за достъп и може да се правят опити с празна парола.

- Цялата команда, която може да бъде написана, е "hydra -s 139 -O -v -l FTN-F90136B0FAF -p -e n -t 16 192.168.1.140 rlogin"
- Получени резултати с успешно разкриване на паролата на машината жертва.

От фиг. 5 се установи, че е успешно разкрита паролата на машината жертва и по този начин киберпрестъпникът ще бъде в състояние да получи достъп до компютърната машина. Кибератаки, използващи шпионски програми от тип "Rootkit". Руткитът "Rootkit" представлява програма, която се използва за [16] придобиване на администраторски права за Windows базирани операционни системи или супер потребителски права за Linux базирани операционни системи [17], без да бъдат забелязани и открити от антивирусните програми. Тези злонамерени програми се закачват или обвиват в специални софтуерни пакети за компютърни игри. След като киберпрестъпникът инсталира тези злонамерени програми, тогава той ще може да управлява всички ресурси на операционната система чрез отдалечен достъп с агент тип "задна врата" [18], да изтрива всички свои направени следи, да компрометира и замаскира злонамерените процеси като нормални системни процеси от операционната система, да събира и анализира конфиденциална информация, използвана от служителя от организацията. Тези кибератаки се разделят на [11], [12], [13], [14], [15]:

- кибератаки, използващи твърдо кодиран код в хардуера;
- кибератаки, използващи ядрото на операционната система;
- кибератаки, използващи приложни софтуерни програми.
- кибератаки, използващи инициализиращата програма (Boot Loader) за зареждане на операционната система.

Кибератаки, използващи шпионски програми от тип "Spyware". Злонамерените извършители [20], [106] използват уязвимости в уеб браузерите като Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari и др. с цел инсталирането на агент, който да следи всички дейности на машината жертва на служителя от организацията. След инсталирането на специалните злонамерени софтуерни агенти без знанието на служителя от организацията, всички записани данни се предават през интернет до машината на киберпрестъпника. Тези кибератаки се разделят на [1], [2], [3], [6], [11], [13], [15], [16], [17], [18], [32], [33]:

- мултимедийни кибератаки на звук и видео;
- кибератаки на работния плот на операционната система;
- кибератаки, използващи глобалната система за позициониране GPS;
- кибератаки, използващи буфера на принтера;
- кибератаки, използващи буфера на факса;
- кибератаки, използващи флаш памети;
- кибератаки, използващи клавиша за заснемане на текущото състояние на прозореца;
- кибератаки, използващи уязвимости в съвременните смарт телефони.

Спайуерът (Spyware) представлява компютърна софтуерна наблюдаваща програма, която се инсталира като скрит допълнителен компонент наред с безплатна или платена програма, която е изтеглена от интернет. Тъй като повечето програми изискват администраторски права за инсталация, тогава скритото инсталиране на такъв шпиониращ софтуер остава незабелязано от служителя във фирмата или организацията. След това откриване на този шпиониращ софтуер е почти невъзможно, защото злонамереният

софтуер се маскира под определен системен процес като svchost.exe в операционна система Microsoft Windows.

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи АИС/М, както и администраторът по сигурността трябва да предприемат и направят следните защитни действия като:

- Създаване на много пароли трудно за отгатване с дължина до 30 или 40 символа.
- Задължително условие при създаването на трудна парола е тя да съдържа малки и големи букви, цифри, специални символи като “$,*(#!@_-“ и др.
- Никога да не се допуска софтуерна програма да управлява паролите на служителя.
- Да не се използват пароли като дата на раждане, име на животното, име на приятел, име на близък, име на дете, номерът на колата, марката телефон и др.
- Постоянно наблюдение и следене на логовете с цел откриване на опити за кибератака от тип груба сила (brute force) срещу паролите на служителя.
- Автоматично да се блокира достъпът до компютърната машина на служителя, в случай че са направени повече от три погрешни опита за достъп.
- Служителят да не притежава администраторски права върху своята операционна система, а само потребителски.
- Редовно проверяване за обновления и актуализации на антивирусните програми и системни кръпки (patches) за операционната системи.
- Криптиране на най-конфиденциалната информация.
- Записване на външен носител на всичката информация в случай на срив на компютърната машина.
- Постоянно видеонаблюдение на персонала и служителите, докато работят на техните компютърни машини.

ЛИТЕРАТУРА:

[1] Ташева, Ж., Боянов П., Сравнителен анализ на злонамерени уеб-базирани атаки, Научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при Националният военен университет „Васил Левски”, гр. Шумен, България, ISBN 978-954-9681-49-9, 6 - 7 Юни 2013, с. 178-183.

[2] Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124.

[3] Allen, L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing, Birmingham, UK, May 2012, ISBN 978-1-84951-774-4, pp. 414.

[4] Bodmer, S., Kilger, M., Carpenter, Gr., Jones, J., Reverse Deception: Organized Cyber Threat Counter-Exploitation, McGraw-Hill Education, 2012, ISBN: 978-0-07-177250-1, pp. 465.

[5] Gorodetski, V., Kotenko, I., Attacks against computer network: formal grammar-based framework and simulation tool, Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, ISBN: 978-3-540-00020-4, pp. 219-238.

[6] Gragido, W., Pirc, J., Cybercrime and espionage: An analysis of subversive multi-vector threats, Syngress, 2011, ISBN: 978-1-59749-613-1, pp. 270.

[7] Grubb, L. S., Cuéllar, L., Survey of network weapons part 1: weapons for profiling, Journal of Computing Sciences in Colleges, vol.19, issue 4, 2004, ISSN: 1937-4771, pp. 314-320.

[8] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[9] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[10] Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[11] Hristov, Hr., Civil Control under security sector, Annual of Konstantin Preslavsky University of Shumen, Shumen, 2016, Vol. VI E, Faculty of Technical Sciences, ISSN 1311-834X, pp.161-173.

[12] Kahya-Özyirmidokuz, E., Gezer, A., Ciflikli, C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, ISBN: 978-1-61208-242-4, pp.18 – 23.

[13] Kaur, R., Singh, G. Analysing, Port Scanning Tools and Security Techniques, International Journal of Electrical Electronics & Computer Science Engineering, Volume 1, Issue 5, October 2014, ISSN : 2348 2273, pp. 58 – 64.

[14] Meyers, C., Powers, S., Faissol, D., Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 22.

[15] Meyers C., Powers S., Faissol D., Probabilistic Characterization of Adversary Behavior in Cyber Security, No. LLNL-TR-419023, Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 52.

[16] Shimeall, T. J., Spring, J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[17] Simmons, C., Shiva, S., Dasgupta, D., Wu, Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[18] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[19] Fetfov O., Tonev V. Bedzhev B. "Information Encryption with Combination Generator", CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[20] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA", Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски", 2015г.

[21] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[22] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference “Technics. Techologies. Education. Safety ’18”, Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[23] Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., Educational simulation the local area network of academic departments with securely configured FTP server, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.

[24] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[25] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.

[26] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[27] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[28] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[29] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[30] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[31] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal with Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[32] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[33] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност”, ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

Име на автора: доц. д-р инж. Петър Красенов Боянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com, petar.boyanov@shu.bg
Име на съавтора: доц. д-р инж. Христо Атанасов Христов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, началник на катедра „Управление на системите за сигурност“
E-mail: h.a.hristov@shu.bg, hristov63@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 42 - 51 Problems of Security Systems

IMPLEMENTATION OF SOCIAL ENGINEERING CYBER ATTACK AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS

PETAR KR. BOYANOV

ABSTRACT: *In this paper implementation of social engineering cyber-attack against the government agencies, private organizations and academic institutions is made.*

KEYWORDS: *Footprinting, Government agencies, Information Security, Modern cyber-attacks, Social engineering, Vulnerability, Threat.*

ПРИЛОЖЕНИЕ НА КИБЕРАТАКАТА ОТ ТИП СОЦИАЛНО ИНЖЕНЕРСТВО СРЕЩУ ПРАВИТЕЛСТВЕНИ АГЕНЦИИ, ЧАСТНИ ОРГАНИЗАЦИИ И АКАДЕМИЧНИ ИНСТИТУЦИИ*

ПЕТЪР КР. БОЯНОВ

АБСТРАКТ: *В тази статия са извършени научни експерименти и изследвания относно начините на приложение на кибератаката тип социално инженерство срещу правителствени агенции, частни организации и академични институции.*

1. Въведение

Тези кибератаки причиняват най-огромни щети на фирми, компании, организации и физически лица чрез несанкционирано проникване в ресурсите на компютърните и мрежови системи [1], [2] независимо от изградените защитни стени, системи за откриване на проникване IDS, системи за предотвратяване на прониквания IPS, виртуални локални компютърни мрежи и виртуални публични мрежи [10], [23], [24]. Типовете атаки на социално инженерство са:

- **Човешко базирани атаки.** При тях злонамереният извършител може да се представи като легитимен краен потребител [11], много важен потребител или като лице от центъра за техническата поддръжка [12]. И при трите вида замаскираният злонамерен извършител цели да получи достъп до конфиденциална информация за компанията, фирмата или организацията [5], [6], [7]. Трябва да се знае, че към този подвид атаки спадат още техниките, при които киберизвършителите следят и наблюдават всичко зад гърба на своята жертва. По този начин киберпрестъпник може да получи желаната информация само с леко шпиониране и заглеждане зад гърба или рамото на служител в организацията. Още по-опасно е, когато стои зад гърба на системния администратор, който е отговорен за цялата информационна сигурност на организацията. Също така злонамереният извършител може да използва специални разузнавателни средства (СРС) [25] за аудио и видеоразговори в реално време. Друг начин, по който киберпрестъпникът може да получи информация за своята жертва, е претърсването на кофите с боклуци с цел намиране на писма,

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

важни документи, скици, написани пароли и потребителски имена, проекти, планове и др. [23], [24], [25]. Преобличането и представянето на киберпрестъпника за легитимен представител на голяма организация също може да му помогне да получи информация за своите избрани жертви като крайната цел в повечето случаи е финансови измами и искане подкупи в големи суми от пари [1], [2], [3], [4], [5], [6], [7], [15], [16], [17], [18], [19], [20], [21], [22].

- **Компютърно базирани атаки.** Те се характеризират с факта, че се използват различни зловредни програми и софтуерни приложения [8], [9] като заразени писма, изпратени по електронната поща, използване на компютърни вируси, троянски коне и др. Типовете компютърно базирани атаки са [1], [2], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]:
    - Изпращане на фалшиви съобщения по електронна поща [1].
    - Изкачащи прозорци. При тези атаки се използват изкачащи прозорци, които алармират, че обикновеният потребител се е разкачил от компютърната мрежа [1] и е необходимо наново да си въведе потребителското име и парола [5]. Най-често се използва електронно писмо с хипер връзка, която пренасочва към фалшива уеб страница, изискваща въвеждането на лична информация или изтегляне на злонамерена програма като троянски кон или шпионска програма, следяща натискането на всеки клавиш от клавиатурата.
- **Мобилно базирани кибератаки**. Те се разделят на:
    - Публикуване на зловредни приложения. При тези атаки киберпрестъпниците създават зловредни приложения с атрактивни конфигурации, подобни на истинските доверени приложения в голям онлайн магазин за продажба на приложения. След това непредпазливите обикновени потребители свалят тези приложения и след това биват заразени от зловреден софтуер, който изпраща цялата им лична информация към компютърната машина на киберпрестъпника [23], [24], [25].
    - Изпращане на фалшиви кратки съобщения по мобилните телефони.

2. Изложение

Кибератаката от тип социално инженерство е една от най-силните и почти винаги успешно завършени от киберпрестъпниците. Те са характеризират със следните особености [1], [2], [4], [5], [6], [7], [10], [11], [12], [14], [15], [16], [17], [18], [19]:

- В повечето случаи хората са най-податливи на различни внушения и влияния и по този начин киберпрестъпникът може да се възползва от този факт и получи желаната от него информация.
- В компютърната практика почти е невъзможно да се засекат или открият опити за социално инженерство.
- Факт е, че за момента не са намерени ефективни или почти никакви методи и начини, с които да се осигури пълна защита от социално инженерство.
- В практиката не съществуват нито хардуерни, нито софтуерни защити срещу кибератаката от тип социално инженерство.

Фазите, през които трябва да се премине, за да бъде ефективна и успешна кибератака от тип социално инженерство, са:

- Намиране на начин да се посети организацията жертва. Също така е възможно да се отиде до казаните с боклуци до организацията с цел претърсване и намиране на записани пароли и потребителски имена на служители.
- Откриване на недоволни или обидени служители от организацията жертва.
- Сприятеляване с определени служители от организацията с цел получаване на по-конфиденциална информация като финансови справки и банкови сметки, телефонни номера, електронни пощи, профили в социалните мрежи, бъдещи планове и проекти на организацията, текущи и бъдещи продукти и услуги и др. [23], [24].

След като получи тази важна информация киберпрестъпникът, тогава последиците за организацията могат да бъдат следните [1], [5], [6], [10], [12], [13], [24]:

- Загуба на поверителност между сътрудници и служители.
- Предпоставки за опасност от терористични актове.
- Водене на досъдебни производства между служители в организацията.
- Възможно е дори да се стигне до затваряне на компанията или организацията.
- Претърпяване на сериозни финансови загуби.

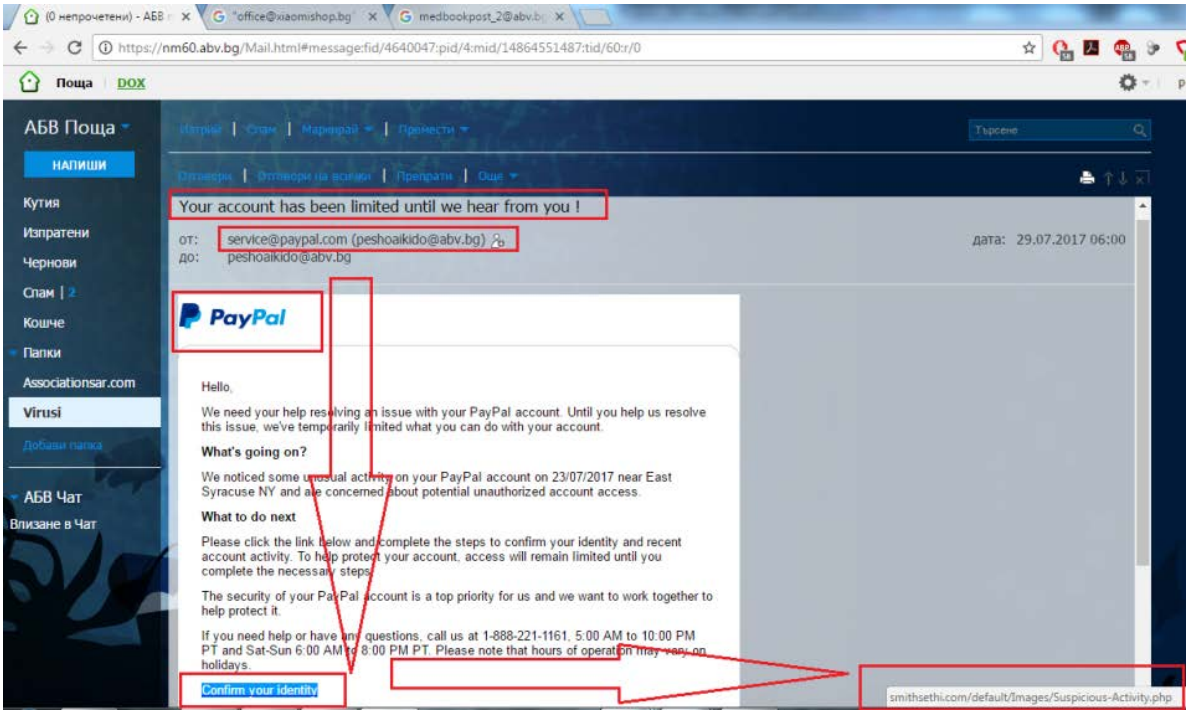
Основните жертви на кибератаката от тип социално инженерство са:

- Системни администратори.
- Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М).
- Служителите по развитие и експлоатация на АИС/М.
- Потребителите на АИС/М като обслужващ персонал в call център, рецепционисти, домакини на организацията.
- Технически мениджъри по информационни проблеми в дадена организация или фирма.
- Обикновени потребители или клиенти на компанията, фирмата и организацията.
- Представители на големи и малки компании за софтуерни и хардуерни продукти и услуги.

На фиг. 1 е представена една от най-разпространените и в повечето случаи успешно завършващи кибератаки, а именно "фишинг". Целта на тази кибератака е да подлъже и измами служителите в дадена организация с цел да си дадат своите потребителски имена и пароли за онлайн банкиране (https://online.rbb.bg/page/default.aspx?user_id=&session_id=&xml_id=/bg-BG/.login), онлайн търговия (https://www.emag.bg/), уеб системи за онлайн плащания на сметки като (https://www.epay.bg/v3main/front) и др. Цялата кибератака стартира с електронно съобщение, което изглежда като абсолютно официално и легитимно съобщение от система за онлайн банкиране като https://www.paypal.com/bg/home. След това ако даденият служител кликне върху уеб връзката, посочена по-долу във фалшивото писмо, тогава той бива пренасочен към фалшива уеб страница, която представлява точно копие на истинската уеб страница на системата за онлайн банкиране. Ако служителят се подмами на тази фалшификация, е принуден да си въведи парола, потребителско име, номер на

кредитната карта, датата на изтичане на кредитната карта, три цифри за сигурност отзад на кредитната карта. След това всичката тази информация попада в ръцете на опитния киберпрестъпник и той от своя страна източва банковата сметка на служителя съвсем спокойно и необезпокоявано. Трябва да се знае, че той използва специални прокси сървъри за извършване на тези парични онлайн транзакции с цел скриване на неговия реален IPv4 или IPv6 адреси. Това означава, че киберпрестъпникът може да се намира реално в град Полски Тръмбеш в Република България, но в същото време да се фалшифицира с друго местоположение като например в град Àйндховен в Кралство Нидерландия. След това процесът на издирване на престъпника става много сложен или може би почти невъзможен [1], [3], [7], [9], [11], [12], [13], [16], [17], [18], [19].

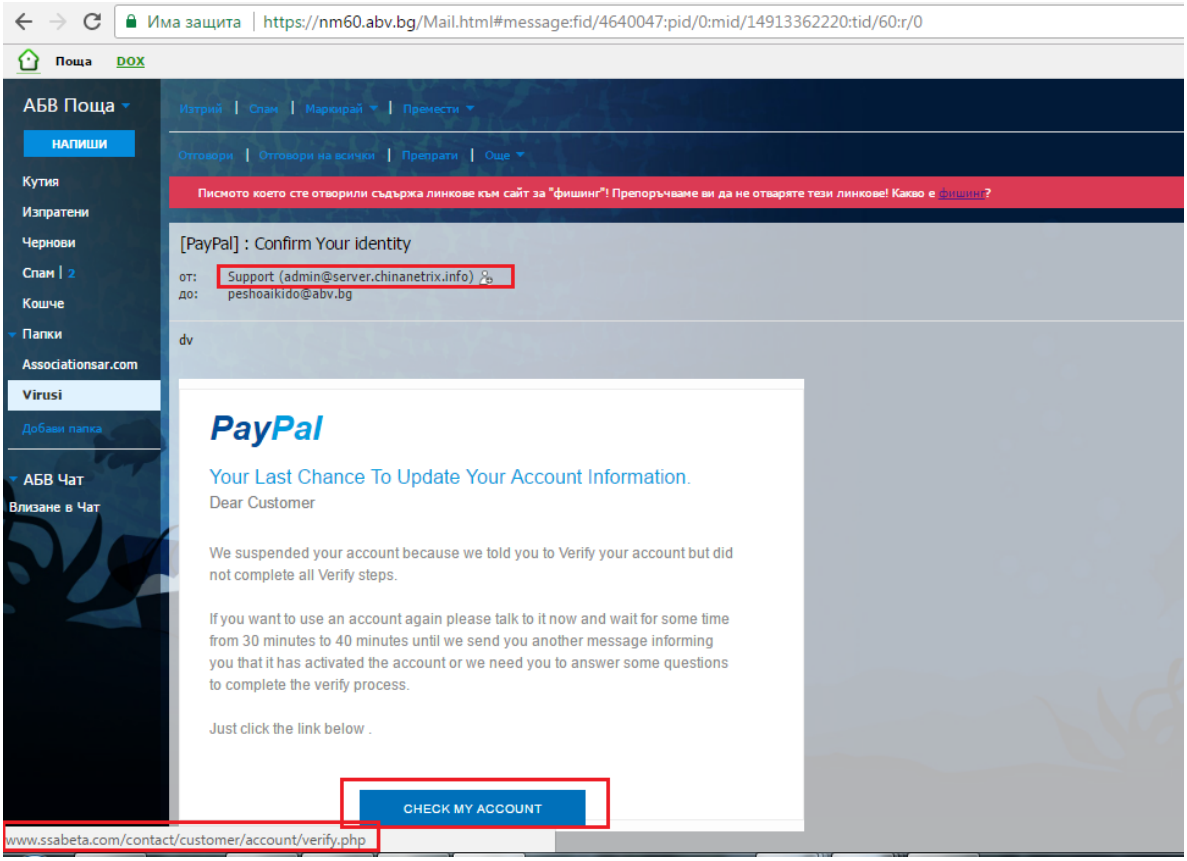
На фиг. 1 е представена реална компютърно-базирана кибератака от тип социално инженерство, при която е изпратено фалшиво електронно съобщение до източник "peshoaikido@abv.bg" и с подател "service@paypal.com (peshoaikido@abv.bg)" и с име на темата на писмото "Your account has been limited until we hear from you !". Ако се мине с курсора на мишката върху бутон-текста "Confirm your identity", тогава долу вдясно се появява уеб адресът на връзката за достъп - "http://smithsethi.com/default/Images/Suspicious-Activity.php". Ако беше истинско писмото, трябваше задължително името на домейна от източника да съвпада с уеб адреса на уеб страницата. В този случай това е истинска фалшификация и измама!!!



Фиг. 1. Фалшификация с електронни съобщения

На фиг. 2 е представена друга реална компютърно-базирана кибератака от тип социално инженерство, при която е изпратено фалшиво електронно съобщение до източник "peshoaikido@abv.bg" и с подател "Support (admin@server.chinanetrix.info)" и с име на темата на писмото "[PayPal] : Confirm Your identity". Ако се мине с курсора на мишката върху бутон-текста "CHECK MY ACCOUNT", тогава долу вдясно се появява уеб адресът на връзката за достъп - "http://www.ssabeta.com/contact/customer/account/verify.php". Ако беше истинско писмото,

трябваше задължително името на домейна от източника да съвпада с уеб адреса на уеб страницата. В този случай това е истинска фалшификация и измама!!!

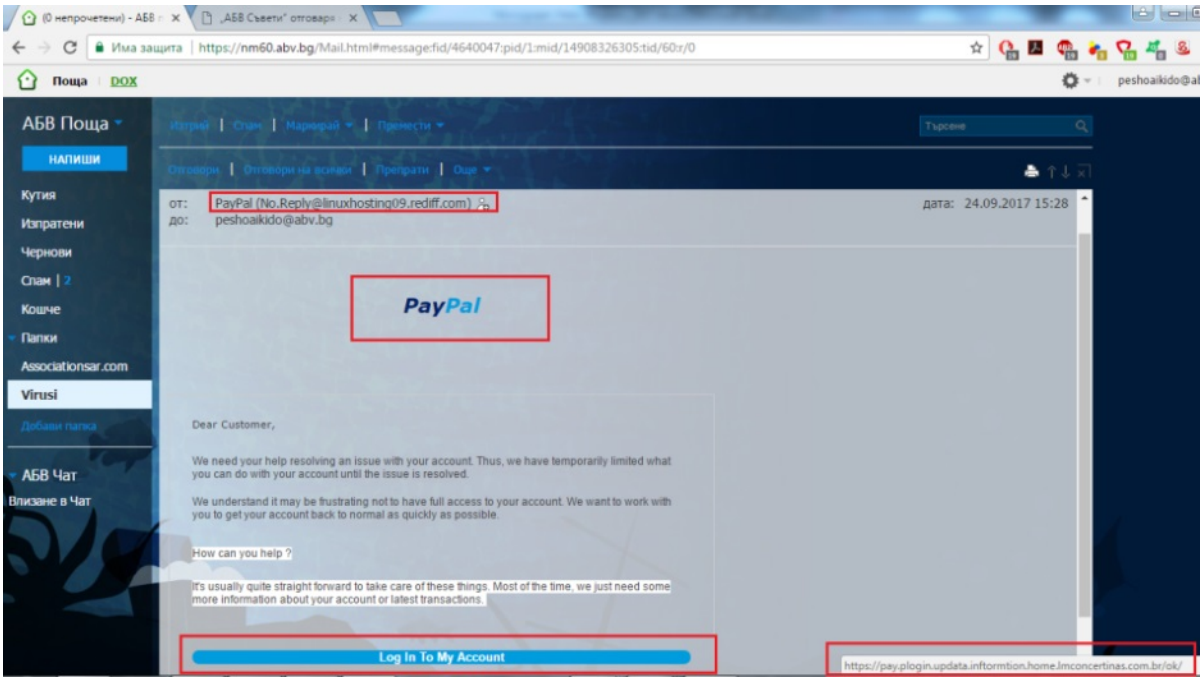


Фиг. 2. Фалшификация с електронни съобщения

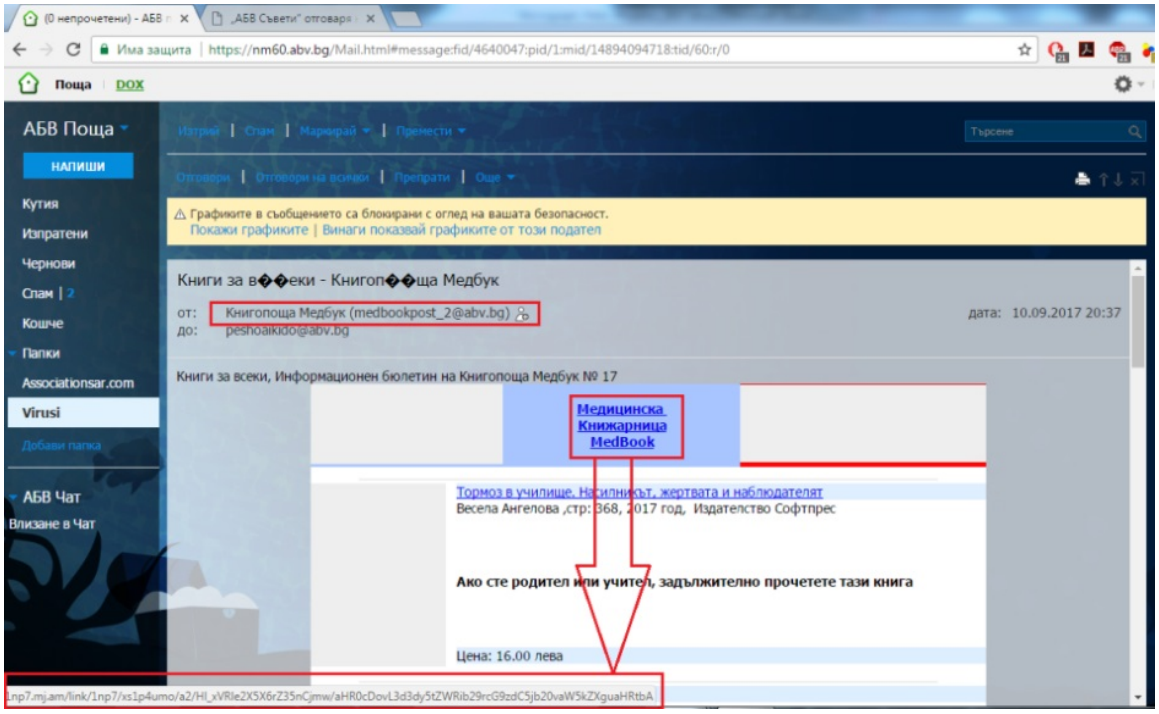
На фиг. 3 е представена поредната реална компютърно-базирана кибератака от тип социално инженерство, при която е изпратено фалшиво електронно съобщение до източник "peshoaikido@abv.bg" и с подател "PayPal (No.Reply@linuxhosting09.rediff.com)" и с име на темата на писмото "Your PayPal Account Will Be Closed in 24 Hours.". Ако се мине с курсора на мишката върху бутон-текста "Log In To My Account", тогава долу вдясно се появява уеб адреса на връзката за достъп "https://pay.plogin.updata.inftormtion.home.lmconcertinas.com.br/ok/". Ако беше истинско писмото, трябваше задължително името на домейна от източника да съвпада с уеб адреса на уеб страницата. В този случай това е истинска фалшификация и измама!!!

На фиг. 4 е представена поредната реална компютърно-базирана кибератака от тип социално инженерство, при която е изпратено фалшиво електронно съобщение до източник "peshoaikido@abv.bg" и с подател "Книгопоща Медбук (medbookpost_2@abv.bg)" и с име на темата на писмото "Книги за в►►еки - Книгоп►►ща Медбук". Ако се мине с курсора на мишката върху бутон-текста "Медицинска книжарница MedBook", тогава долу вдясно се появява уеб адресът на връзката за достъп "http://1np7.mj.am/link/1np7/xs1p4umo/a2/Hl_xVRle2X5X6rZ35nCjmw/aHR0cDovL3d3dy5tZWRib29rcG9zdC5jb20vaW5kZXXguaHRtbA". Ако беше истинско писмото, трябваше

задължително името на домейна от източника да съвпада с уеб адреса на уеб страницата. В този случай това е истинска фалшификация и измама!!!



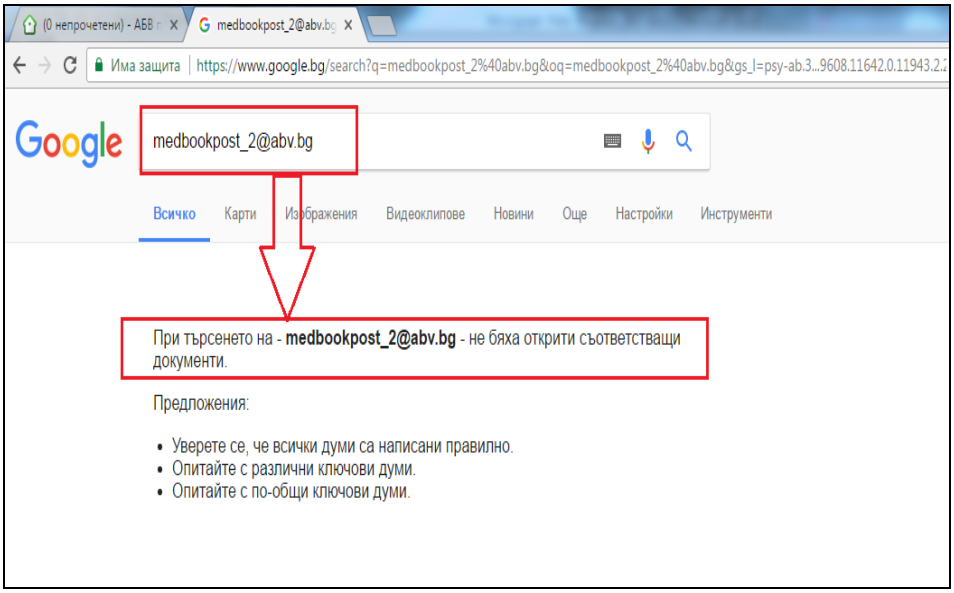
Фиг. 3. Фалшификация с електронни съобщения



Фиг. 4. Фалшификация с електронни съобщения

За да бъде потвърдена легитимността на подателя на писмото, е необходимо да се напише просто неговият имейл "medbookpost_2@abv.bg" в търсещата машина Google.bg.

От фиг. 5 се установи, че такъв имейл изобщо никъде не съществува и това означава в действителност, че е поредната кибератака "фишинг" от тип социално инженерство.



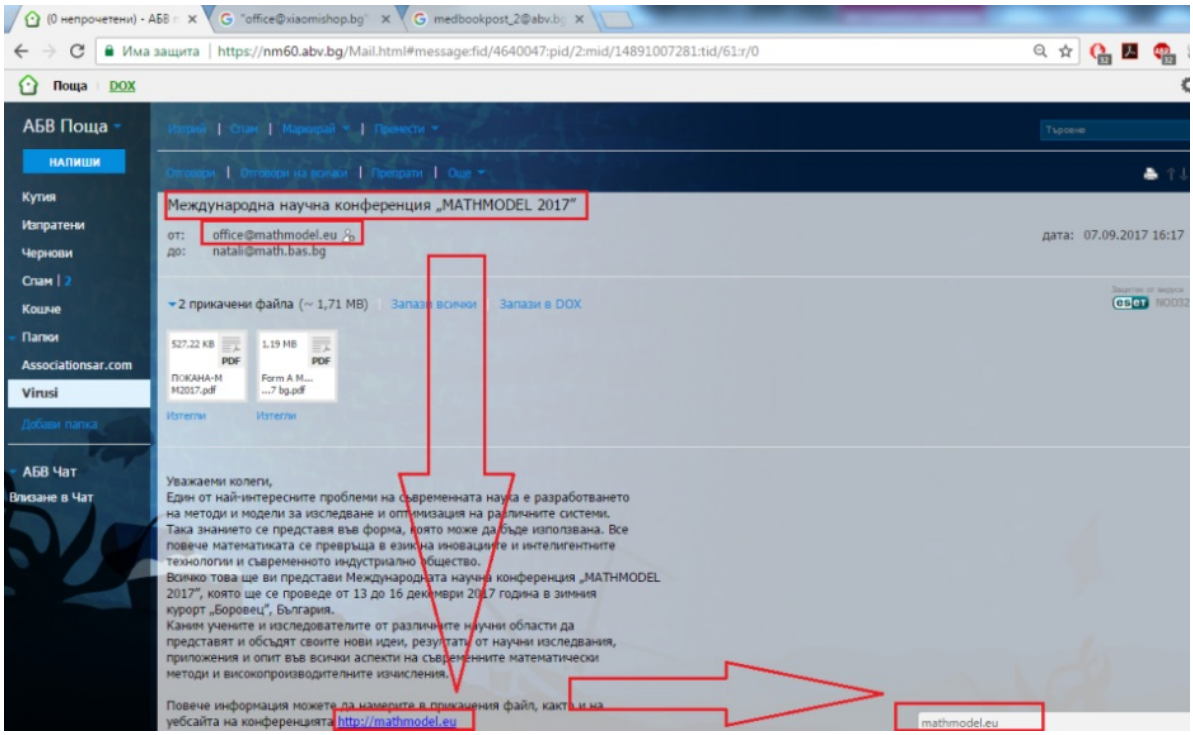
Фиг. 5. Проверка за легитимност на имейла на подателя

На фиг. 6. е представено нормално изпратено електронно съобщение до източник "peshoaikido@abv.bg" и с подател "office@mathmodel.eu" и с име на темата на писмото "Международна научна конференция "MATHMODEL 2017". Ако се мине с курсора на мишката върху бутон-текста "http://mathmodel.eu", тогава долу вдясно се появява уеб адресът на връзката за достъп - "mathmodel.eu". В този случай това е истинско електронно писмо, защото домейнът от подателя на писмото съвпада с уеб адреса на уеб страницата му!!!

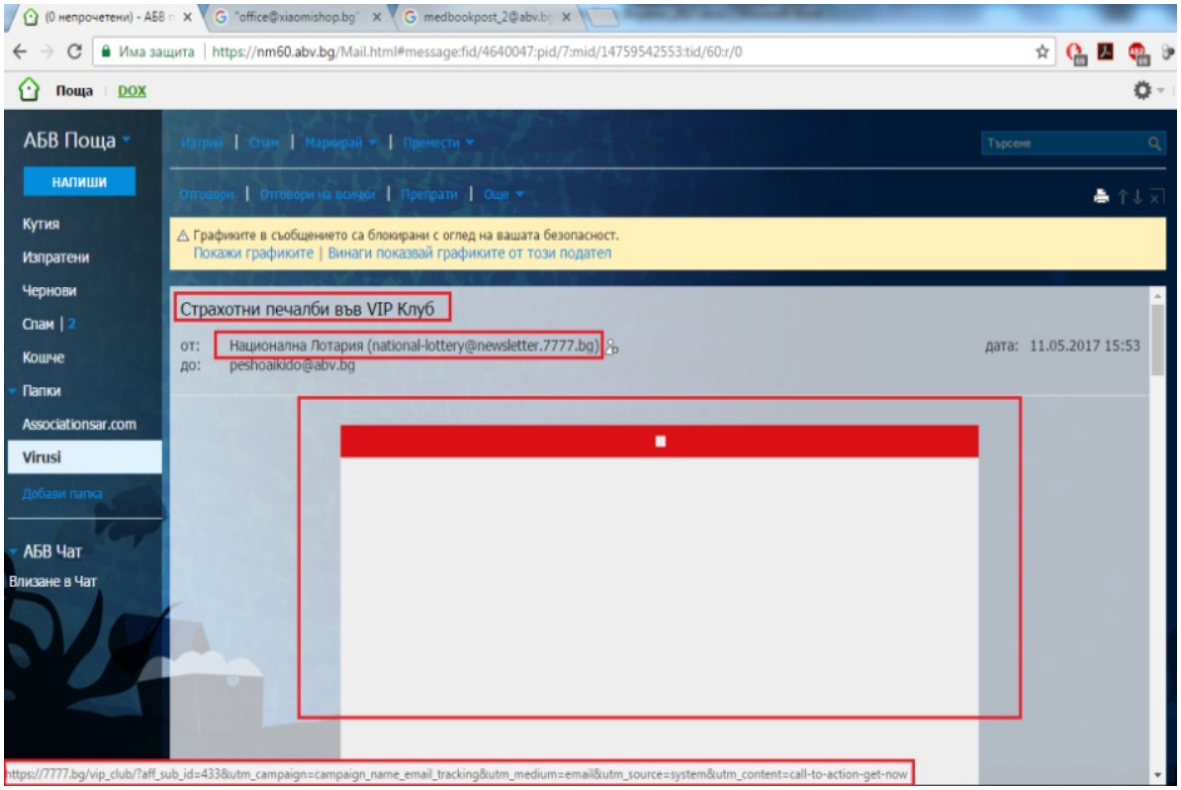
На фиг. 7. е представено нормално изпратено електронно съобщение до източник "peshoaikido@abv.bg" и с подател "Национална лотария (national-lottery@newsletter.7777.bg)" и с име на темата на писмото "Международна научна конференция "Страхотни печалби във VIP Клуб". Ако се мине с курсора на мишката върху празното уеб поле, тогава долу вдясно се появява уеб адресът на връзката за достъп "https://7777.bg/vip_club/?aff_sub_id=433&utm_campaign=campaign_name_email_tracking&utm_medium=email&utm_source=system&utm_content=call-to-action-get-now". В този случай това е истинско електронно писмо, защото домейнът от подателя на писмото съвпада с уеб адреса на уеб страницата му!!!

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).



Фиг. 6. Истинско изпратено електронно съобщение



Фиг. 7. Истинско изпратено електронно съобщение

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да предприемат и направят следните защитни действия като:

- Задължително периодично сменяне на паролите на служители.
- Блокиране на потребителския акаунт на служителя, в случай че са направени повече от три или повече неуспешни опита. Времето за блокиране може да бъде настроено за 1 ден.
- Използване на специални машини за унищожаване на документи от тип Шредер. По този начин киберпрестъпникът няма да може да намери никакви запазени листа от хартия в кофите за боклук на организацията.
- Задължителна идентификация на служителите чрез уникални идентификационни карти, пръстови отпечатъци, специални униформи, гривни на ръцете, устройства за сканиране на ретината на очите и др.
- Когато в организацията има ден на отворените врати, е необходимо да има специални лица, които да следят всички гости какво правят и къде ходят.
- Задължително преминаване на специални курсове за повишаване на квалификацията на служителите и подписване на специални документи за това, че са разбрали и ще спазват политиките на информационна сигурност. В случай че служителят не спазва регламентираните вътрешни правило, го грози наказателна отговорност според наказателния кодекс и наказателно процесуалния кодекс на Република България.

ЛИТЕРАТУРА:

[1] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[2] Fetfov O., Tonev V. Bedzhev B. “Information Encryption with Combination Generator”, CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[3] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[4] Hristov, Hr., Boyanov, P., Trifonov, T., Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 101-107.

[5] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[6] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[7] Hristov, Hr., A modern survey on problems of business organization’s security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[8] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[9] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference “Technics. Techologies. Education. Safety ’18”, Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[10] Shimeall T. J., Spring J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[11] Shimonski R. J., Schmied W., Shinder W. T., Chang V., Simonis D., Imperatore D., Building DMZs for Enterprise Networks, Syngress Publishing, 2003, ISBN: 1-931836-88-4, pp. 831.

[12] Shipley Todd G., Bowker A., Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress, 2014, ISBN 978-0-12-407817-8, pp. 497.

[13] Sikorski M., Honig A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, San Francisco, USA, 2012, ISBN: 978-1-59327-290-6, pp. 800.

[14] Simmons C., Shiva S., Dasgupta D., Wu Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA ’14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[15] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[16] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.

[17] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[18] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[19] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[20] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[21] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal with Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[22] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[23] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[24] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност”, ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

[25] Савов, И., Относно някои аспекти от процедурите по използване на трафичните данни в Република България и някои европейски страни, Международна конференция „Противодействие на радикализацията и тероризма”, Академия на МВР, април 2017 г., ISBN 978-954-348-145-3, с. 249-259.

Име на автора: доц. д-р инж. Петър Красенов Боянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com, petar.boyanov@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 52 - 59 Problems of Security Systems

IMPLEMENTATION OF CYBER ATTACKS AGAINST WEB SERVERS AND WEB APPLICATIONS

PETAR KR. BOYANOV

ABSTRACT: *In this paper implementation cyber-attacks against web servers and web applications is made.*

KEYWORDS: *Footprinting, Information Security, Modern cyber-attacks, Social engineering, Vulnerability, Web server, Web applications.*

ПРИЛОЖЕНИЕ НА КИБЕРАТАКИ, НАСОЧЕНИ СРЕЩУ УЕБ СЪРВЪРИ И УЕБ ПРИЛОЖЕНИЯ*

ПЕТЪР КР. БОЯНОВ

АБСТРАКТ: *В тази статия са извършени научни експерименти и изследвания относно начините на приложение на кибератаки, насочени срещу уеб сървъри и уеб приложения.*

1. Въведение

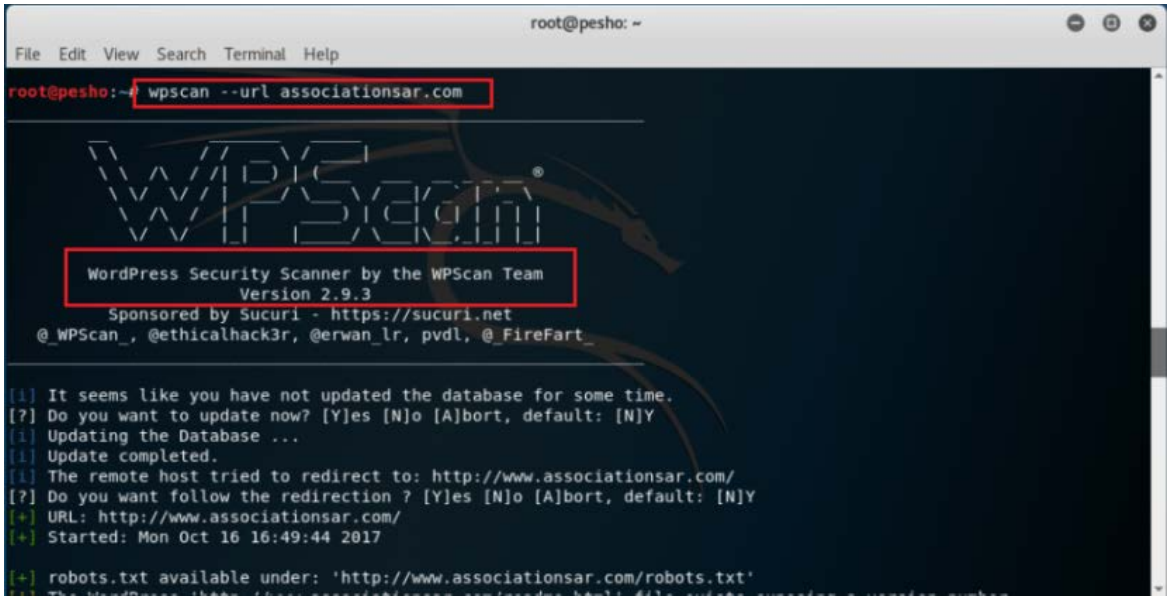
Тези атаки се разделят на [1], [2], [3], [4], [5], [6], [8], [10], [12], [14], [15], [24], [25]:

- Кибератаки, насочени към функциите на отдалеченото администриране;
- Кибератаки, насочени към необходими услуги;
- Кибератаки насочени към разпръскващи съобщения за грешки;
- Кибератаки, насочени при използване на пароли по подразбиране;
- Кибератаки, насочени при използване на прости скриптове и конфигурации;
- Кибератаки, насочени към приложението SSH с използване на груба сила;
- Кибератаки с човек по средата;
- Кибератака с отказ на услуги;
- Кибератаки с инжектиране на софтуерен SQL програмен код.

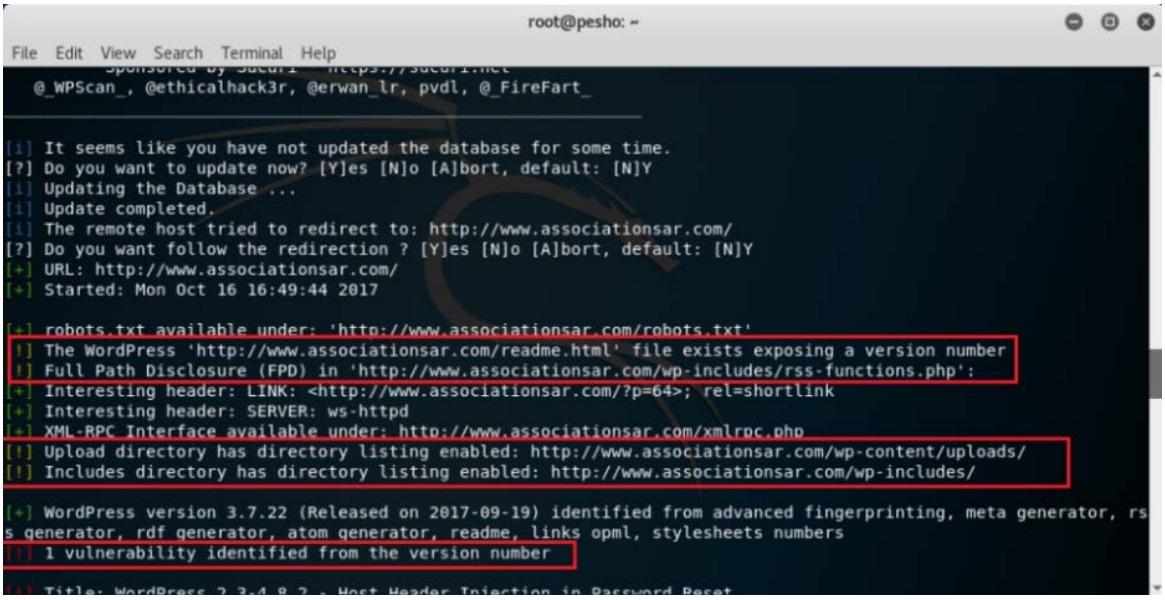
2. Изложение

На фиг. 1 е показано използването на командата "wpscan --url associationsar.com". Целта на програмата wpscan е да сканира избрания уеб сайт на жертвата и след това на базата на получените резултати да се открият какви уязвимости притежава този уеб сайт [4], [5], [6], [7]. В случая уеб сайтът associationsar.com е създаден с помощта на cms уеб платформата - WordPress. В практиката повечето готови платформи, които се използват за създаване на уеб сайтове, крият сериозни опасности, защото с всеки изминал ден се появяват нови и нови уязвимости и експлойти [1], [2], [3], [4], [5], [7], [8], [9], [11], [15], [16], [17], [18], [19], [20], [21], [22], [23].

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.



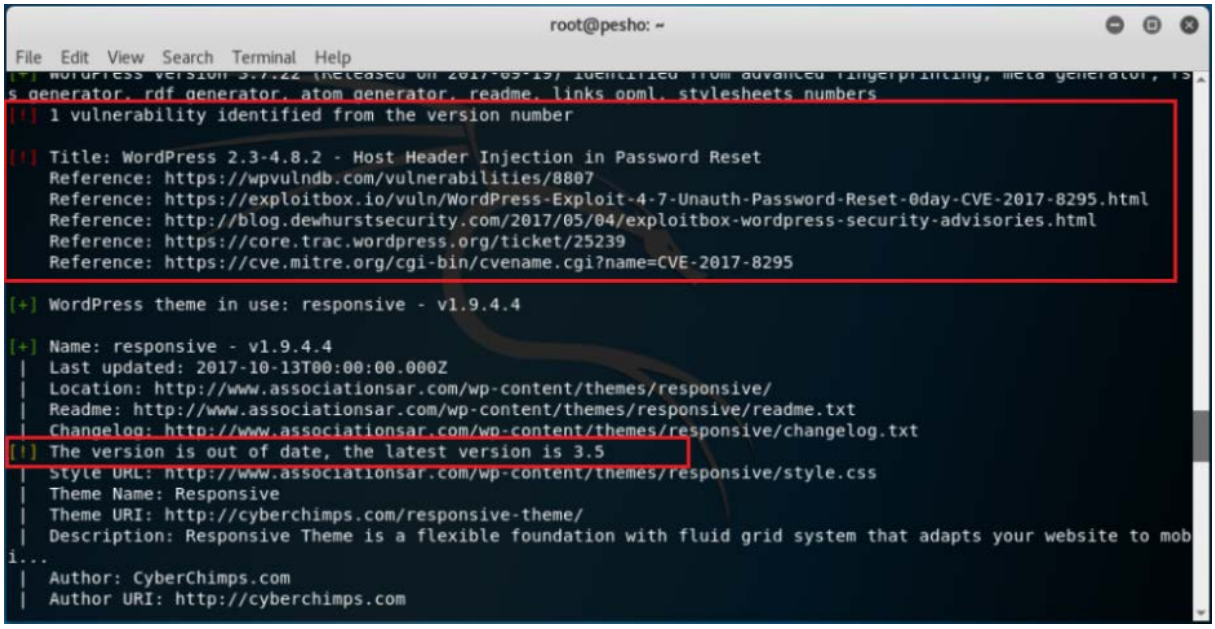
Фиг. 1. Първоначално конфигуриране на параметрите на програмата wpscan



Фиг. 2. Получени резултати след стартиране на програмата

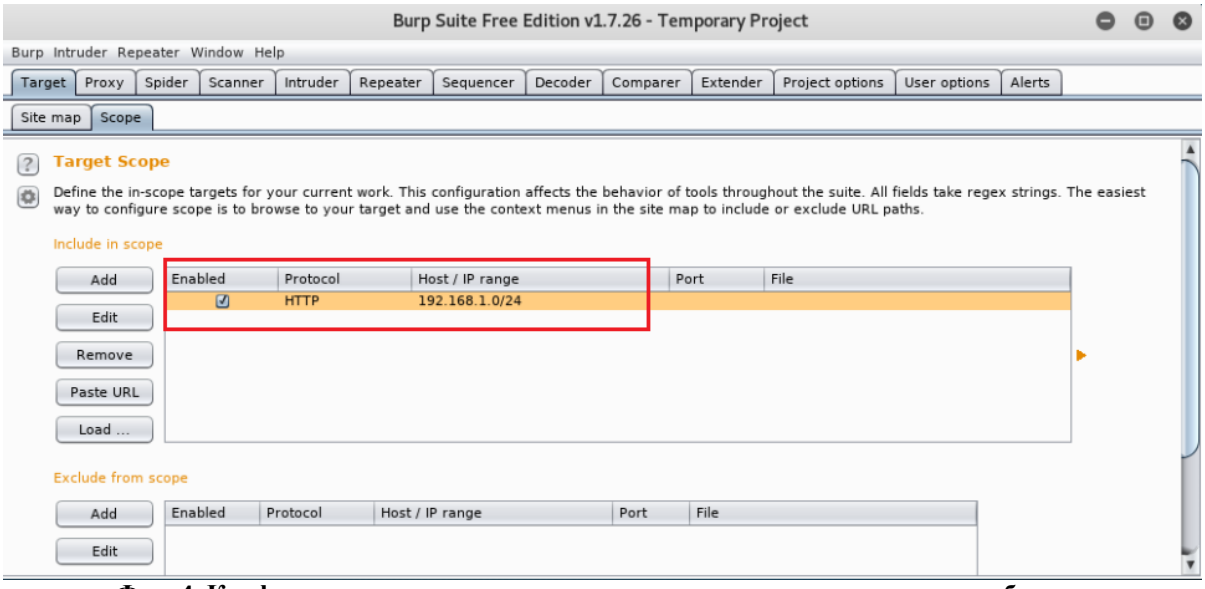
От фиг. 2 се установи, че е активирана функцията за разлистване на директориите на уеб сайта - "http://www.associationsar.com/wp-content/uploads/". По този начин киберпрестъпникът ще може да разлиства всички възможни файлове от всички създадени директории на уеб сайта. Възможно е дори той да намери важна информация, която не трябва да бъде споделена за други външни лица [1], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22].

От фиг. 3 се установи, че е открита една сериозна уязвимост, носеща името "Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset". Ако злонамереният извършител експлоатира тази уязвимост, тогава той ще получи пълен администраторски достъп до уеб сайта жертва. Обикновеният потребител не може по никакъв начин да се противопостави на тази нова открита уязвимост. Единственото решение е да се обнови цялото ядро на уеб платформата до най-новата версия, която съществува на официалната страница на платформата [24], [25].



Фиг. 3. Получени резултати след стартиране на програмата

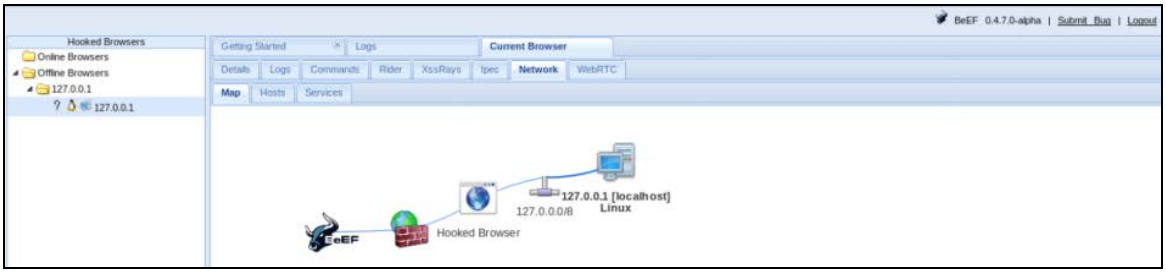
На фиг. 4 е показан графичният потребителски интерфейс на софтуерната програма за сканиране на уеб уязвимости в уеб сървъри и приложения. В случай е избрана цялата компютърна мрежа 192.168.1.0/24 да бъде сканирана. Програмата е стартирана отново под Linux базирана операционна система.



Фиг. 4. Конфигуриране на цялата компютърна мрежа за сканиране на уеб уязвимости

Друга изключително много зловредна програма, предназначена за атакуване на уеб приложения и уеб сайтове, е BeEF с версия 0.4.7.0-alpha. В действителност BeEF представлява голяма софтуерна рамка, която съдържа в себе си различни библиотеки, компоненти, модули и софтуерни програми, насочени изцяло за атакуване на различни уеб сайтове и уеб приложения [1], [14]. Тази софтуерна платформа се използва под Linux базирани операционни системи. На фиг. 5 е показана цялата карта на мрежата за атакуване. Трябва да се знае, че с тази програма се постига пълен успех при реализирането

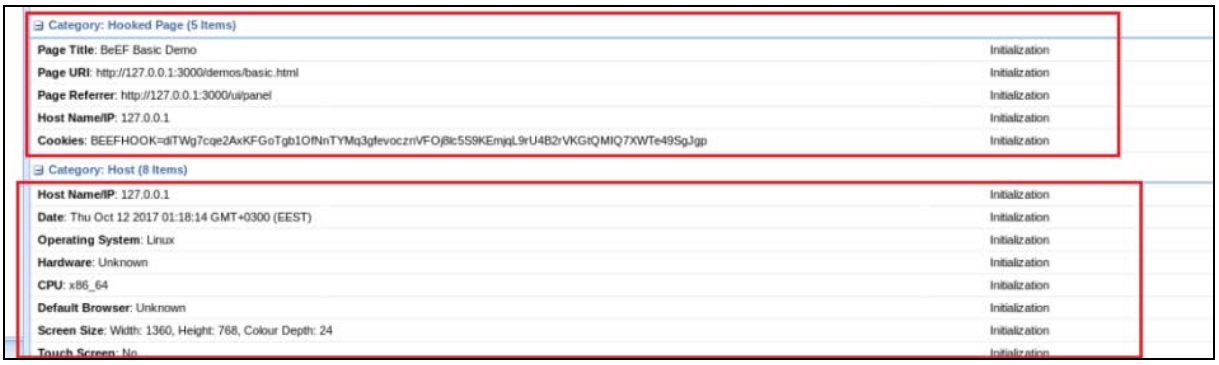
на кибератака срещу уеб сайтове и поради тази причина е избран вътрешният мрежов адрес 127.0.0.1 (локалния хост) за тестове цели.



Фиг. 5. Конфигурирана мрежова карта

На фиг. 6 са показани всички конфигурирани параметри, които ще бъдат използвани за осъществяване на кибератаки към уеб сайтове и уеб приложения. Под термина уеб приложение трябва да се има предвид, че става въпрос за компоненти, които са нужни за правилната работа на уеб браузера като [1], [2], [3], [3], [4], [5], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [24], [25]:

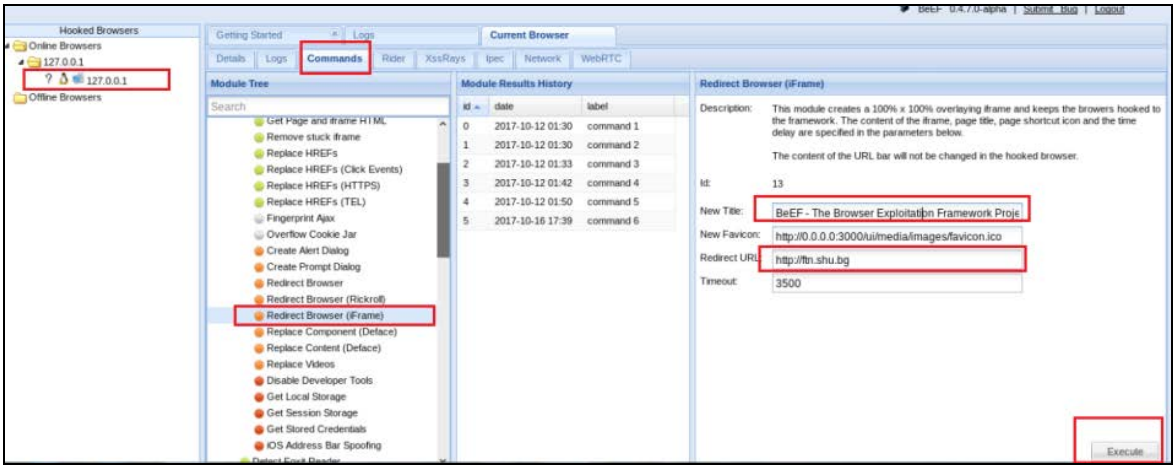
- Adobe Flash Player.
- VBScript.
- Google applications.
- QuickTime movie.
- RealPlayer.
- Windows Media Player.
- Adobe Reader.
- ActiveX контроли.
- Бисквити за сесиите и др.



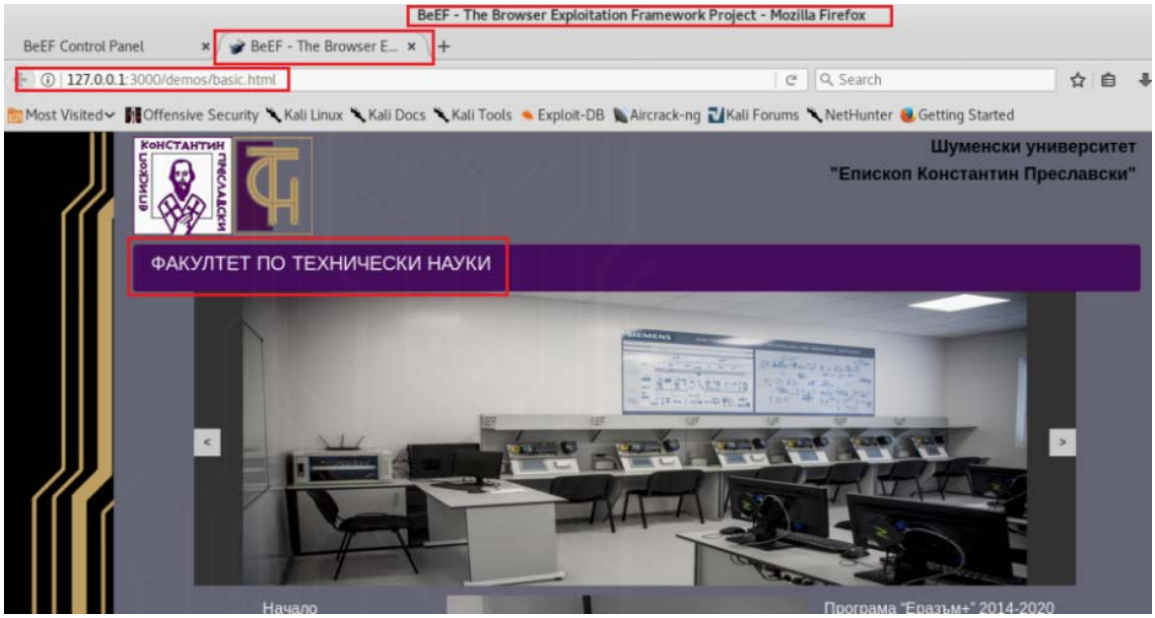
Фиг. 6. Конфигурирани параметри за използване на атакуваща уеб платформа

На фиг 7 е показана първата уеб атака, при която киберпрестъпникът изпраща следния уеб линк "http://127.0.0.1:3000/demos/basic.html" към своята жертва. В действителност този уеб линк ще пренасочи жертвата към друг заразен уеб сайт. Като уеб сайт за пренасочване е избран - "http://ftn.shu.bg". Крайният резултат е показан на фиг. 8.

Като краен резултат се установи, че вместо да се зареди съдържанието на уеб страницата http://127.0.0.1:3000/demos/basic.html, се зарежда съвсем друга уеб страница - "Факултет по технически науки".



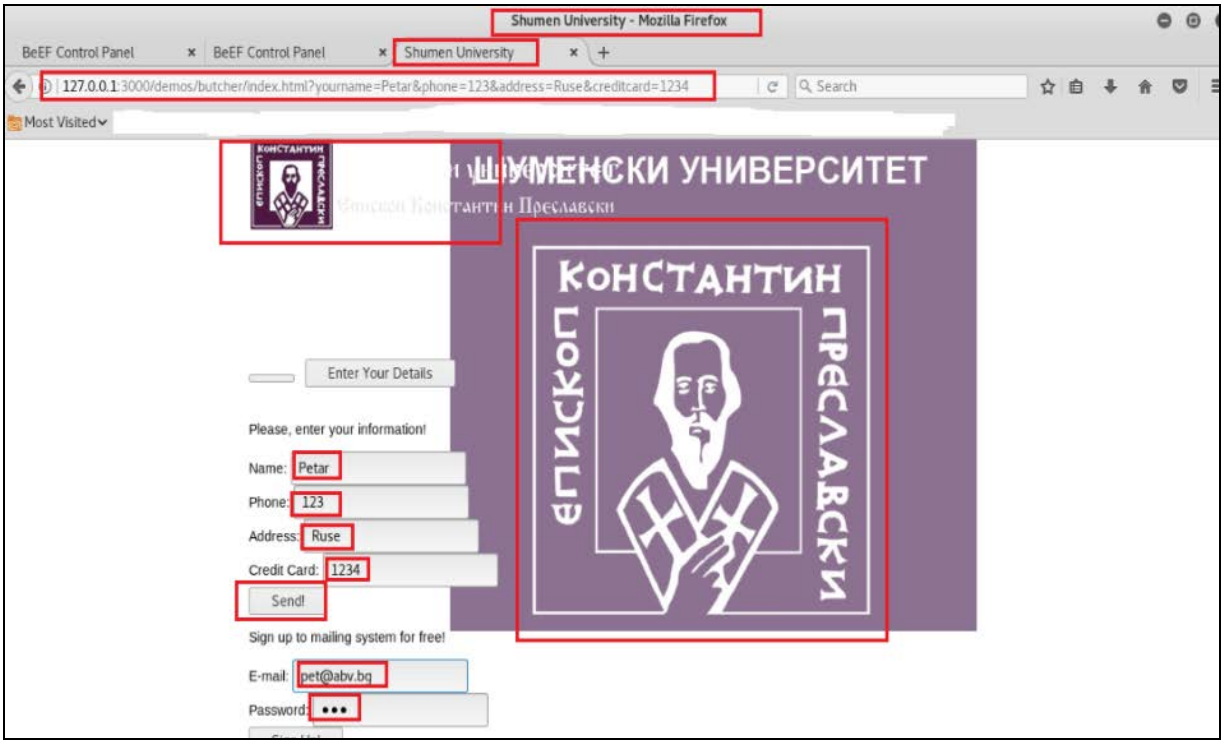
Фиг. 7. Избор на уеб сайт за пренасочване



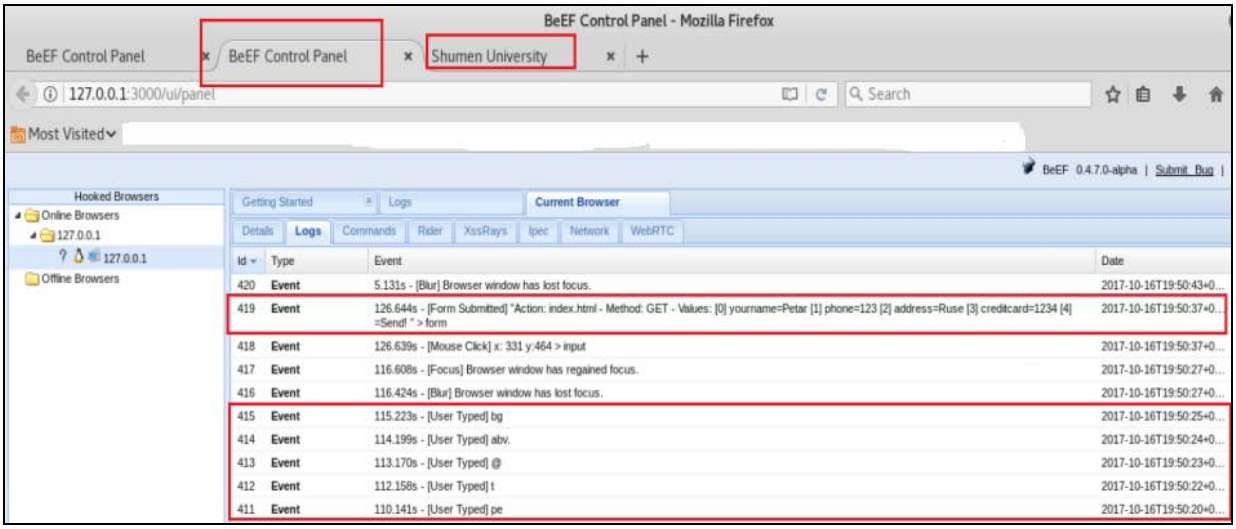
Фиг. 8. Получен резултат след пренасочването на уеб страниците

В днешно време една от най-зловредните кибератаки, която се използва за експлоатиране на уязвимости и осъществяване на несанкциониран достъп до ресурсите на машината жертва, е кръстосаното инжектиране на скрипт (XSS). При тази кибератака е възможно киберпрестъпникът да създаде точно оригинално копие на официалния уеб сайт и чрез него да подмами обикновените потребители да си въведат потребителски имена, електронните пощи, паролите, трите имена, адрес и телефон [1], [3], [4], [5], [6], [7], [8], [11], [12], [13], [14], [16], [17], [18], [19], [24].

На фиг. 9 е илюстриран създаден фалшив уеб сайт, на който служителя трябва да си въведе името, телефонния номер, адреса, номера на кредитната карта, електронната си поща и паролата за електронната си поща. След натискане на бутона "Send!", цялата попълнена информация се изпраща на киберпрестъпника и това е показано на фиг. 10.



Фиг. 9. Въвеждане на лични данни във създаден фалшив уеб сайт



Фиг. 10. Получаване на изпратените лични данни на жертвата

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди

лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да предприемат и направят следните защитни действия като:

- Конфигуриране на защитни стени и системи за откриване на прониквания, които да блокират опити за сканиране или опити за получаване на неоторизиран достъп до ресурсите, намиращи се на уеб сървъра.
- Блокиране на всякакви входящи мрежови заявки по протокола ICMP, насочени към уеб сървъра на организацията.
- Да се подсигури единствена връзка за отдалечен достъп до уеб сървъра само на администратора по сигурността.
- Невинаги трябва да се има пълно доверие на защитения приложен протокол HTTPS, защото за кибератаките от тип кръстосано инжектиране на скрипт (XSS) няма намерена защита до момента.
- Изключване на всички акаунти по подразбиране от уеб платформите.
- Редовно сканиране за най-новите появили се уязвимости и инсталиране на софтуерни обновления за затваряне на слабостите и дупките в сигурността.

ЛИТЕРАТУРА:

[1] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[2] Fetfov O., Tonev V. Bedzhev B. “Information Encryption with Combination Generator”, CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[3] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[4] Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., Educational simulation the local area network of academic departments with securely configured FTP server, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.

[5] Hristov, Hr., Boyanov, P., Trifonov, T., Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 101-107.

[6] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[7] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[8] Hristov, Hr., A modern survey on problems of business organization’s security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[9] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[10] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference “Technics. Techologies. Education. Safety ’18”, Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[11] Shimeall T. J., Spring J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[12] Shimonski R. J., Schmied W., Shinder W. T., Chang V., Simonis D., Imperatore D., Building DMZs for Enterprise Networks, Syngress Publishing, 2003, ISBN: 1-931836-88-4, pp. 831.

[13] Shipley Todd G., Bowker A., Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress, 2014, ISBN 978-0-12-407817-8, pp. 497.

[14] Sikorski M., Honig A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, San Francisco, USA, 2012, ISBN: 978-1-59327-290-6, pp. 800.

[15] Simmons C., Shiva S., Dasgupta D., Wu Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA ’14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[16] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[17] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.

[18] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[19] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[20] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[21] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[22] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal with Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[23] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[24] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[25] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност”, ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

Име на автора: доц. д-р инж. Петър Красенов Боянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com, petar.boyanov@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 60 - 67 Problems of Security Systems

IDENTIFICATION OF THE MAIN TYPES AND PHASES OF MODERN CYBER ATTACKS AND THEIR USE FOR IDENTIFYING WEAKNESSES IN COMPUTER NETWORKS AND SYSTEMS IN THE REGIONAL GOVERNANCE OF REGIONAL DIRECTORATES OF INTERIOR

PETAR KR. BOYANOV, VESELIN KR. RAYNOV

ABSTRACT: *In this paper identification of the main types and phases of modern cyber-attacks and their use for identifying weaknesses in computer networks and systems in the Regional Governance of Regional Directorates of Interior is made.*

KEYWORDS: *Computer networks, Modern cyber-attacks, Regional Governance, Regional Direction of Interior.*

ИДЕНТИФИЦИРАНЕ НА ОСНОВНИТЕ ТИПОВЕ И ФАЗИ НА СЪВРЕМЕННИТЕ КИБЕРАТАКИ И ИЗПОЛЗВАНЕТО ИМ ЗА ОПРЕДЕЛЯНЕ НА СЛАБОСТИТЕ В КОМПЮТЪРНИТЕ МРЕЖИ И СИСТЕМИ В РАЙОННОТО УПРАВЛЕНИЕ ПРИ ОБЛАСТНА ДИРЕКЦИЯ НА МВР*

ПЕТЪР КР. БОЯНОВ, ВЕСЕЛИН КР. РАЙНОВ

АБСТРАКТ: *В тази статия са идентифицирани основните типове и фази на съвременните кибератаки и използването им за определяне на слабостите в компютърните мрежи и системи в районното управление при областна дирекция на МВР.*

1. Въведение

В тази статия са идентифицирани основните фази на кибератаките, основните типове атаки и ресурсите на компютърните системи, към които са насочени, както и видовете хакери, осъществяващи тези атаки. В резултат на анализа на техните особености е определена сканиращата фаза като една от най-важните фази на детайлно събиране на информация за злонамерения извършител, позволяваща му в последствие реално да осъществи злонамерени действия [1], [4], [5], [10], [11], [15], [17], [18], [19], [20], [21]. [27].

2. Изложение

Идентифициране на основните фази на кибератаките

За да бъде осъществена определена кибератака е необходимо стриктно и последователно да се преминат всички фази на атаката. Неправилното изпълнение на дадена фаза оставя доказателства и следи за аналитиците и специалистите по компютърна и мрежова сигурност да следят и хванат злонамерения извършител, с което да отговоря пред съдебните институции за своите извършени зловредни деяния. Фазите на кибератака

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

са разузнаване, мрежово сканиране, получаване на достъп, поддържане на достъпа и прикриване на следите [2], [3], [5], [6], [7], [8], [9], [10], [15], [17], [18], [19], [20], [21], [25].

Разузнавателна фаза

Разузнаването е предварителната фаза, където атакуващият събира колкото се може повече важна и конфиденциална информация за избраната организация с цел извършване на несанкционирано проникване в ресурсите на дадена компютърна мрежа. Разузнавателните техники се разделят главно на пасивни и активни техники за събиране на информация.

При пасивното разузнаване злонамереният потребител не взаимодейства директно с компютърната система. Вместо това той разчита на наличната публична информация, социално инженерство и изтичане на информация.

Активните разузнавателни техники [3], [4], [10], [11] от своя страна, включват директно взаимодействие с избраната компютърна жертва чрез използване на мрежови софтуерни инструменти за откриване на отворени портове, достъпни хостове, намиране на местоположението на рутери и комутатори, изобразяване на компютърната мрежа, детайли за операционните системи и приложенията. Активното разузнаване се прилага тогава, когато съществува малка вероятност за разкриване на несанкционираните действия от атакуващия [27].

По този начин атакуващият потребител (хост) изгражда специална стратегия за събиране на всякаква информация за жертвата [9], за да проникне най-лесно в периметъра на сигурност на организацията. Изграждането на детайлна мрежова карта на организацията е друга основна задача, която ще подпомогне атакуващият да разбере архитектурата на цялата мрежа.

Видове и начини за събиране на мрежова информация

Събирането на мрежова информация включва:

- Научаване за името на домейна на организацията [3], [4].
- Научаване за вътрешните домейни имена [1], [6].
- Научаване за мрежовите блокове от IPv4 адреси.
- Разбиране за това, кои IPv4 адреси могат да бъдат достигнати от Интернет.
- Научаване на използваните мрежови и транспортни протоколи, както и различните стартирани услуги на съответния порт.
- Научаване за стартираните вътрешни уеб страници, както и версиите на външните уеб сървъри, заедно със съответните им бази от данни.
- Разбиране за съществуването на защитни механизми, използващи листове за контрол на достъпа, защитни стени и системи за откриване и предотвратяване на несанкционирани прониквания и др.

Събиране на системна информация

Събирането на системна информация включва:

- Лист с имената на потребителите и групите [3].
- Информация за пътищата на маршрутизиращата таблица.
- Информация при активиран SNMP протокол.
- Информация за системната архитектура на системата.
- Информация за активиран отдалечен достъп до системата [4].

- Определяне и разпознаване на различните типове инсталирани операционни системи, софтуерни платформи за интеграция и развитие [5].
- Използване на техники за разпознаване на самоличността на даден хост и цяла компютърна мрежа и откриване на използваните DNS сървъри.
- Намиране на важни уязвимости в операционните системи или в различни софтуерни платформи и програми.

Събиране на информация за организацията

Събирането на информация за организацията.

- Различни детайли за работещите.
- Адреси и телефонни номера на работещите.
- Местоположение и инфраструктура на организацията.
- Уеб сървърни линкове, свързани с компанията в Интернет.
- Различни коментари в HTML сорс кода на уеб страницата [3].
- Информация за организацията във вестници и електронни брошури.

Видове заплахи от разузнавателната атака

Социално инженерство

Този вид заплаха помага на атакуващия да изпълни системна и мрежова атака чрез събрана детайлна информация за съществуващите уязвимости. След това хакерът експлоатира откритите уязвимости, за да може да придобие пълен достъп до машината-жертва или цялата компютърна мрежа.

Изтичане на информация

Изтичането на важна и конфиденциална информация е много сериозен проблем за повечето фирми и организации. Типичен пример за изтичане на важна информация е изхвърлянето на важни принтирани документи в кошчето за боклук, при което атакуващият може да получи информация за трите имена на жертвата, използвани пароли и думи, становище за кредитната карта, банкови извлечения със записан единен граждански номер, разписки след теглене от ATM банкомат, частни телефонни номера, записани кодове за достъп в социалните мрежи като facebook, twitter и google+ [3], [4], [5], [6]. [8].

Корпоративен шпионаж

Корпоративният шпионаж е един от важните механизми за получаване на конфиденциална информация и се извършва най-често чрез поставяне на хора, които имат задачата да следят всички в организацията и след това да предоставят получените данни на своя поръчител [1], [3], [4], [5], [9], [10], [11], [18], [19], [20], [21], [25]. [26].

Сканираща фаза

Сканирането е фазата непосредствено преди същинската кибератака. При тази фаза, атакуващият използва събраната детайлна информация от процеса на разузнаване с цел откриването на специфични уязвимости. Сканирането може да се приеме и като логическо разширение на активното разузнаване, като в практиката повечето от киберекспертите не правят разлика между сканирането и активното разузнаване. Атакуващият събира критично важна информация за архитектурата на компютърните системи, маршрутизаторите, комутаторите, защитните стени, сензорите за засичане и

предотвратяване на изпратени злонамерени мрежови пакети чрез прости инструменти като “tracert” за операционни системи, базирани на Windows. Този мрежови инструмент е изключително полезен, защото показва всички пътища (подскоци), през които преминава изпратения разузнавателен пакет. В случая всеки подскок представлява физическо устройство, наречено рутер с IP адрес, през който преминава пакета. Всеки рутер намалява с единица времето на живот на пакета с цел предотвратяването на пакетни бури и зацикления в дадената компютърна мрежа [1], [3], [4], [5], [9], [10], [11], [25].

Портовите скенери се използват за откриване на слушащи портове, които, от своя страна, носят информация за типа на услугите, протичащи на компютърната машина на жертвата. Основната защитна техника срещу портовите скенери е изключването на системните услуги, които не са задължителни за изпълнение. Друга много важна защитна техника е прилагането на пакетна филтрация на целия трафик в компютърната мрежа. Въпреки това, повечето от професионалните хакери и злонамерени потребители могат да използват софтуерни инструменти, с които да се определят правилата, приложени при пакетната филтрация [1], [3], [4], [5], [9], [10], [11], [15], [17], [25], [27].

Най-често използваните софтуерни инструменти са скенерите за уязвимости, които имат способността да сканират хиляди от известните уязвимости на жертвата. Това, от своя страна, дава предимство на атакуващия, защото трябва да намери една единствена системна пролука и да експлоатира тази уязвимост. Повечето организации, които използват системи за откриване на нарушители, трябва да бъдат много бдителни, защото хакерите могат да използват отбягващи техники с модифицирани софтуерни инструменти. Най-сериозните атаки са външният отказ на услуги, които могат или да изчерпят ресурсите, или да спрат услугите, стартирани на машината на жертвата. Услугите могат да бъдат спрени от съответния прилежащ процес чрез използването на логическа или времева бомба, реконфигуриране и рухване на софтуерната система. Ресурсите могат да бъдат изчерпани локално чрез натоварване и запълване на изходящите мрежови връзки с доста излишна информация [1], [3], [4], [5], [9], [10], [11], [17], [18], [19], [20], [21].

Фаза за получаване на достъп

Достъпът може да бъде получен чрез физически досег, локалната мрежа, глобалната мрежа INTERNET и неактивно състояние без наличие на мрежа. Типични атаки са препълване на буфера на стека, услуга с отказ на услуги, несанкционирано открадване на мрежовата сесия. Атакуващият използва измамна техника, наречена “spoofing”, с която се експлоатира компютърната система чрез претендирането той да бъде легитимен потребител или друга приета система. Те използват тази техника да изпращат пакети с данни, съдържащи определен дефект за машината на жертвата с цел експлоатирането на уязвимост [11]. Отдалеченото изпращане на огромен брой пакети може да се използва за спиране на наличността на основните услуги. Смърф атаката причинява процеса на взаимно наводнение с пакети между потребителите в компютърната мрежа. По този начин всеки един потребител се превръща в атакуващ хост, докато истинският хакер остава анонимен през цялото време [1], [3], [4], [5], [9], [10], [11], [26], [27].

Шансовете на хакера да получи достъп да компютърната система са повлияни от фактори като архитектурата, конфигурацията на жертвата, нивата на умения на извършителя и първоначалното придобито ниво на достъп.

Най-вредният тип на атака е отказът на услуги, който може да се превърне в разпределен отказ на услуги, където злонамереният извършител използва специализиран софтуер, разпределен между няколко машини в глобалното пространство с цел започване на координирана атака с отказ на услуги от множество източници.

Фаза за поддържане на достъпа

Веднъж получил достъп до компютърната система на жертвата, извършителят е способен да използва системата заедно с нейните ресурси, да използва разобличената машина за сканиране и експлоатиране на други системи, да съхранява малък профайл за своя акаунт и да продължава по-детайлно да експлоатира текущата система. Всичките тези дейности причиняват жестоки и непоправими щети на жертвата. Злонамереният извършител може също така да инсталира специална програма, наречена снифър [2], с която да се следи целия мрежови трафик, включващ и отдалечени сесии по услугите Telnet и FTP (File Transfer Protocol) [1], [3], [4], [5], [9], [10], [11], [26], [27].

Извършителите, които искат да останат незабелязани, премахват всички доказателства от системните записки и регистри и инсталират странична врата или инструмент, наречен троянски кон, с които да получат повторен достъп. Също така е възможна инсталацията в нивото на ядрото на съвкупност от инструменти за получаване на права като супер потребител или администратор за съответната операционна система. Тези инструменти се наричат още руткитове, които получават достъп на ниво операционна система, а троянските коне получават достъп на приложно ниво. И двата вида злонамерени софтуерни инструмента изискват от потребителя да ги инсталира на своята операционна система. При Windows базираните операционни системи, повечето троянски коне се инсталират от само себе си като услуга и се изпълняват като локална система, която има администраторски права [1], [3], [4], [5], [9], [10], [11].

Злонамерените извършители използват троянските коне [6] за трансфер на потребителски имена, пароли и всякаква друга информация, съхранявана на операционната система. По този начин те поддържат контрол върху системата за много дълъг период от време чрез затваряне на намерените уязвимости. Това се извършва за предотвратяване на възможността други злонамерени извършители да получат контрол върху тях.

Организациите могат да използват системи за откриване на нарушители или да разгърнат капани, наречени медени гърнета и мрежи, с които също да засекат нарушителите. Тези настройки е препоръчително да се извършват от компютърни специалисти и аналитици по мрежовата сигурност.

Фаза за прикриване на следите

След успешното инсталиране на троянския кон, извършителят има за цел да изпълни скрипт в троянския кон или rootkit [7], където множество от критични файлове са заменени с нови версии, скриващи атакуващия за секунди. Други техники включват стеганография и тунелиране. Стеганографията е процесът, при който се скриват данни в звукови и картинни файлове. Тунелирането взема предимство при протоколите за предаване чрез носене на един протокол над друг. Дори и при малко количество от допълнително място в TCP сегмента и заглавната част на IP протокола, той може да се използва за скриване на информация. Атакуващият може да използва компрометирана система, с която да започне нови атаки срещу други системи или да достигне до друга система през компютърната мрежа незабележимо. По този начин тази фаза на атака може да се превърне в разузнавателна фаза [1], [3], [4], [5], [9], [10], [11], [15], [17], [18], [19], [20], [21], [26], [27].

Определяне на основните типове злонамерени кибератаки

Атаки към операционните системи

Съвременните операционни системи съдържат множество функционалности, което ги прави изключително комплексни и сложни. Тези функционалности използват допълнителни процеси и услуги, което, от своя страна, разкрива повече уязвимости за експлоатиране [8], [12].

Атакуващите постоянно следят различните операционни система за нови уязвимости. Системните администратори трябва постоянно да са информирани за различни нови експлойти и постоянно да следят техните компютърни мрежи [12].

Инсталирането на нови обновления и поправки за дадена операционна система е задължителна стъпка за намаляване на риска от експлоатиране на уязвимост [22], [23], [24], [25].

Атаки към приложното ниво

В повечето случаи софтуерните разработчици се намират под постоянно напрежение, за да създадат определена софтуерна програма и да изпълнят своя краен срок. По този начин те нямат необходимото време напълно да тестват техните крайни софтуерни продукти преди да бъдат продадени, което оставя неразкрити дупки в сигурността [2]. Този факт е изключително опасен за по-новите софтуерни приложения, които се състоят с множество функции, допълнения и екстри. Тази сложност означава, че съществуват повече възможности за уязвимости [25].

За съжаление сигурността не е най-важния приоритет за софтуерните разработчици и затова след излизането на даден софтуерен продукт на пазара се предоставят различни допълнителни компоненти, наречени „add-on” [6], [9], [12], [13], [14], [15], [26], [27]. Проверката за грешки в тези софтуерни приложения може да бъде на много ниско ниво или почти да липсва, което от своя страна ще доведе до атаки с препълване на буфера.

Атаки към програмния код

Софтуерните програмисти често използват свободни и безплатни библиотеки и лицензиран код от други източници в техните програми. Това означава, че голяма порция от много софтуерни парчета ще бъде почти с една и съща структура и алгоритми и ако се открият уязвимости в този код, тогава всички тези парчета ще бъдат подложени на риск [1], [3], [4], [5], [9], [10], [11], [22], [23], [24], [26], [27].

Проблемът в цялата ситуация е, че повечето софтуерни разработчици оставят техните системни библиотеки и кодове непроменени [7], [13], [14]. Програмистите трябва да пренапишат и редактират всички системни библиотеки и кодове през определен интервал за време с цел намаляване на процеса на експлоатиране на уязвимости.

Атаки при неправилна конфигурация на системата

Независимо, че определена компютърна система изглежда сигурна и защитена, може само при една неправилна конфигурация да бъде разобличена. Системните администратори трябва много внимателно да конфигурират компютърните [7], [63] си системи и винаги да знаят какво се изпълнява върху тях. Необходимо е да се направи проста и ефективна конфигурация, премахваща всички ненужни услуги и софтуерни продукти и инструменти [1], [3], [4], [5], [9], [10], [11], [13], [14], [18], [19], [20], [21].

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста.

Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева." // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Идентифицирането на основните типове и фази на съвременните кибератаки и използването им за определяне на слабостите в компютърните мрежи и системи в Районното управление при Областна дирекция на МВР е изключително актуален проблем, на който служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да изградят специални политики за сигурност в случай на опити за несанкциониран достъп до информационните ресурси на съответната държавна институция.

ЛИТЕРАТУРА:

[1] Allen, L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing, Birmingham, UK, May 2012, ISBN 978-1-84951-774-4, pp. 414.

[2] Bodmer, S., Kilger, M., Carpenter, Gr., Jones, J., Reverse Deception: Organized Cyber Threat Counter-Exploitation, McGraw-Hill Education, 2012, ISBN: 978-0-07-177250-1, pp. 465.

[3] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[4] Hristov, Hr., Development of warfare and counter-terrorism. Journal Science Education Innovation, ISSN 1314-9784, vol. 3. 2014, pp. 104-111.

[5] Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[6] Kahya-Özyirmidokuz, E., Gezer, A., Ciflikli, C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, ISBN: 978-1-61208-242-4, pp.18 – 23.

[7] Kaur, R., Singh, G. Analysing, Port Scanning Tools and Security Techniques, International Journal of Electrical Electronics & Computer Science Engineering, Volume 1, Issue 5, October 2014, ISSN : 2348 2273, pp. 58 – 64.

[8] Meyers, C., Powers, S., Faissol, D., Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 22.

[9] Meyers, C., Powers, S., Faissol, D., Probabilistic Characterization of Adversary Behavior in Cyber Security, No. LLNL-TR-419023, Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 52.

[10] Shimeall T. J., Spring J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[11] Simmons, C., Shiva, S., Dasgupta, D., Wu, Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[12] Fetfov O., Tonev V. Bedzhev B. "Information Encryption with Combination Generator", CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[13] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[14] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[15] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference “Technics. Techologies. Education. Safety ’18”, Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[16] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[17] Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., Educational simulation the local area network of academic departments with securely configured FTP server, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.

[18] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[19] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София“, ISBN 978-954-01-3785-8, 2018 г.

[20] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[21] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[22] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[23] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[24] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal with Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[25] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[26] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[27] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност”, ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

Име на автора: доц. д-р инж. Петър Красенов Боянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: peshoaikido@abv.bg, peshoaikido@gmail.com, petar.boyanov@shu.bg
Име на съавтора: докторант Веселин Красимиров Райнов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: vesselin.raynov@gmail.com

INTEGRATED MONITORING AND CONTROL SYSTEM

DIMITAR G. CHOBANOV

ABSTRACT: *An integrated system, which combines the functions of three sub-systems: video surveillance system, system for access control and system for perimeter security is described. The systems' functionality is controlled by specialized software for surveillance and control.*

KEYWORDS: *Access control, Video surveillance, Perimeter security.*

ИНТЕГРИРАНА СИСТЕМА ЗА НАБЛЮДЕНИЕ И КОНТРОЛ*

ДИМИТЪР Г. ЧОБАНОВ

АБСТРАКТ: *Интегрирана система, която комбинира функциите на три подсистеми: система за видео наблюдение, система за контрол на достъпа и система за периметрова охрана. Функционалността на системите се контролира от специализиран софтуер за наблюдение и контрол.*

1. Въведение

Интегрираните системи за физическа сигурност включват в себе си комплекс от организационни и технически мероприятия за защита на обектите от всякакво несанкционирано проникване, от несанкционирано събиране на конфиденциална информация, от кражби, действия на вандализъм или саботаж. Те намаляват търговските рискове и опасността от нарушаване на бизнес процесите . Интегрираните системи могат и трябва да бъдат използвани в случаи на настъпване на събития, които са от значение за информационна безопасност – използване в съдебното производство, корпоративните разследвания, при промяна на мениджмънт системата на информационната безопасност на компаниите [1], [9], [10], [11], [12].

Част от възможните взаимосвързани елементи на интегрираните физически системи за сигурност включват в себе си:

- система за видеонаблюдение, включително тайно видеонаблюдение, дистанционни системи за видеонаблюдение, безжични, разпределени и централизирани системи за видеонаблюдение;
- аудио контрол, включващ дистанционен аудио контрол;
- системи за контрол на достъпа, системи за дистанционен контрол и управление на достъпа, системи за контрол на работното време, получаване на информация за местонахождението на служителите в обектите [10];
- системи за разпознаване на регистрационните номера в паркингите;
- защита с технически средства на помещения и обекти от несанкционирано събиране на информация [11];
- контрол на радиационната безопасност;
- различни системи за пожарна сигнализация;

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

- монтиране на бариери, турникети и пр.;
- комплекс от средства за защита от силово проникване.

Интегрираните системи за безопасност могат да бъдат изградени в различни отдалечени обекти с общ център за управление.

В настоящо време системите за видеонаблюдение включват в себе си не само стандартните възможности за възпроизвеждане и запис на видеоинформацията от камерата. Без участието на човека, те могат да решават автоматично редица задачи, като се започне от детекция на движения в обхвата на видеонаблюдението и се стигне до извършването на точно преброяване на преминалите автомобили или хора (система за преброяване на посетителите).

Системите за видеонаблюдение сами по себе си не са завършени охранителни системи. И когато целта е пълноценна охрана, то успоредно със системата за видеонаблюдение е необходимо да се изгради контрол на достъпа.

Правилно проектирана системата за контрол на достъп гарантира много високо ниво на ефективност, чрез ограничаване на достъпа до контролирания обект.

2. Интегрирани системи за физическа сигурност

Системите за сигурност се проектират с цел ограничаване на достъпа до обекти с ценни предмети и информация, следене и контрол на човекопотока през площите на даден обект, контрол на работно време, сигнализиране при нарушаване на установените ограничения, лесна и недвусмислена идентификация на нарушителя, както и документиране на нарушението. Всяка от гореописаните цели се реализира от отделна подсистема, като всички подсистеми в общият случай образуват цялостна система за сигурност на обекта, като взаимодействат помежду си и обменят информация. [2]

Видовете охранителни системи включват:

- *Сигнално-охранителни системи* - С използването на подобен род системи се цели предотвратяване на злонамерен достъп до площи от обекта или целия обект посредством устройства за детекция на движение в охраняемите обеми, детекция на проникване откъм периферията на обекта чрез охрана на стъклените площи, врати, леки стени и др. След обработка регистрираните сигнали се препращат към организация за централизиран мониторинг за вземане на мерки.
- *Системи за контрол на достъп и работно време* - От една до хиляди врати могат да бъдат контролирани от системите за контрол на достъп. Всеки който трябва да има достъп ще получи карта чрез която по безконтактна технология ще може да получава достъп до желани помещения, през желани дни и в желани часове. Контролирането на работното време на персонала също е лесна задача за системите, които се предлагат, като това е особено подходящо при заплащане по часови ставки.
- *Системи за видеонаблюдение* - Състоят се от взаимодействащи помежду си устройства за заснемане на видеопоток, устройства за събиране и визуализация на изображенията и устройства за запис на получените сигнали. Подобен род системи са незаменими при изграждане на охрана на обекти от голям и среден мащаб с наличие на локална физическа охрана. Тази система изпълнява ролята на „незаспиващи очи“, бдящи 24 часа в денонощието за това, което се случва в критично важните точки от наблюдавания обект [3], [10].

Първоначално сигнално-охранителните системи се изграждат на принципа детектор (регистриращ, обработващ получената вече промяна на състоянието му), захранващо устройство, кабелна линия за пренасяне на сигнала от детектора до релеен комплект

(централна поща), кабелна линия - централна станция, която обработва и визуализира индивидуално получения сигнал. Общата звукова и индивидуална светлинна сигнализация дава възможност на оператора да разбере от кой детектор или малка група детектори е получен сигнала и на тази база да предприеме необходимите действия. Предвид несложното обслужване, така изградени сигнално-охранителни системи все още се използват в практиката.

Развитието на информационните технологии позволи през последните години, да се реализират устройства с много повече и по-сложни функции, които намират приложение и в техническите системи за сигурност. Конкретен пример за това са модерните системи срещу проникване като цяло и контролните им панели в частност, системи за контрол на достъпа и интегрираните системи за сигурност. В почти всички такива системи е реализирана възможност за събиране и запаметяване на огромен обем информация за всички регистрирани събития, в това число и за действията на оперативния състав. Тези действия се улесняват от изграден мониторинг на входни сигнали, позволяващ отличаване на алармата от техническа неизправност или опит за саботаж, придружени с телевизионни системи за наблюдение Много често е предвидена възможност за съвместна работа на няколко системи или за икономиката и отбраната на държавни обекти, разрушаването и повреждането на които, освен големи материални загуби, най-често довежда и до заплаха за здравето и живота на много хора. Едно от средствата за намаляване на тези рискове е охраната по периметъра на такива обекти. Това е трудоемка и скъпа система особено за частния бизнес, но тя е доказала своята ефективност. Съответно събитията, които могат да бъдат регистрирани от една периметрова сигнално-охранителна система, са въоръжено нападение, терористична акция, неоторизирано проникване, шпионаж, саботаж, кражба.

Смисълът от използване на периметрова сигнално-охранителна система е във възможността за фиксирането на нарушения при пресичане на периметровата граница, т.е. получаване на информация за нарушение и възможен начин да се спечели време за противодействие. Също така е желателно системата да определя посоката на проникване - отвън навътре или обратно.

Предназначението на системите за контрол на достъпа е да контролира и регулира преминаването на хора и превозни средства. Контрола на достъпа се основава на идентификация на обекта посредством RFID безконтактни карти, пръстови отпечатъци, кодове, маркери за превозни средства или други идентификатори, съобразени с изискванията на клиента.

Системата за контрол на достъпа може да бъде интегрирана с други обхващаща интегрираната система за сигурност като системи за CCTV наблюдение, DVR, защита на периметъра и откриване на нежелателно проникване. Интегрирането се изпълнява посредством серийните портове на елементите на системата, LAN връзка или посредством сухи контакти.

Общите приложения на тези системи се свеждат до:

- Системата контролира влизането в сградата и ограничените зони;
- Идентификацията на оторизирания персонал става посредством доближаване картата до четеца;
- Вратите се заключват посредством електрически насрещници за врати;
- Системата за контрол на достъпа са управлява от работна станция за контрол на достъпа;
- В централната зала за управление се разполагат сървъри за контрол на достъпа и работна станция за управление;

- Сървъра може да бъде използван като платформа за централния управляващ компютър, която да интегрира различни подсистеми;
- Сървъра за контрол на достъпа комуникира с другите подсистеми.

Системите за контрол на достъпа включват следните елементи:

- Сървър за контрол на достъпа;
- Контролер;
- Четец за безконтактни карти;
- Електромагнитен насрещник за врати;
- Пропускни съоръжения;
- Потребителски софтуер;

Модел за интегрирана система за наблюдение и контрол

Предложената интегрирана система за наблюдение и контрол обединява функциите на три типа подсистеми:

- система за видеонаблюдение;
- система за контрол на достъпа;
- система за периметрова охрана.

Работата на трите подсистеми се контролира от специализиран софтуер за наблюдение и контрол. В интегрираната система е предвидена обратна връзка, чрез система за автоматично генериране на гласови съобщение при навлизане в зони за видеонаблюдение, преминаване през периметрова охрана, достъп или опит за достъп до зони контролирани от системите за контрол на достъпа [10], [12].

Архитектурата на интегрираната система за наблюдение и контрол е представена на фигура 1.

Интегрираната система включва четири системи за периметрова охрана, две системи за видеонаблюдение и четири системи за контрол на достъпа.

Интегрираната системата е проектирана за работа със системи за периметрова охрана с релеен изход / инфрачервени, микровълнови бариери, външни детектори и т.н /. Релейният изход на всяка система за периметрова охрана е свързан с контролера.

Системите за видеонаблюдение подават информация за достъп в дефинирани зони, чрез функция детекция на движение, посредством релейни алармени изходи.

Системите за контрол на достъпа осъществяват комуникация със специализирания софтуер по сериен асинхронен комуникационен канал RS485.

Разработеният за системата контролер, по заявка от специализираният софтуер, сканира входовете, към които са включени системите за периметрова охрана и видеонаблюдение, и предава състоянието им. Идентификация за състоянието на конкретно устройство се осъществява по номера на съответният вход.

Чрез контролера, специализираният софтуер, последователно сканира системите за контрол на достъпа и при наличие на представени идентификатори получава идентификационните им кодове.

Фиг. 1. Архитектура на интегрирана система за наблюдение и контрол

Алгоритъма на работа на интегрираната система е следния:

1. Специализираният софтуер изпраща запитване към контролера за състоянието на включените към него устройства.
2. Контролерът сканира състоянието на входовете, пакетира получената информация и я изпраща към софтуера.
3. При наличие на навлизане в дефинирана зона за видеонаблюдение се генерира и излъчва гласово съобщение за навлизане в съответната зона. Генерира се алармено съобщение към оператора. Събитието се архивира в база данни.

4. При преминаване през периметрова охрана се генерира и излъва гласово съобщение за навлизане в охраняема зона. Генерира се алармено съобщение към оператора. Събитието се архивира в база данни.

5. Специализираният софтуер сканира последователно системите за контрол на достъпа. При наличие на представен идентификатор проверява в база данни дали е оторизиран за допускане до контролираната зона. При оторизиран индикатор се генерира и излъчва гласово съобщение със съдържание данни за идентификатора. При представен неоторизиран идентификатор се генерира и излъчва гласово съобщение за неразрешен достъп. Събитието се архивира.

6. Преминава се към точка 1.

В конкретна реализация са използвани следните устройства:

- Двулъчева инфрачервена бариера ABT – 100;
- Четириканален DVR DS – 7204HVI –ST;
- Четец на 125 kHz, 64 битови безконтакти идентификатори, разработен за интегрираната система за наблюдение и контрол.

Контролера е базиран на микроконтролер PIC18F4550. Използвана е среда за програмиране MPLABX с компилатор XC8.

Специализираният софтуер е разработен в IDE Lazarus.

ЛИТЕРАТУРА:

[1] Асоциация „Прозрачност без граници”, Индекс за възприятие на корупцията за 2016г., http://transparency.bg/bg/transp_indexes/.

[2] ДКСИ, Методика за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация. София (2012).

[3] Слатински Н., Сигурността — същност, смисъл, съдържание. Военно издателство, София (2011), 34.

[4] Лалев, Хр., Системи за видеонаблюдение. Тр. (2008), 76.

[5] Лалев, Хр., Системи за физическа сигурност. Шумен (2013).

[6] https://www.jmt.bg/productfiles/7490_79.pdf

[7] https://www.hikvision.com/UploadFile/image/2012061414262946905.pdf

[8] http://ww1.microchip.com/downloads/en/DeviceDoc/39632D.pdf.

[9] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[10] Фетфов, О., Боянов, П., Николов, Ив., Ташева, Ж., Трифонов, Т., Сравнителен анализ на съвременните видове безжични IP видеокамери в компютърните мрежи за наблюдение и контрол, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 143-149.

[11] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[12] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

Име на автора: гл. ас. д-р инж. Димитър Георгиев Чобанов
Месторабота: НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, гр. Шумен
E-mail: chobanov.d@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 74 - 78 Problems of Security Systems

AN ALGORITHM FOR QUICK SEARCH OF IDENTIFIERS IN AN ACCESS CONTROL SYSTEM

DIMITAR G. CHOBANOV

ABSTRACT:. *An algorithm for the fast reading of identifiers is described. It is based on a hash table with the use of the method for handling collisions "Hashing with Chaining".*

KEYWORDS: *Access control, RFID, Hash table.*

АЛГОРИТЪМ ЗА БЪРЗО ТЪРСЕНЕ НА ИДЕНТИФИКАТОРИ В СИСТЕМА ЗА КОНТРОЛ НА ДОСТЪПА*

ДИМИТЪР Г. ЧОБАНОВ

АБСТРАКТ: *Представен е алгоритъм за бързо търсене на идентификатор в система за контрол на достъпа. Алгоритмът е базиран на хеш - таблица с използване на метода за решаване на колизии „нареждане в списък".*

1. Въведение

В системите за контрол на достъп, проектирани за голям брой потребители, използването на метода на последователното търсене води до неприемливо увеличаване времето за идентификация. За решаването на този проблем е необходимо използването на алгоритми съкращаващи времето за търсене и добавяне на идентификатори в локалната база данни [3].

В докладът е представен алгоритъм, имплементиран в четец на 64 – битови RFID идентификатори, с капацитет 4000 потребителя.Алгоритмът е базиран на хеш таблица. За решаване на проблема с колизиите е приложен метода „нареждане в списък" (chaining) [1].

2. Алгоритъм за бързо търсене на идентификатори в системи за контрол на достъпа

При разработване на алгоритъма е взет под внимание обема от данни, съхранявани за всеки потребител, необходими за проектираната функционалност на системата за контрол на достъпа/четецът за безконтактни чип – карти/. Предвидена е възможността за рестрикция на достъпа и по време [2], [3], [4], [5]. Ограничението по време се осъществява, чрез задаване на времеви прозорец, асоциран към всеки идентификатор. Рестрикцията по време може да се организира в седмичен цикъл. Така в база данни за всеки потребител се съхраняват осем байта идентификационен код, два байта „начален час", два байта „краен час", един байт „дни от седмицата", четири байта резервирани за бъдещи разработки, два байта указател необходим за реализиране на метода за решаване

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

на колизии „нареждане в списък“. Картата на паметта за всеки потребител е представена чрез Таблица 1. Адресите са относителни [1], [2].

Таблица 1. Карта на паметта на данни за потребител

Адрес	Наименование	Предназначение
Start_Address	Card_ID_0	Идентификационен код
Start_Address + 1	Card_ID_1	Идентификационен код
Start_Address + 2	Card_ID_2	Идентификационен код
Start_Address + 3	Card_ID_3	Идентификационен код
Start_Address + 4	Card_ID_4	Идентификационен код
Start_Address + 5	Start_Hour	Начален час – час
Start_Address + 6	Start_Minute	Начален час - минута
Start_Address + 7	End_Hour	Краен час – час
Start_Address + 8	End_Minute	Краен час - минута
Start_Address + 9	Days_Of_Weak	Дни от седмицата
Start_Address + 10	Reserved	Резервиран
Start_Address + 11	Reserved	Резервиран
Start_Address + 12	Reserved	Резервиран
Start_Address + 13	Reserved	Резервиран
Start_Address + 14	Old_Pointer_High_Byte	Указател – старши байт
Start_Address + 15	Old_Pointer_Low_Byte	Указател – младши байт

Общия обем памет използван от алгоритъма е 65024 байта. Паметта е разделена на три секции както следва:

- Map_Allocate – с обем 512 байта
- Hash_Table – с обем 512 байта
- Users_Table – с обем 64000 байта

Секторът Map_Allocate изпълнява функциите на карта на разпределение на паметта за потребители / Users_Table /. Съобразно проектираният капацитет на системата за контрол на достъпа, алгоритъмът използва 4000 байта, номерирани последователно от 0 до 3999. На всеки бит съответства фрагмент от секция Users_Table с обем 16 байта съгласно Таблица 1. Логическа нула записана в бит от Map_Allocate указва, че кореспондиращият фрагмент от Users_Table е свободен за запис на данни. Съответно логическа единица указва, че в сектора са съхранени валидни данни за потребител.

Секторът Hash_Table съхранява вектори към Users_Table. Векторите се изчисляват на базата на данните записани в сектор Map_Allocate. Дължината на вектора е два байта и кореспондира с проектирания капацитет на системата за контрол на достъпа. Адресът на клетките от паметта, в които се записва стойността на всеки вектор, се изчислява чрез осем битова хеш – функция с входен параметър пет – битов идентификатор.

В секторът Users_Table се съхраняват данните за потребителите. Картата на паметта използвана от описаният алгоритъм е представена чрез таблица 2.

Таблица 2. Карта на паметта

0x0000	Map_Allocate
• • •	• • •
0x0200h	Hash_Table_
• • •	• • •
0x03FEh	Hash_Vector_High_255
0x03FFh	Hash_Vector_Low_255
0x0400h	Users_Table
• • •	• • •
0xFDF0h	ID_4000[0]
0xFDF1h	ID_4000[1]
0xFDF2h	ID_4000[2]
0xFDF3h	ID_4000[3]
0xFDF4h	ID_4000[4]
0xFDF5h	Start_Hour
0xFDF6h	Start_Minute
0xFDF7h	End_Hour
0xFDF8h	End_Minute
0xFDF9h	Days_Of_Weak
0xFDFah	Reserved
0xFDFBh	Reserved
0xFDFCh	Reserved
0xFDFDh	Reserved
0xFDFEh	Hash_Vector_High
0xFDFFh	Hash_Vector_Low

Видно от Таблица 2 секторът Map_Allocate е с начален адрес 0x0000. Заема 512 клетки до адрес 0x01FF.

Секторът Hash_Table е с начален адрес 0x0200 и заема клетки до адрес 0x03FF. Клетки 0x0200 и 0x0201 съдържат стойността на първият вектор / с индекс 0 /. Клетки 0x03EF и 0x03FF – векторът с индекс 255.

Секторът Users_Table е с начален адрес 0x0400 и краен адрес 0xFDFF. Клетки с адреси от 0x0400 до 0x040F съдържат данните за потребител с индекс 0. Клетки с адреси 0xFDF0 до адреси 0xFDFF – данните за потребител с индекс 3999.

Така направеното разпределение на паметта е съобразено с изискванията при адресиране в режим запис на използваната физическа памет / режим Page Write при I2C EEPROM памети/.

Алгоритмът за бързо търсене на идентификатори използва осем битова хеш – функция с образуващ полином $x^8 + x^5 + x^4 + 1$ / CRC Dallas/Maxim / [2].

Посочената хеш – функция връща стойност от 0 до 255. В описаният алгоритъм е имплементирана с входен параметър пет - байтов идентификационен код /

идентификационен код на RFID идентификатор /. Изчислява се стойността Hash_Address по формула (1):

(1) Hash_Address = Hash (ID)*2

където:

- Hash – хеш – функция
- ID – пет байта идентификационен код

Изчисленият по формула (1) Hash_Address е началният адрес на две клетки от сектора Hash_Table, в който се записва стойността на двубайтов вектор / Hash_Vector / към област от сектор Users_Table / данни за потребител /. Стойността на записаният вектор се изчислява на базата на анализа на данните записани в сектор Map_Allocate, Изчислява се по следната формула:

(2) Hash_Vector = Byte_Number*8 + Bit_Position

където:

- Byte_Number – поредния номер на байта съдържащ стойността на кореспониращ към Users_Table бит
- Bit_Position – позиция на бита в съответния байт

При запис и търсене на данните за потребител чрез кореспондиращият идентификатор се изчислява адресът на областта от секция Users_Table, в която се съхраняват съответните данни. Адресът User_Address в сектор Users_Table се изчислява по формула (3):

(3) User_Address = 00400h + Hash_Vectror*16

Коефициентът 16 във формула (3) кореспондира с обема информация съхранявана за всеки потребител.

Алгоритъм за бързо търсене на идентификатори включва следните подалгоритми /модули /:

- Инициализация / Нулиране /
- Добавяне на потребител
- Намиране на идентификатор
- Изтриване на идентификатор

Използва се глобална променлива „Old_Vector“

Модул „Инициализации“ изпълнява следната софтуерна последователност:

- в сектора Map_Allocate се записват 512 байта със стойност 00h
- в сектора Hash_Table се записват 512 байта със стойност FFh

Модулът „Добавяне на потребител“ се изпълнява по алгоритъма:

1. Локализация на първият бит със стойност логическа нула и изчисляване на Hash_Vector съгласно формула (2)
2. Изчисляване на User_Address съгласно формула (3)
3. Изчисляване Hash_Addres съгласно формула (1)
4. Прочитане на Hash_Vector от Hash_Table, записан на адрес Hash_Addres

5. Запис на ID[0] ÷ ID[4], Start_Hour, Start_Minute, End_Hour, End_Minute, Reserved_ Bytes , Hash_Vectop, в Users_Table, на адрес User_Address
6. Запис на Hash_Vector, изчислен в точка 1, в Hast_Table на адрес Hash_Address изчислен в точка 3

Модулът „Намирането на идентификатор“ се осъществява по алгоритъма:

1. Изчисляване на Hash_Address съгласно формула (1).
2. Прочитане на Hash_Vectror от Hash_Table записан на адрес Hash_Address.
3. При стойност на Hash_Vector = FFFFh преминаване към край на алгоритъма със съобщение Hash_Vector = FFFFh.
4. Изчисляване на User_Address съгласно формула (3).
5. Сравняване ID на търсеният идентификатор с ID записан адрес User_Address в Users_Table.
6. При съвпадение преминаване към край на алгоритъма със съобщение Hash_Vector на намерения идентификатор.
7. При липса на съвпадение се прочита Hash_Vector, записан в Users_Table за текущия идентификатор. В глобална променлива Old_Vetcor се записва прочетеният Hash_Vector.
8. Повтарят се точки 3 до 7 до регистриране на съвпадение или до прочитане на Hash_Vector със стойност FFFFh / търсеният идентификатор не е намерен/.

Алгоритмът за изтриване на идентификатор е следния:

1. Изпълнява се алгоритъмът за търсене на идентификатор.
2. При съобщение FFFFh се преминава към край на алгоритъма.
3. При съобщение различно от FFFFh се прочита Hash_Vector записан в Users_Table за намереният идентификатор.
4. При стойност на Old_Vector = FFFFh се изчислява.
   Hash_Address по формула (1) с ID на подлежащия на изтриване идентификатор.
   На така изчисленият адрес, в Hash_Table се записва Hash_Vector от точка 3
5. Съответсващия на Hash_Vector от точка 3 бит в Map_Allocate се нулира.
6. При стойност на Old_Vector различна от FFFFh се изчислява User_Adress по формула 3) със стойност на Hash_Vector = Old_Vector. В Users_Table се записва стойноста на Hash_Vector.
7. Изпълнява се точка 5.

ЛИТЕРАТУРА:

[1] http://opendatastructures.org/ods-cpp/5_1_Hashing_with_Chaining.html.

[2] https://www.maximintegrated.com/en/app-notes/index.mvp/id/27.

[3] Fetfov O., Bedzhev B., Mutkov V.,“Algorithms for synthesis of signals for radars, based on space crafts”,“Aerospace Research in Bulgaria”, No 22.

[4] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[5] Начев А. И., Надеждност на програмното осигуряване На примера на програмни системи и комплекси, Шумен, Университетско издателство „Епископ Константин Преславски“, 2017.

Име на автора: гл. ас. д-р инж. Димитър Георгиев Чобанов
Месторабота: НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, гр. Шумен
E-mail: chobanov.d@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 79 - 84 Problems of Security Systems

THE EUROPEAN CIVILIZATION DISCOURSE AND THE SECURITY

DOBROMIR ZH. DOBREV

ABSTRACT: *Will the elites of Europe to respond to the challenges? Can Europe from itself to become an economic giant in the global political factor? Can you combine the democratisation in the individual European countries with the intensification of integration processes?*

KEYWORDS: *Europe, economic, democratization, intensification.*

ЕВРОПЕЙСКИЯТ ЦИВИЛИЗАЦИОНЕН ДИСКУРС И СИГУРНОСТТА[1]

ДОБРОМИР Ж. ДОБРЕВ

АБСТРАКТ: *Пътищатаq, по който Обединена Европа може да поеме днес са разнопосочни и това поставя много въпроси. Можем ли да изградим достоверна хипотеза за предстоящите решения или поне да направим опит за такава ? Когато се опитваме да градим предположения е много важно на каква основа правим това. Фундамента на европейската интеграция е нашата отправна точка. Всъщност това е и въпрос на който трябва да отговорим. Какъв е този фундамент, достатъчно устойчив ли е той и съотносим ли е с всички европейски държави ?*

1. Въведение

Когато се опитваме да градим предположения е много важно на каква основа правим това. Фундамента на европейската интеграция е нашата отправна точка. Всъщност това е и въпрос на който трябва да отговорим. Какъв е този фундамент, достатъчно устойчив ли е той и съотносим ли е с всички европейски държави?

Започнатото от Европа след Втората световна война, е уникално усилие да прекъсне лошата безкрайност на конфликтите. За наднационалната демокрация европейците нямаха рецепта или изпитан модел. Това беше скок в бъдещето, без аналог в историята.

„Ако европейското демократично бъдеще не е никак ясно, това се дължи, както вече казах, на липсата на модел – ако гръцкият полис ни дава ограничен опит за изграждането на национални държави, то историческият процес на изграждане на национални държави не ни служи аналогично, при изграждането на наднационална демокрация. Обратно на националните държави, изградени въз основа на насилие и принуда, навътре и навън, европейският градеж се характеризира с това, че е мирен и консенсусен проект, който желае да бъде съвместим с националните институции и идентичности“[2].

Ще се опитам, доколкото е възможно, да избягам от термина „западна цивилизация“, придържайки се към един цялостен поглед за Европа. Понякога използването на западна цивилизация като синоним на европейска е изкушаващо, но не винаги е коректно. Ясно е, че дуализма на Изтока и Запада е факт, включително в религиозно отношение. Но дори и в този случай имаме обща основа от която се развива християнската църква.

---

[1] Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.
[2] Торебланка, Х. Кой управлява в Европа? С., 2015, 29-30.

Напълно споделям тезата на Норман Дейвис, че използването на Западна цивилизация, не дава пълнота в разбирането за европейската история и цивилизация. Нещо повече „тази концепция е крайно смаляваща и безсрамно селективна“[3].

2. Изложение

Европейските ценности изграждащи основата на обединението предполагат да са в началото на всеки разговор за бъдещето на континента. Техният генезис и развитието им ще бъде проследено и анализирано. Тук възниква и още един въпрос, а именно как да определим европейското и неговите характеристики?

„В миналото не са липсвали опити за изясняване на духовното и културно измерение на Европа. Така след Първата световна война поетът и есеист Пол Валери предложи една интерпретация, която получи немалък отзвук. Наричам европейски, казвал по същество Валери, народите които в хода на своята история са претърпели три големи влияния, чиито символи бихме могли да отъждествим с градовете Рим, Йерусалим и Атина. От Рим идва империята с организираната държавна власт, правото и институциите, статусът на човека като гражданин. От Йерусалим, или по-скоро от християнството, европейците са наследили субективния морал, съда над собствената си съвест, универсалната справедливост. Най-сетне Атина им е завещала вкусът към познанието и към рационалната аргументация, идеала за хармония, идеята за човека като мярка за всички неща. Който се позовава на това тройно наследство, заключава Валери, може с право да се смята за европеец“4.

Много пъти ще се връщаме към изворите на европейската идентичност. Те са фундамента на който стъпваме в опитите за анализ.

Появата на Европа е свързана с една легенда. Но дори в нея можем да открием рационални моменти. Белият бик откраднал любопитната принцеса от Финикия, я отвежда на Запад, на остров Крит. Такова е движението на гръцката култура, от Изток на Запад, изграждайки ядрото на това което наричаме Европа.

Не трябва да се пропуска и факта, че европейските ценности отдавна са излезли от рамките на Стария континент и са се превърнали в евроатлантически ценности. Най-близките партньори и съюзници на Европа са именно страните споделящи тези ценности – САЩ, Канада, Австралия и др. Отношенията с тях са особено интересни когато анализираме устойчивостта и бъдещето на Стария континент.

Тук трябва да припомним и това което винаги е различавало Европа от всички останали, а именно плурализма и факта, че определена теза не е успявала да потисне или още повече да смачка другите възгледи и идеи. Дървото на европейската мисъл винаги е било обилно разцъфнало, с много разклонения и разнообразни плодове. Осъществяването на Великите географски открития през XV век, Просвещението от XVIII век и научните революции век по-късно, поставят Европа на върха на световното господство. Няколко европейски държави владеят света, нямат реален конкурент и тази безпрецедентна мощ им изиграва лоша шега. Когато те влизат в конфликт помежду си, по време на двете световни войни, се оказва, че няма сила която с намесата си да играе балансираща или възпираща роля. Същественият въпрос е защо големите играчи в Европа влязоха в самоубийствен конфликт, след дълъг период на икономически и социален просперитет? Ще се опитаме да погледнем малко встрани от традиционните исторически отговори на този въпрос.

[3] Дейвис, Н. Европа Изток и Запад. В. Търново, 2007, с. 49.
[4] Цит. по: Тодоров, Цв. Страхът от варварите. С., 2009, с. 250-251.

Не трябва да ни убягва обаче, че в Европа присъства и друг голям играч, за който няма как да твърдим, че споделя евроатлантическите ценности. Русия е част от проблемите на Европа, но би могла да стане и част от решението на тези проблеми. Активизирането на Русия след като властта там беше поета от Владимир Путин, ясно показа, че страната иска да върне статута си на глобална сила от времето на СССР. В тази връзка динамиката на руската външна политика, прерастваща на моменти в агресия (Грузия, Крим, Източна Украйна…), и откровената хибридна война която страната води, предполагат да се отдели достатъчно внимание на тази тема.

Не може да не се забележат и процесите в Централна и Източна Европа, където постепенно либералните идеи отстъпиха пред националистически и антиевропейски тенденции. Задружният отказ на източноевропейците да приемат мигранти по време на бежанската криза поставиха много въпроси пред единството на Съюза. Европа без граници за която толкова дълго говорихме и мечтаехме се оказа неподготвена за подобна криза.

Появата на лидери като Виктор Орбан в Унгария, също е предизвикателство пред европейската интеграция и нейната либерална основа. Една от характерните реплики на Орбан, че „демокрацията не е задължително да бъде либерална“, и нейното продължение, че „само защото нещо не е либерално, не означава, че то не може да бъде демокрация"5, са показателни за настроенията в тази част на света. За отношенията между Запада и Изтока на Европа в наши дни, и процеса на тяхното опознаване може да се напише отделно съчинение. Целта на статията е по-скоро да покаже необратимостта на обединителните тенденции след Втората световна война, и общото бъдеще на Европа.

Тази цел няма да ни попречи да изброим и много, надявам се преодолими, препятствия към Обединена Европа.

Когато към мигрантската вълна и явната неподготвеност на Европа да се справи добавим злополучният референдум във Великобритания довел до Брекзит, и опитите на Каталуния да получи независимост от Испания, картината наистина добива тъмни краски.

Не трябва да пропускаме и това което се случи с европейската икономика преди няколко години и според мен беше в основата на последвалите центробежни процеси. Става дума за дълговата криза, която постави на изпитание европейската солидарност. Макар, че проблеми имаха всички държави от южния фланг на еврозоната, най-ясно те кристализираха в Гърция. Големите дългове и невъзможността страната да ги обслужва изправиха на нокти евробюрократите и катализираха редица процеси. Христо П. Тодоров ни дава ясна картина на диалектиката в тези процеси: „Широко тиражираните в публичността на много европейски страни настойчиви искания за излизане на Гърция – страната с най-големи фискални задължения – от еврозоната са недвусмислен сигнал за това, че солидарността на европейските народи с Гърция е много близка до своите предели. Тъй като обаче правителствата на страните от еврозоната досега неизменно настояват въпреки всички свой задължения Гърция все пак да остане в еврозоната, неизбежно между правителствата и нагласите и настроенията на избирателите възникват напрежения. Така се откриват възможности за натрупване на политическо влияние на иначе маргинални национал-популистки партии. Получават шанс откровени антиевропейски идеи и програми. Появяват се рискове за политическата стабилност в отделни страни“6.

---

[5] Врагът отвътре: Защо Централна Европа предизвиква ЕС? https://www.dnevnik.bg/evropa/2018/04/28/3167496_vragut_otvutre_zashto_centralna_evropa_predizvika_es/.

[6] Тодоров, Хр. Политическа интеграция и солидарност в Европейския съюз. – В: Дискурсът за Европа. С., 2013, 67–68.

Тук се изкушавам да припомня интересният поглед на Юрген Хабермас, който видя нови възможности пред Европа дори по време на кризата с общата валута.

„Чрез малко политическа опора кризата на общата валута може да породи това, на което някога малцина се надяваха и очакваха от една обща европейска външна политика: надскачащо националните граници съзнание, че споделят обща европейска съдба“7.

Съзнанието за Европа като наш общ дом, е факт който се противопоставя на заразните националистически тенденции.

Въпросът пред който сме изправени е дали различните кризи не ерозират постепенно европейската идея за обединение? Коментари за това не липсваха и множество спекулации чертаеха мрачни картини. Може би Европа за пореден път не си беше научила урока по история?

Двете световни войни и кървавите идеологически конфликти през XX век съсипаха Стария континент – икономически, политически, демографски. От световни лидери западноевропейските държави се превърнаха в нуждаещи се от помощ страни с разрушена инфраструктура.

Създаването на Европейският съюз имаше огромната амбиция да не допуска нов конфликт на континента, до обедини враждуващите от столетия Германия и Франция, да възроди икономиката и надеждите на милиони европейци. Никой не може да отрече успехите на Съюза, който за няколко десетки години изпълни много от надеждите който му възлагаха. Трудът на следвоенното поколение и помощта на американците посредством плана Маршал отново върна Европа в авангарда на цивилизацията, където тя неотлъчно присъства още от времето на Великите географски открития.

По-парадоксален начин, обаче именно когато се радваше на просперитет и значително разширяване към Централна и Източна Европа, Европейският съюз загуби инерцията си, започна да изпитва недостиг на солидарност и залитане към добре познатото заболяване на национализмите. Можеше ли за пореден път национализма да пресече обединителните процеси в стария свят?

Аз съм уверен, че този дискурс заслужава да бъде подробно анализиран в контекста на европейската история и да се подчертае пряката му връзка с опустошителните конфликти на континента.

В противовес на мрачните прогнози, реалността беше по-различна. Слуховете за смъртта на Европейския съюз се оказаха силно преувеличени. В своето годишно обръщение председателя Жан-Клод Юнкер, опирайки се на високият ръст на икономиката в стария континент, недвусмислено заяви: „… вярвам, че попътният вятър отново издува платната на Европа. Пред нас се откриват възможности, с които няма да разполагаме завинаги. Нека да използваме импулса и да уловим попътния вятър!“ 8.

Наистина ли попътния вятър ще отведе Обединена Европа към мира и благоденствието за нейните граждани или споровете и разногласията ще продължат? Най-вероятно, познавайки историята и традициите на Стария континент, ще наблюдаваме развитието и на двете тенденции.

В годините след като изложи идеята си за краят на историята Франсис Фукуяма беше критикуван, че последвалите събития го опровергават. Дали обаче тези критикари имат основания и дали времевия хоризонт не е твърде кратък за да произнасяме присъди е нещо над което може да се разсъждава. Наистина днес изглежда, че самата Европа, а и САЩ на Доналд Тръмп не са толкова активни в претенциите си да бъдат глобален модел

[7] Хабермас, Ю. За конституцията на Европа. Опит. С., 2011, с. 169.

[8] Обръщение за състоянието на Съюза 2017 г. file:///C:/Users/d.dobrev/Downloads/SPEECH-17-3165_BG.pdf (2.12.2017).

на подражание. Нещо повече в риториката на Тръмп могат да се уловят много моменти на изолационизъм, който звучи достатъчно непривично за съвременната американска политика.

Но ако западния модел е в криза и останалият свят не го припознава като свой, как да обясним милионите емигранти който всяка година гласуват с краката си поемайки трудният път към Европа, САЩ, Канада и други „загниващи“ либерални демокрации. Ясно е, че днес е много по-лесно да отидеш да живееш там където ти харесва отколкото с революция да променяш своята собствена страна. Тази тенденция създава мигрантски натиск върху Европа и плаши нейните граждани. Елитите на Стария континент трябва да намерят баланса между тези страхове и необходимостта от свежа работна ръка за застаряващите европейски общества. Това е предизвикателство на което управляващите в Европа трябва да реагират.

И още нещо което се отрази достатъчно мобилизиращо на хората с европейски избор. Дълги години всички гледаха на ЕС и на интеграционните процеси като неотменима даденост. Икономическата криза, дълговите проблеми на Гърция, имиграцията, тероризма, Брекзит, възраждането на национализмите и много други фактори показаха, че Обединена Европа не е природна даденост и десетките години интеграция могат да бъдат унищожени. Това без съмнение подейства отрезвяващо на големи групи от хора в европейските страни. В същото време европейските елити получиха време, не кой знае колко но все пак някаква отсрочка, за да реагират на предизвикателствата.

Много актуално ми прозвуча примера който дава Иван Кръстев с австро-унгарският експеримент като либерално, мултикултурно обединение в Европа. Краят на Хабсбургската империя в началото на XX век, предизвиква у автора на „След Европа“ усещане за déjà vu 9. Възможно ли е неуспехът на тази империя, опитала да обедини хора от различни националности в едно достатъчно либерално за времето си общество, да е показателен за съдбата на Европа през XXI век?

Едно такова предположение може се подкрепи с тезата на руският философ Николай Бердяев, че всички опити за универсално обединение, включително и най-великият – Рим, в края на краищата се превръщат във велики провали10.

В случая нашата задача не е да проследяваме есхатологическият смисъл който Бердяев придава на разсъжденията си. Важното е да разберем, дали историческият опит на континента му дава шанс да излезе от лошата безкрайност на войни и революции.

Фактът, че предизвикателството е огромно, има и своите добри страни. Например подплатеното с много примери твърдение на Арнълд Тойнби, че трудната среда стимулира развитието11. Ако останем при Тойнби, можем да посочим и закона за предизвикателството и отговора. Развитието на всяка цивилизация се определя от способността на нейните граждани да реагират на предизвикателствата на историята. Ако реакцията не е адекватна, в обществото възникват аномалии. Когато елитите не могат да решават проблемите, когато използват насилие, в обществото настъпва „разединение на духа“. Тези процеси се отразява силно върху т.н. „вътрешен пролетариат“12 .Това са хората отхвърлили, отчуждили се от доминиращото малцинство. Като такъв вътрешен пролетариат днес могат да се посочат всички живеещи в развитите държави, вкл. и в Европа, но останали встрани от процесите на глобализацията. Те не могат да се възползват

[9] Вж.: Кръстев, И. След Европа. С., 2017, с. 7.
[10] Вж.: Бердяев, Н. Смисълът на историята. – В: Новото средновековие. Т. 2. С., 2003, с. 411.
[11] Тойнби, А. Изследване на историята. Т. 1. С., 1995, с. 154.
[12] Пак там, с. 43.

от предимствата която тя дава на добре образованите и мобилни съсловия. Точно хората ощетени от глобалните процеси гласуваха за Брекзит и избраха Доналд Тръмп за президент на САЩ.

3. Заключение

Ако направим още една аналогия със съвремието, такива аномалии които водят до системно отчуждаване на гражданите от техните елити са скандалите от рода на скритите офшорни сметки в разследванията, добили известност като „Панама пейпърс“/2016 г./ и „Парадайз пейпърс“/2017 г./ . Въпреки коментарите, че в повечето случаи формално законите не се нарушават, скриването на сметки и спестяването на данъци от корпорации, публични фигури и държавници предизвиква огромна морална ерозия в обществото.

Ще успеят ли елитите на Обединена Европа да реагира на предизвикателствата? Може ли самата Европа от икономически гигант да се превърне и в глобален политически фактор? Може ли да се съчетае демократизацията в отделните европейски държави със засилването на интеграционните процеси? Въпросите са много, както са много и посоките в който се търсят отговорите.

В настоящият момент ЕС стои пред две възможности. Едната е връщане назад към „Европа на отечествата“ и национализмите. Другата е намирането на един модерен и гъвкав федерализъм, гарантиращ способността на стария континент да запази просперитета и сигурността си.

ЛИТЕРАТУРА:

[1] Бердяев, Н. Смисълът на историята. – В: Новото средновековие. Т. 2. С., 2003

[2] Дейвис, Н. Европа Изток и Запад. В. Търново, 2007

[3] Кръстев, И. След Европа. С., 2017

[4] Торебланка, Х. Кой управлява в Европа? С., 2015

[5] Тодоров, Цв. Страхът от варварите. С., 2009

[6] Тодоров, Хр. Политическа интеграция и солидарност в Европейския съюз. – В: Дискурсът за Европа. С., 2013

[7] Тойнби, А. Изследване на историята. Т. 1. С., 1995

[8] Хабермас, Ю. За конституцията на Европа. Опит. С., 2011

[9] Врагът отвътре: Защо Централна Европа предизвиква ЕС? https://www.dnevnik.bg/evropa/2018/04/28/3167496_vragut_otvutre_zashto_centralna_evropa_predizvika_es/.

[10] Обръщение за състоянието на Съюза 2017 г. file:///C:/Users/d.dobrev/Downloads/SPEECH-17-3165_BG.pdf (2.12.2017).

Име на автора: професор д-р Добромир Жечев Добрев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: ddobrev68@gmail.com

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 85 - 95 Problems of Security Systems

MODERN TRENDS AND ASPECTS OF THE INFORMATION SECURITY IN THE AUTOMATED INFORMATION SYSTEMS AND NETWORKS

NIKOLAY Y. DOSEV, VELIKO P. PETROV

ABSTRACT: *In this paper a comparative analysis of the purposes and services of the information security in the automated information systems and networks is made.*

KEYWORDS: *Automated information systems and networks Computer networks, Information Security, Modern cyber attacks, Risk management, Software vulnerability, Threat.*

СЪВРЕМЕННИ ТЕНДЕНЦИИ И АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ И МРЕЖИ (АИС/М)*

НИКОЛАЙ Й. ДОСЕВ, ВЕЛИКО П. ПЕТРОВ

АБСТРАКТ: *В тази статия е направен сравнителен анализ на целите и услугите на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М).*

1. Въведение

В тази статия, за да бъде въведено понятието сигурност на информацията, ще бъде първо разгледано по-общото понятие сигурност. Сигурността означава защита на различните видове активи от вреди или щети.

Многобройни са примерите за активи в нашето съвремие. Това са личната собственост, човешкото тяло, околната среда, информацията, нацията, и др. Според вида на активите, които се защитават, се различават следните видове сигурност в автоматизираните информационни системи и мрежи (АИС/М) [1], [2], [3], [19], [20], [21], [22], [23], [24], [29], [30], [31], [32], [33], [34], [35], [36]:

- Безопасност, която е свързана със здравето на отделния човешки индивид. В практиката осигуряването на безопасността означава, че трябва да се спазват съвкупност от норми и правила за предотвратяване на аварии и повреди, както и спасяване на живота на хората при рискови ситуации [10], [27], [28].
- Национална сигурност [1], [2], [3], [4], [17], [18] която е свързана със защита на основните свободи и права на гражданина и човека, политическата стабилност на страната, суверенитета и независимостта на нацията, с ясната цел за увеличаване и запазване на благосъстоянието на държавата и нацията.
- Сигурност на информацията, която е свързана с осигуряване на конфиденциалност, цялостност и наличност на информацията.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

- Сигурност на околната среда, която е свързана с мероприятията и мерките за осигуряване на чиста околна среда.

2. Изложение

Информационна сигурност (сигурност на информацията) в автоматизираните информационни системи и мрежи (АИС/М)

Информационна сигурност (сигурност на информацията) представлява защита на информационните активи от причинени вреди или щети. Най-разпространените примери за информационни активи са специализирани бази от данни, информационно оборудване, файлове с данни, софтуер и инфраструктура. Природата на нанесените вреди или щети може да бъде много разнообразна. Случайни или умишлени, въздействие върху информацията могат да нанесат природни събития или хора [3], [7], [5], [6], [27], [28]. Най-често такива са опитите за компютърно проникване на злонамерени извършители [10], [11], [12], [13], [14], [15], [29] грешки на обслужващия персонал, хардуерно блокиране на програмни и апаратни средства, стихийни бедствия (цунами, земетресение, тайфун, ураган, пожар и т.н.) [2], [27], [28].

По този начин целта на сигурността на информацията е да се прилагат съвкупност от мерки за [2], [7], [8], [9], [10], [11], [13], [14], [16], [30], [31], [32], [33], [34], [35]:

- откриване на повреда на информационните активи и получаване на обратен отговор за това кой е предполагаемият злонамерен извършител.
- предотвратяване на щети на информационните активи [27], [28];
- адекватна реакция и съдействие за възстановяване на щетите на информационните активи.

От по-горе изложеното се установи, че информационната сигурност се състои от защитата на информационните активи от разрушаване или увреждане. В компютърните мрежи и системи информацията се пояснява с трите й състояния: обработка, предаване и съхраняване. По този начин информационните активи се състоят от физически, електронни и човешки устройства за съхранение на информация, електронни или физически носители при предаване на информацията, както и електронни или физически методи и процеси за обработка на информацията [2], [3], [7], [8], [9], [29].

Следователно информационната сигурност е състояние на защитеност на съхраняваните, обработваните и предавани данни от незаконно преобразуване, редактиране, получаване и унищожаване [2], [3], [10] а също така и състоянието на защитеност на информационните ресурси от въздействия за нарушаване на тяхната функционалност и работоспособност.

Информационната сигурност на компютърните мрежи и системи се осъществява чрез прилагане на множество мерки [1], [3], [9] за обезпечаване на цялостност, конфиденциалност, юридическа значимост на информацията, достоверност, оперативен достъп до нея [1], [4], а също така и по обезпечаване на достъпността и цялостността на информационните ресурси и компоненти на компютърните мрежи и системи [2].

Цели и услуги на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)

За правилното и коректно функциониране на една информационна система са необходими петте основни характеристики на информацията [2], [3], [5], [7], [8], [9]:

- отчетност на информацията;

- конфиденциалност на информацията;
- наличност на информацията;
- увереност за приложените политики на сигурност;
- цялостност на информацията.

Отчетност на информацията в автоматизираните информационни системи и мрежи (АИС/М)

Отчетността представлява изискване действията на даден обект или субект да могат да бъдат еднозначно проследени точно с този обект или субект. Отчетността представлява често изискване към политиките за компютърна и мрежова сигурност, като директно осигурява недопускане на спиране, отхвърляне и изолиране на грешки и дефекти, откриване на несанкционирано компютърно проникване и неговото предотвратяване, както и действия за възстановяване и правни действия [1], [3], [11], [12], [13].

Конфиденциалност на информацията в автоматизираните информационни системи и мрежи (АИС/М)

Конфиденциалност на информацията [1], [2], [3], [4], [8], [10], [29] е свойството да бъде достъпна само за точно определен кръг потребители на компютърните мрежи и системи. По този начин конфиденциалността е свойство на информацията да бъде известна само на автентифицирани и оторизирани субекти и обекти [103] на системата (услуги, домейн, програми, процеси, потребители). За всички останали обекти на компютърната система информацията трябва да е неизвестна [2], [14].

Наличност на информацията в автоматизираните информационни системи и мрежи (АИС/М)

Наличност на информацията [1], [2], [3], [4] е свойството да бъде достъпна при поискване от автентифициран и оторизиран потребител на компютърната система. Наличността представлява необходимо изискване, с цел гарантиране, че компютърните мрежи и системи функционират бързо, точно и навреме, както и че няма да се откаже достъп на оторизирани потребители до съответна информационна услуга в компютърната система.

Цялостност на информацията в автоматизираните информационни системи и мрежи (АИС/М)

Цялостността на информацията [1], [2], [3], [4], [14] е свойството да съхранява своето съдържание и структура в процеса на съхранение и предаване. Цялостността на информацията се обезпечава в случая, когато данните в компютърната система не се различават в семантическо отношение от данните в изходния електронен документ, т.е. ако не е направена преднамерена или случайна промяна или разрушение на данните. Цялостността се състои два в важни аспекта цялостност на системата и цялостност на данните.

Цялостност на системата в автоматизираните информационни системи и мрежи (АИС/М)

Това представлява свойство показващо, че компютърната система извършва своите задачи и функции по безупречен начин, без наличието на неоторизирана намеса.

Цялостност на данните в автоматизираните информационни системи и мрежи (АИС/М)

Това представлява свойство илюстриращо, че данните не са променени по несанкциониран начин по време на тяхната обработка, съхранение или предаване.

Цялостността представлява втората по важност цел на компютърната и мрежова сигурност на всяка една организация след наличността [2], [3], [11], [13].

Увереност за приложените политики на сигурност в автоматизираните информационни системи и мрежи (АИС/М)

Увереността се намира в основата на убедеността и това означава, че предприетите мерки за компютърна и мрежова сигурност, както оперативни, така и технически, се изпълняват според своето предназначение [3], [11]. [17], за да се защити информацията и компютърната система, която се обработва в нея. Другите четири цели на компютърната и мрежова сигурност (конфиденциалност, отчетност, наличност, и цялостност) са реализирани от конкретното приложение, когато [1], [2], [3], [4], [5], [6], [25], [26]:

- има достатъчно противодействие на умишлено заобикаляне или компютърно проникване;
- съществува достатъчна защита срещу неволни грешки от потребителите на инсталирания приложен софтуер или компютърната система;
- изискваната функционалност е налице и се извършва коректно и точно.
- увереността е от важно значение за компютърната сигурност, защото без нея другите цели няма да бъдат реализирани [2], [3], [12].

Определяне на основните контроли на сигурността

При процеса на изграждане и реализация на политика за компютърна и мрежова сигурност компютърните специалисти и администратори трябва да определят какъв ще бъде крайният постигнат резултат. Повечето корпорации, компании, частни фирми и държавни учреждения имат за цел да защитават хостовете, като само инсталират базови защитни стени, но без да разучават важни изисквания, норми, нива, мерки и цели на компютърна и мрежова сигурност. Екипите от компютърни специалисти, вземащи участие и принос в процеса на проектиране и реализация на компютърни и мрежови защитни механизми, са длъжни да предложат ефективни идеи и решения за конфигуриране на защитните стени [1], [3], [9], [10], [11], [14], [15]. При евентуално добавяне на нов защитен механизъм компютърните специалисти и администратори трябва винаги да се съобразяват с общите цели за сигурност [2], [3], [29], [32], [33], [34], [35].

Създаването на строго определена защитна основа в цялата организация намалява риска от бъдещи сериозни промени в политиките на сигурност [3], [16], [17].

Компютърният специалист по сигурността е директно отговорен за управлението и контрола много параметри на програмата за сигурност. Според големината на организацията, секторът или администрацията по сигурността може да включва един човек или няколко лица, работещи по децентрализиран или централизиран метод [2], [3], [13], [14]. Независимо от броя на работещите в сектора за сигурност е необходимо всеки специалист да дава отчети, да следи и тества всички приложени защитни механизми на съответното ниво на достъп. При редовна и правилна комуникация между отделните специалисти се гарантира осигуряване на сигурност на всички нива и намаляване на риска от злонамерени кибератаки [4], [14].

Собствениците на информационните ресурси са длъжни да определят кои други потребители да имат достъп до техните информационни ресурси. Препоръчително е даването на права само за четене на електронните ресурси. В случай че даден потребител поиска изпълнение на файл и програма, тогава собственикът трябва да прецени дали си заслужава риска да се дадат повече права на този потребител и какви ще бъдат евентуалните последствия за сигурността на системата [4], [9], [11], [12], [13]. За осъществяване на директивите за управление на сигурността се използват следните защитни контроли [2], [14], [15], [17], [25], [26], [37], [38].

Административен контрол

- Административният контрол се изразява в [2], [3]:
- управление и намаляване на риска;
- проучване на персонала за защита от корпоративен шпионаж;
- разработване и публикуване на стандарти, политики, процедури и бъдещи насоки;
- провеждане на обучение под формата на семинари и конференции по проблемите на компютърната и мрежова сигурност [17], [18];

Технически контрол

Техническият контрол, известен още като логически контрол, се изразява в [2], [4], [20], [23], [26]:

- управление на потребителски пароли и информационни ресурси;
- методи за удостоверяване със сертификати и идентифициране;
- поддържане на защитни механизми за управление на достъпа;
- устройства за мрежова сигурност;
- конфигурация на инфраструктурата на сървърните помещения.

Физически контрол

Физическият контрол се състои от [2], [3], [4], [16]:

- защита на периметъра на комуникационните съоръжения [17];
- осъществяване на контрол на индивидуалния достъп до съоръженията и различните отдели на компанията;
- прилагане на система за мониторинг за проникванията [18], [19];
- прилагане на система за превенция с проникванията [20];
- заключващи системи и премахване на излишни флопи или CD, DVD и Blue-ray дискови устройства;
- контрол на обкръжаващата среда.

Термините "заплаха " (threat), "уязвимост " (vulnerability), "риск" (risk) и "излагане на опасност" (exposure) се използват за илюстриране на едно и също нещо, въпреки че те имат различни значения [7], [8], [10], [11]. Разбирането на всеки един термин е задължително условие за всички компютърни специалисти, служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), служителите по развитие и експлоатация на автоматизираните информационни системи и мрежи (АИС/М), администраторът по сигурността, както и потребителите на АИС/М [9], [14], [16], [17], [29].

Компютърна заплаха

Терминът заплаха е всяка потенциална опасност за компютърните мрежи и системи. Тя е процес на идентифициране на конкретна уязвимост от киберпрестъпник и използването ѝ срещу дадена корпорация, организация, компания или отделно физическо лице [14], [16]. Трябва да се отбележи, че лицето или устройството, което може да се възползва от уязвимостта, се нарича агент на заплахата [2], [10], [10], [11], [14], [16], [25].

Агентът на заплахата е злонамерен потребител, получил достъп до компютърната мрежа през отворен или нефилтриран порт на изградената защитна стена, услуга, процес, достъп до данни, по начин, който нарушава политиката за компютърна и мрежова сигурност [17], торнадо, тайфун, цунами, унищожили информационните съоръжения или служител, направил неумишлена грешка, която може да разкрие конфиденциална информация или пълно унищожаване на файла [2], [3], [4], [17], [18], [29], [32], [33], [34], [35].

Компютърен риск

Вероятността за наличие на агент на заплаха, използващ и прилагащ определена софтуерна уязвимост, се нарича риск.

При наличие на повече от един отворен, затворен или нефилтриран порт в определена компютърна машина с изградена защитна стена, съществува пълна вероятност даден киберпрестъпник да експлоатира един [10] от тези портове с цел получаване на достъп до операционната система на служителя от организацията [7], [8], [9], [16], [17], [25], [29]. Ако не е изградена хибридна защитна стена със система за откриване на проникване в компютърната мрежа, има по-голяма вероятност дадената кибератака да не бъде открита, засечена и анализирана. По този начин рискът обвързва понятията уязвимост, заплаха и вероятността от използването им за определено въздействие върху бизнеса и държавните институции [2], [3], [4], [11], [12], [17], [18], [32], [33], [34], [35].

Излагане на опасност

Излагане на корпорацията, организацията, компанията, държавното учреждение или физическото лице до евентуални щети или загуби от агента на заплаха се нарича излагане на опасност.

Уязвимостта излага организацията или държавното учреждение на евентуални щети [25], [26]. Ако управлението на потребителските пароли не притежава защитни механизми, тогава организацията е застрашена от сканиране и прихващане на потребителските пароли, с което злонамерените извършители ще могат да получат несанкциониран достъп до компютърната система на жертвата [4], [7], [8], [11], [12], [13], [16], [17], [18], [26].

Противодействащи защитни механизми с защитни стени и системи за откриване на прониквания

Противодействащите защитни механизми представляват задължително средство, намиращо приложение за намаляване на появилия се риск. В повечето случаи противодействието се осъществява като се блокира действието на злонамерена софтуерна програма, скрипт на определен програмен език или хардуерно устройство, [2], [3] които имат за цел да атакуват компютърната машина на служителя с цел получаване на достъп до ресурсите и [10], [11], [12], [13], [15], [25]. Противодействието може да бъде осъществено чрез назначаване на специално обучени лица като физическа охрана [17], [18], използване на изключително дълги и силни пароли, специални политики и

механизми на сигурност за управление на контрола на достъпа в операционна система на служителя, поставяне на пароли за основната входно/изходна система BIOS (Basic Input/Output System). Ако бъде поставена такава парола, тогава ако тя не бъде въведена правило, компютърната машина никога няма да разреши стартирането на операционната система. Друго много важна дейност е повишаване на квалификацията на потребителите и служителите в организацията относно противодействието със съвременните видове кибератаки [14], [15]. [16], [32], [33], [34], [35].

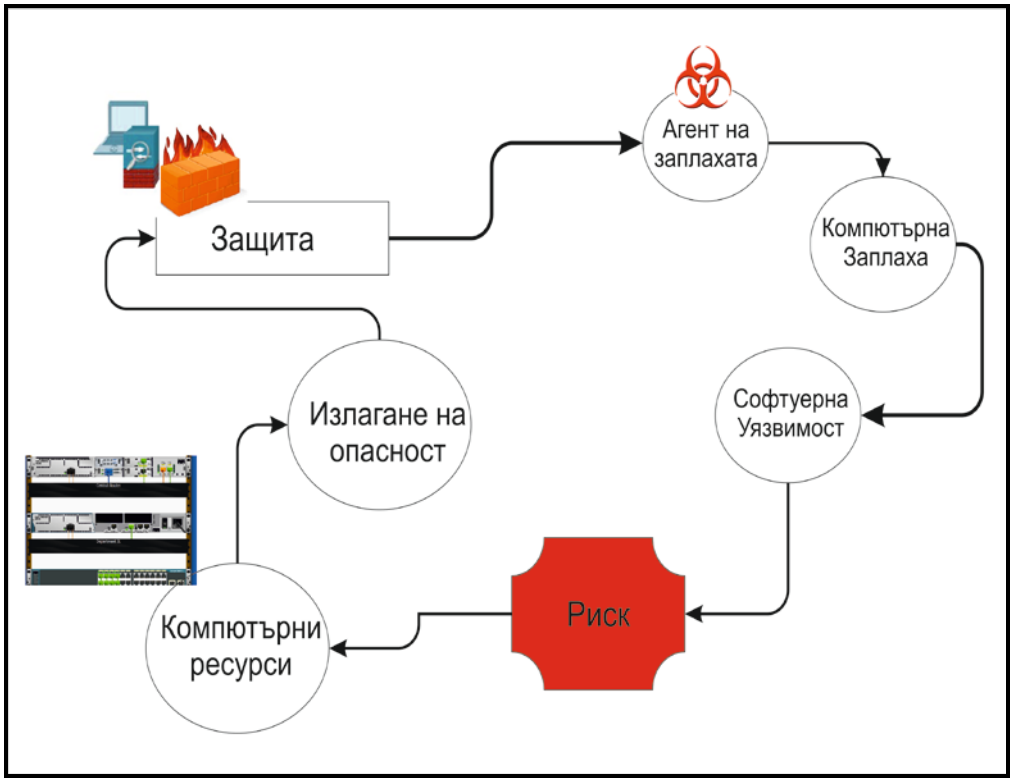
Връзка между риск, уязвимост, заплаха и противодействащи защитни механизми в автоматизираните информационни системи и мрежи (АИС/М)

Връзките между рискове, софтуерни уязвимости, компютърни заплахи и противодействащи защитни механизми ще бъдат изяснени със следния пример. Ако една държавна организация или частна компания [1], [2], [3], [7], [8], [9], [11], [12], [13], [14], [15], [18], [26], [29] използва антивирусен софтуер, но в същото време не се поддържат механизми за автоматично обновяване на антивирусните дефиниции, тогава организацията или компанията е изключително уязвима откъм злонамерени кибератаки от тип социално инженерство, компютърни вируси, компютърни червеи, "задни врати", както и шпионска софтуерна програма, следяща и записваща всеки натиснат клавиш (keylogger) и др [6]. Компютърната заплаха се характеризира с факта, че злонамерен компютърен вирус или троянски кон може зарази операционната система и да намали драстично производителността на компютърната машина на служителя [18], [26]. Вероятността, с която може да се появи компютърният вирус в компютърната машина, както и предизвикването на нанасяне на щети представлява рискът. Ако компютърният вирус проникне в компютърната мрежа на компанията, тогава следва процес на експлоатиране на тази уязвимост и по този начин организацията е изложена на сериозна опасност, която може да доведе дори до пълна загуба на информацията и блокиране на цялата компютърна машина [11], [12], [13], [17], Противодействието може да бъде актуализиране на антивирусните дефиниции и конфигуриране на защитни стени и системи за откриване на прониквания [1], [2], [3], [4], [5], [7], [8], [9], [25], [26] срещу съвременните видове кибератаки [14]. Взаимоотношенията между уязвимостите, рисковете, заплахите и мерките за противодействие са показани на фиг. 1.

Прилагане на стриктни и точни защитни механизми [7], [8], [9], [10], [11], [26] може да блокира уязвимостта на време с цел намаляване на риска и по този начин организацията да бъде в състояние да блокира в ранен етап агента на заплаха [1], [2], [12], [17], [18], [29], [37], [38].

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).



Фиг. 1. Процес на взаимодействие между агент на заплахата, компютърна заплаха, софтуерна уязвимост, риск, компютърни ресурси, излагане на опасност и защита

3. Заключение

Органите по информационна сигурност на национално ниво в Република България са:

- Държавна комисия по сигурността на информацията.
- Дирекция "Информационна сигурност" на Държавна агенция "Национална сигурност".

Органите, осигуряващи информационна сигурността в дадена организация, са:

- Служител по сигурността на автоматизираните информационни системи и мрежи (АИС/М).
- Орган по развитие и експлоатация (ОРЕ).
- Администратор по сигурността.
- Потребители на (АИС/М).

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), служителите по развитие и експлоатация на АИС/М, администраторът по сигурността, както и потребителите на АИС/М трябва задължително да се запознати със задължителните процедури, общи условия и разпоредби за сигурност на автоматизираните информационни системи и мрежи (АИС/М), което е регламентирано в закона за защита на класифицираната информация (ЗЗКИ) в Република България в глава VI, раздел V от чл. 89 до чл. 94. В тези изброени членове са описани всички процедури и общи условия за информационна сигурност.

ЛИТЕРАТУРА:

[1] Ташева, Ж. Н., Р. А. Богданов, Технологични решения за информационна сигурност, Издателство на НВУ „Васил Левски, ISBN 978-954-753-130-7, 2013, 110 с.

[2] Ташева, Ж. Н., Хардуерни и софтуерни средства за информационна сигурност, Издателство на НВУ „Васил Левски, ISBN 978-954-753-188-8, 2014, 136 с.

[3] Ташева, Ж. Н., Информационни технологии за сигурност, Издателство на НВУ „Васил Левски, ISBN 978-954-753-190-1, 2014, 176 с.

[4] Ташева, Ж. Н., Боянов, П. Кр., "Сравнителен анализ на злонамерени уеб-базирани атаки", Научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при Националният военен университет „Васил Левски”, гр. Шумен, Българаия, ISBN 978-954-9681-49-9, 6 - 7 Юни 2013, стр. 178-183.

[5] Allen, L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing, Birmingham, UK, May 2012, ISBN 978-1-84951-774-4, pp. 414

[6] Bodmer, S., Kilger, M., Carpenter, Gr., Jones, J., Reverse Deception: Organized Cyber Threat Counter-Exploitation, McGraw-Hill Education, 2012, ISBN: 978-0-07-177250-1, pp. 465.

[7] Boyanov, P., Using the Colasoft Capsa network analyzer to diagnose, pinpoint and detect a variety of malicious cyber-attacks and to improve the vulnerabilities for a SOHO network, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 93-100.

[8] Boyanov, P., Using the security network scanner GFI Languard to discover and improve the vulnerabilities in the computer network systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 4, 2013, pp.74-79.

[9] Boyanov, P., Analysis and assessment the security vulnerability in communication processes in a given computer network, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, VOL. 2. 2014, pp. 39-44.

[10] Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

[11] Boyanov, P., Hristov, H., Implementation of network enumeration cyber-attacks and defense the computer resources of the local and wide area networks, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 392-397.

[12] Boyanov, P., Hristov, H., Defense the computer resources of the government agencies, private organizations and academic institutions against the wannacry (wanacrypt0r 2.0) ransomware cyber-attack, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 398-407.

[13] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 386-391.

[14] Boyanov, P., A taxonomy of the cyber attacks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, Vol.3, 2013, pp. 114-124.

[15] Hristov, Hr., Boyanov, P., Trifonov, T., Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 101-107.

[16] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[17] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[18] Hristov, Hr., A modern survey on problems of business organization's security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[19] Kahya-Özyirmidokuz, E., Gezer, A., Ciflikli, C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, ISBN: 978-1-61208-242-4, pp.18 – 23.

[20] Kaur, R., Singh, G. Analysing, Port Scanning Tools and Security Techniques, International Journal of Electrical Electronics & Computer Science Engineering, Volume 1, Issue 5, October 2014, ISSN : 2348 2273, pp. 58 – 64.

[21] Meyers, C., Powers, S., Faissol, D., Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 22.

[22] Meyers C., Powers S., Faissol D., Probabilistic Characterization of Adversary Behavior in Cyber Security, No. LLNL-TR-419023, Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009, pp. 1 – 52.

[23] Shimeall, T. J., Spring, J. M., Introduction to Information Security: A Strategic-Based Approach, Syngress, 2014, ISBN: 978-1-59749-969-9, pp. 359.

[24] Simmons, C., Shiva, S., Dasgupta, D., Wu, Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.

[25] Савов, И., Един поглед върху същността на киберпрестъпленията, списание „Политика и сигурност", ВУСИ, 2017, ISSN 2535-0358, с. 36-47.

[26] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[27] Fetfov O., Tonev V. Bedzhev B. "Information Encryption with Combination Generator", CERC 2002 – Military Technical Academy, Bucharest, Conference Proceedings , Section of Radar and Guiding Missiles System, Num. 4, May 2002.

[28] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA", Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски", 2015г.

[29] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[30] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal with Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[31] Боянов, П. Кибератаки и противодействие. Монография, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-206-9, гр. Шумен, 2017 г., 210 с.

[32] Nikolov, L., Slavyanov Kr., On the contemporary cybersecurity threats, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953; url: http://confsec.eu/sbornik/2-2017.pdf.

[33] Nikolov, L., Същност, роля, място и задачи на кибер защитата в сигурността и отбраната. International scientific conference "Technics. Techologies. Education. Safety '18", Proceedings, Year II, Issue 1 (4), Sofia, Bulgaria, 2018, Volume 1, Section: Military Sciences, ISSN 2535-0315, http://techtos.net/sbornik/1-2018.pdf.

[34] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София", ISBN 978-954-01-3785-8, 2018 г.

[35] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[36] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[37] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие "40 години Шуменски

университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

[38] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

Име на автора: доц. д-р инж. Николай Йорданов Досев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: ndosev@abv.bg, n.dosev@shu.bg
Име на съавтора: проф. д-р инж. Велико Панчев Петров
Месторабота: НВУ „Васил Левски“, Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи“, Катедра "Информационна сигурност"

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 96 - 108 Problems of Security Systems

ABOUT THE FINANCIAL PROVISION OF THE ACTIVITY OF A COMPANY COUNTER-INTELLIGENCE UNIT

IVAN I. KANTARDZHIEV, STANIMIR S. STANEV, HRISTO A. HRISTOV

ABSTRACT: *The paper considers the structure and tasks of the company's counter-intelligence unit, the approaches and problems of financing its activities. Specific details are provided on how to form the budget framework of these units.*

KEYWORDS: *Competitive Intelligence, Counterintelligence, Company Security Services, Financing, Budget.*

ОТНОСНО ФИНАНСОВОТО ОСИГУРЯВАНЕ НА ДЕЙНОСТТА НА ФИРМЕНО КОНТРАРАЗУЗНАВАТЕЛНО ЗВЕНО[1]

ИВАН И. КАНТАРДЖИЕВ, СТАНИМИР С. СТАНЕВ, ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *Разглеждат се структурата и задачите на фирмено контраразузнавателно звено, подходите и проблемите на финансиране на неговата дейност. Предлагат се конкретни данни за формиране на рамките на бюджета на тези звена.*

1. Въведение

В световен мащаб компаниите стават все по-зависими от корпоративното разузнаване за информация относно конкурентите, околната среда, доставчиците, продуктите и дори клиентите си. Корпоративното контраразузнаване е обратната страна на бизнес шпионажа и корпоративното разузнаване. Основната му цел е да защитава фирмите от потенциалните заплахи и, разбира се, да повишава сигурността им. За да останат конкурентоспособни, фирмите трябва да отделят ресурси и за контраразузнаването[1]. Структурите за контраразузнаване са задължително звено на службите за сигурност на големите корпорации [2].

За успешното функциониране и ефективното управление на фирмените служби за сигурност (ФСС) е необходимо да им се предоставят материални, технически, финансови, човешки и информационни ресурси. Финансирането на ФСС е въпрос на осъзната необходимост за ръководителите на фирмите. Наличието на такава служба не е самоцел или въпрос на престиж. ФСС трябва да се приема като един от бизнес проектите на фирмата, като нейна дейност, като процес, който следва да бъде планиран и реализиран по икономически показатели. Проблемът с финансирането на службата за фирмена сигурност е сложен и специфичен и зависи от много фактори. Неговото решаване трябва да подобри ефективността на управлението и допринесе за устойчивото развитие, да минимизира рисковете, намали загубите и възможните щети [26]. Без финансово осигуряване на дейността на ФСС е безсмислено въобще да се говори за нейното функциониране.

Един от най-често възникващите въпроси е доколко са обосновавани разходите за осигуряването на дейността на ФСС [3].

[1] Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Анализът на публичните литературни и мрежови източници не дава необходимата информация за прогнозиране и планиране на конкретните разходи от страна на собствениците на фирмата, а достъпната е частична и касае финансиране на различни по сложност структури на системата за сигурност.

Целта на настоящата статия е разглеждането на основни проблеми и подходи при финансовото осигуряване на дейността на контраразузнавателно звено, влизащо в състава на фирмена служба за сигурност.

2. Изложение

2.1. Проблемът за финансовото осигуряване на ФСС в светлината на задачите и структурата им.

Световните корпорации имат на пазара от два до четири конкурента с които водят постоянна борба. Според западни източници, загубите на корпорациите в света от икономически престъпления е 2,3 % от общия национален продукт [4]. Поради това с конкурентно разузнаване активно се занимават както държавни, така и фирмени служби за сигурност [5]. Най-ефективната система за икономическа сигурност днес функционира в САЩ както на държавно, така и на корпоративно ниво, с добре разклонени мрежи от служби за разузнаване. Разходите за превантивни бизнес-програми за осигуряване на фирмената сигурност са повече от 36 милиарда долара [6].

В началото на 80-те години американските корпорации са понесли загуби от икономически шпионаж за около 20 милиарда долара годишно. В същото време големи корпорации са похарчили близо 1,5 милиарда долара за разузнаване, т.е. за всеки долар на тайно извличане на информация са получени повече от 13 долара приходи. За сравнение, добри печалби в традиционния бизнес се считат тези от 15-25 цента на долар от разходите, а в рисков бизнес - 1-2 долара. Някои корпорации имат хиляди и дори десетки хиляди агенти на икономическото разузнаване и службите за сигурност [7].

Подобни тенденции има и в Русия. По неофициални данни на сътрудници на ФСБ, практически всяка голяма руска фирма краде информация от своите конкуренти и едновременно с това страда от аналогични действия от тяхна страна [8].

За разлика от обширната публична информация за дейността на конкурентното разузнаване в развитите индустриални страни, за задачите и действията на фирмените контраразузнавателни звена на големите корпорации по света [1,7], у нас изглежда странно ограничаването на понятието фирмена сигурност до практически действия само по техническата и физическата охрана на големи български фирми. Има и обективни причини за това – преди всичко значително по-малкия мащаб на дейности на самите фирми, а от там и ограничените задачи на собствените фирмени системи за сигурност, ако такива са създадени. Сега за тях не е приоритет противодействието на чужди корпоративни разузнавания за кражба на научни и технологични секрети и „ноу-хау“ на наши водещи фирми. При разглеждане на задачите на съществуващи или перспективни фирмени контраразузнавателни звена на наши фирми, подробно разгледани в[9], би трябвало те да се подредят по приоритет като се отчитат сегашните и в близко бъдеще условия у нас.

Вероятно в следващите години проблемите пред контраразузнавателните звена ще станат подобни на тези, посочвани в публичните чуждестранни източници.

За съжаление сега липсва достоверна българска статистики за загубите на фирмите от икономически престъпления.

Схемата на развитие на бизнеса у нас, независимо от участието ни в ЕС, копира и много от чертите на развитието на частния бизнес в постсъветското пространство поради

много причини, само мащабите са по-различни. Поради това при липса на наши данни за прогнозиране на тенденциите в развитието на сигурността на фирмите е полезно да се анализират публикации на подобни процеси в редица крупни руски компании [10, 11]. Това може да подпомогне работата по осигуряване на собствените служби за сигурност.

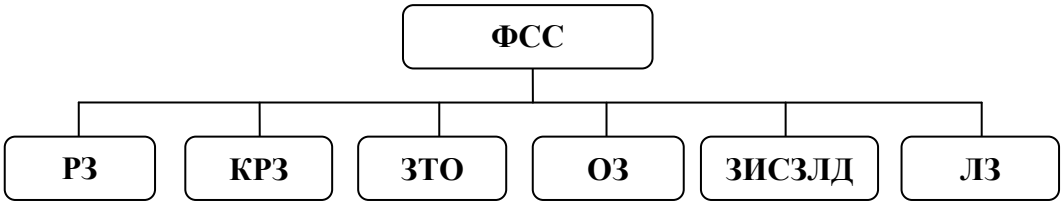
Собствениците на фирми може да се срещнат с редица негативни проблеми - кражби, измами, непрофесионални действия на свои служители, липса на лоялност на персонала, липса на координация на вътрешните бизнес процеси, ненадеждни доставчици и партньори и др. Заплахите за бизнеса включват и изтичане на вътрешна информация, конкурентни, вътрешнокорпоративни войни, "повишено внимание" на държавните служби и власти, изнудване, нападение и др. Всички тези заплахи са в състояние да донесат на компанията не само щети в сегашно време, но могат да се отразят и на бъдещото развитие на фирмата и нейното съществуване. Решението на всички тези проблеми изисква време, човешки и материални ресурси, както и най-важното – съществуването, знанията и опита на експертите на ФСС. Тя трябва да осигури сигурността на фирмата [11].

Под сигурност в настоящата работа се разбира състояние на защитеност на фирмата от външни и вътрешни заплахи и способността й да гарантира своето съществуване (цялост, дейност, растеж и развитие) за постигане на цели си с оптимален разход на ресурси.

Един от основните въпроси за осигуряване на необходимото ниво на сигурност е икономическата ефективност. След анализ на необходимите разходи за целта трябва да се направи избор - създаване на собствена служба за сигурност или използването на външна такава под формата на аутсорсинг. Глобалната тенденция показва, че 18% от компаниите прибягват до определен вид аутсорсинг на дейности по фирмената сигурност, а само някои от тях до пълен. В Русия, ситуацията е още по-консервативна, особено що се отнася до фирмената информационна сигурност. Средната стойност на разходите за информационна сигурност на фирмите е само 3% (световната цифра е 7%) от общия им бюджет за информационни технологии [10]. Само 5,5% от анкетираните считат, че е възможен цялостен ауторсинг на информационната сигурност.

Организационната структура на службата за сигурност се определя главно от размера на бизнеса и отрасъла на компанията. В съвременните условия службата за сигурност на фирмата трябва да има звена за разузнаване и контраразузнаване [8]. Работата и на двете зависи от финансирането, количеството и опита на оперативния състав.

За целите на настоящото изследване на фиг. 1 е предложен структурен модел на ФСС-съставна част на голяма българска частна фирма с развита структура в страната.



Фиг.1. Модел на ФСС

В схемата РЗ е разузнавателно звено; КРЗ – контраразузнавателно звено; ЗТО – звено техническо осигуряване; ОЗ – охранително звено; ЗИСЗЛД – звено информационна сигурност и защита на личните данни; ЛЗ – логистично звено.

Очевидно е, че в този случай не се предполага прилагане на аутсорсинг или аутстафинг за някои от дейностите на ФСС, тъй като в нейната структура има звена, които обхващат всички направления за осигуряване на сигурността на фирмата.

Фиг. 2. Структура на контраразузнавателно звено

На фиг.2 е предложен модел на КРЗ. За пълноценното изпълнение на всички задачи, представени в [9], минималния състав съгласно предложената структура трябва да бъде 12-14 души. Звеното за специфични дейности може да включва финансист, психолог, служител на специализираното деловодство, юрист по наказателно право и парамедик.

Към настоящият момент могат да се посочат приоритетни задачи на фирменото КРЗ. Това са разкриване и предотвратяване опитите за изтичането на поверителна информация за дейността на фирмата от инсайдери, в това число и във взаимодействие със ЗИСЗЛД чрез съвременните способи на стеганологичната защита [12], пресичане на опитите за инфилтрация и вербовка на агенти от страна на конкуренцията, партньори и престъпни структури, превантивна проверка на лоялността на служителите, официално разследване на фактите за фалшифициране и кражба, оперативно прикриване на персонала, сгради и обекти на собствената фирма [6].

Практиката показва, че причиняването на вреда на компанията от нейни служители обикновено не се ограничава до банални кражби. Към тях могат да се добавят още разкриването на поверителна информация, злоупотреба с материали и оборудване на фирмата, вандализъм, саботаж, злоупотребата с алкохол и наркотици на работното място, "кражбата на работно време", плащането на фиктивен отпуск по болест и т.н. Наред с това, звеното за контраразузнаване трябва да обърне достатъчно внимание на предотвратяването на възникването на негативни процеси в колектива на фирмата-трудови конфликти с администрацията, влошаване на междуетническите отношения, заплахи за стачки, групови нарушения на обществения ред и др. Идентифициране и отстраняване на причините и условията за тези кризи трябва да се извършва като със специални (с използване на административни дисциплинарни методи) така и с социално-психологически методи (съгласуването на противоречивите интереси на страните) [6].

2.2. Подходи за финансовото осигуряване на КРЗ

Възможностите за извършване на видовете дейности от фирменото звено за контраразузнаване се определят от количеството и професионалните качества на служителите и от финансовото осигуряване [6, 13]. Количеството и професионалната подготовка на служителите на звеното ще дадат възможните начини за действие, докато финансовото осигуряване ще зададе реално изпълнимите. Оптималния разход на ресурси по отношение дейността на контраразузнавателното звено ще даде баланс между прогнозните щети от евентуална реализация на заплахата, предприетите мерки за противодействие на посегателствата и реализираните ползи.

Контраразузнавателната дейност е непрекъснат процес, свързан с постоянно и задълбочено изучаване и познаване на процесите извън и вътре в организацията, на работещите в нея и т.н.

Определянето на разходите на звеното за контраразузнаване на фирмата е постоянен във времето, динамичен процес, който се влияе от различни фактори като големина на фирмата, териториалното й разпределение, броя на хората работещи в нея, обекти подлежащи на защита, външната среда и др. Те се формират на базата на прецизен анализ на уязвимостите, рисковете, заплахите и планиране на действията на контраразузнавателното звено. Анализът е необходимо да бъде извършен както към текущото така и към прогнозното състояние за определен период на база плановете за развитие на фирмата. Също така е необходимо определяне на финансов резерв за употреба при непредвидени обстоятелства даващ възможност за по-бърза и ефективна реакция от страна на звеното за контраразузнаване спрямо уязвимостите и заплахите [24], [25], [26], [27], [28], [29], [30], [31], [32].

При планирането на бюджета и стратегията за развитие е необходимо да се отчете и факта, че фирменото звено за контраразузнаване ще противодейства и на посегателства от страна на конкурентни организации с по-големи ресурси и възможности [14].

При осигуряване на финансирането могат да възникнат и определени проблеми, свързани с недофинансиране или свръхфинансиране.

Недостатъчното финансиране поради ограничен определен бюджет за КРЗ [14] води до удължаване на времето за работа на служителите по поставените контраразузнавателни задачи.

За разлика от държавното контраразузнаване, финансирането на частните служби за сигурност зависи от вижданията на собствениците и топ мениджърите. В редица български фирми се наблюдава подценяването на проблемите на фирмената сигурност, а от там и намаляване на съответните разходи. Това се отразява значително при работа с информационните източници, особено на конфиденциалните, защото това намалява техния брой заради стремежа за преодоляване на времевия дефицит. Недофинансирането може да доведе до невъзможност за компенсиране на щети от реализация на неидентифицирани заплахи. Положителното при недофинансирането в малък процент е, че може да стимулира по-голяма активност и самоинициатива на служителите на КРЗ.

Свръхфинансирането на дейността на КРЗ води до презастраховане в определени направления и като резултат разходите да надхвърлят очакваните ползи.

Определения бюджетна КРЗ трябва да бъде изключително добре прецизиран като се предвиди определен резерв, който ще предостави гъвкавост и възможност за бърза реакция в настоящата динамична среда.

Възможният модел от [14] за намаляне на разходите чрез работа на служителите от КРЗ по съвместителство на непълен работен ден е недопустим. Това допълнително ще намали времето за работа и ще забави реакцията на КРЗ, ще предизвика занижаване на ефективността на работата и невъзможност служителите да изпълняват в пълен обем задачите си.

По тези причини ръководителите на ФСС трябва да участват активно в обосновка на финансовите потребности на службата за сигурност и да осигуряват собствениците на фирмите с точни разчети за тази дейност.

2.3. Рамки на финансовото осигуряване на КРЗ

Финансовата рамка, определена на базата на анализа по сигурността на фирмата и планираните действия от страна на звеното за контраразузнаване ще даде естествена

регулация на мерките за противодействие на посегателствата и недопускане състояние на недостиг или преразход на финансови средства.

При устойчиво развитие на икономиката, а така също и когато фирмата се намира на етап за разширяване на производството, тогава бюджетът на ФСС се осигурява в размер на 60-70% за сметка на собствените средства на компанията и 30-40% за сметка на възвръщане на средствата в резултат от дейността на ФСС („самофинансиране на ФСС"). В условия на значителен икономически подем и увеличаване рентабилността на бизнеса, частта „самофинансиране на ФСС" се увеличава, а обемът на получените средства от компанията спадат на 40-50%. По време на кризи и депресии при понижаване обема и ефективността на производството (търговия, услуги) при инвестициите за сигурност рязко се понижава частта („кредитиране на СС") и се увеличава отделената тежест („възвръщаеми средства за сигурност") до 70-80%[13].

Бюджетът за сигурност и структурата му зависи до голяма степен от степента на развитие на региона, в който осъществявате бизнес. Обикновено, ако в една миннодобивна компания се харчат около 30% за физическа сигурност чрез въоръжена охрана, то в една компютърна компания структурата на бюджета за сигурност ще бъде различна и по-голямата част от него ще бъде насочена към осигуряване на сигурността на информационния компонент на бизнеса. Според оценката на западните експерти, разходите за корпоративно разузнаване представляват 1,5% от оборота на транснационалните компании [15]. Оптималните разходи за сигурност на големите компании са 1% от техните годишни приходи [16].

Разбира се, трябва да се отчитат и разликите в дейността и способите за финансиране на държавното и корпоративно контраразузнаване [2]. Една от важните от тях е възможността за застраховане на частните компании за компенсиране на загубите от корпоративното разузнаване, вместо разходи за поддръжка на ФСС.

При формирането на бюджета на ФСС и КРЗ в частност са възможни три подхода при планиране на финансовото им осигуряване.

Един от тях е да се определи обща сума за финансиране, която да се разпредели между звената на службата според състава и задачите, които изпълнява. При този вариант планирането на дейностите се съобразява със зададената финансова рамка. Друг подход е ръководителите на звената в службата за сигурност на базата на оценка на рисковете и заплахите и планираните действия по противодействие да определят необходимия за дейността им бюджет, който да защитят пред ръководителите на корпорацията. При този вариант планирането на финансите се съобразява изцяло с изискванията на службата за сигурност с цел осигуряване на необходимото ниво на сигурност на корпорацията. За най-приемлив се счита комбинирания между предходните два варианта [17]. При него се дава възможност да се оценят реалните нужди на службата за сигурност и възможностите за разходи за сигурност на корпорацията като се стига до балансиран вариант на финансиране.

Планирането на бюджета се извършва за година, като текущото отчитане на извършените разходи на месец, тримесечие и половин година. Това дава възможност за гъвкаво управление на финансовия ресурс.

Прецизният анализ и планирането на финансирането на контраразузнавателната дейност ще предпази фирмата от преразход или недостиг на средства. Структурата и планирането на развитието на системата за сигурност на корпорацията се извършва след обстоен анализ на уязвимостите, рисковете и заплахите върху сигурността като финансовата рамка се явява естествен регулатор на процесите.

Анализът на явните литературни и мрежови източници не дава необходимата информация за прогнозиране на конкретни разходи от страна на собствениците на компанията, а достъпната е откъслечна и касае финансиране на различни по сложност структури на системата за сигурност. В явните източници относно дейността на службите за сигурност този въпрос също не е засегнат, но въпроса за финансирането заедно с целите и задачите са определящи за успеха или неуспеха на службата за сигурност.

Определена информация за финансиране на КРЗ може да се получи по аналогия с исторически данни от публични източници за финансирането на държавни контраразузнавателни звена. За съжаление поради спецификата на въпроса по разбираеми причини подробности по съвременните им бюджети не са известни.

Има публични данни за финансиране на Службата за сигурност на Украйна в размер на 4,6 % от общия държавен бюджет и увеличаване за 2018 година на разходите на контраразузнаването [18]. В Русия за същата година разходите за ФСБ са 0,15 % от бюджета[19], а у нас разходите за ДАНС са 0,46% от бюджета на България за 2018 год.[20].

В таблица 1 на базата на [13] се предлага вариант за видовете разходи в разпределението на бюджета на фирмено контраразузнавателно звено. Те са разделени на устойчиви и променливи. Устойчиви са тези, които през последващи финансови периоди са относително постоянни. Те пряко зависят от плановете за развитие на структурата за сигурност и са лесно предвидими. Променливи от своя страна се отнасят до специфичните дейности на структурата за сигурност и зависят от редица фактори.

Таблица 1

Устойчиви разходи		
№	Вид на разхода	Относно
1	Работна заплата	- Служители и ръководство
2	Техника	- Компютри - Сигнално-охранителна техника - Специална техника
3	Програмно осигуряване	- Управление на бази от данни - Управление на специална техника
4	Разходи за събиране на информация по официален път	- Интернет, библиотека - Медии - Бази данни - Външни организации предлагащи информационни услуги
5	Комуникационни услуги	- Закупуване на комуникационни средства - Абонаменти за

		оператори на услуги - Интернет
6	Заплащане на услуги на външни организации	- Външни информационни компании привлечени при изпълнение на особено сложни задачи - Такси за информационни услуги на държавни структури - Технически фирми, разполагащи със скъпа техника и богат опит, извършващи услуги в областта на информационната безопасност
7	Медицински услуги	- Годишни медицински прегледи - Подпомагане при конкретно лечение
8	Застраховки	- На служители - На активи
9	Консумативни	- Наем за офисни помещения - Битови разходи
Променливи разходи		
10	Разходи за доверителни източници	- Плащане за конкретна дейност - Резервен фонд за допълнително заплащане при критични ситуации
11	Представителни	- Подаръци - Разходи на обществени места и заведения, необходими за създаване и поддържане на делови и доверителни контакти
12	Консумативни за специфична дейност	- Хотели, квартири и други места за

		конфиденциални срещи с доверени лица
13	Командировъчни	- Храна - Транспорт - Дневни

Още преди Втората световна война е стоял въпроса с недостатъчното финансиране на държавните служби за сигурност. На базата на исторически данни за конкретни суми по видове дейности през този времеви период, в таблица 2 е дадено процентно разпределение на най-важните разходи [21].

Преводачи	Канцелария и фотография	Служебни командировки	Наем конспиративни квартири	Секретни разходи
3%	8,5%	17,5%	3,5%	67,5%

От таблицата се вижда, че най-голям дял около 70 % от общото финансиране е за разходи по специфичните дейности на контраразузнавателното звено, а останалите приблизително 30% са за устойчивите (постоянните) разходи. На базата на тези данни, изчисляйки конкретните суми за постоянни разходи, може да бъде изчислена сумата на променливите, а от там и обща конкретна сума за финансиране на КРЗ с достатъчно точна прогнозна стойност за практиката.

Разбира се, аналогията с държавните разходи е само отправна точка за определяне на общите разходи, която да даде първоначална представа на ръководството на фирмата. Точното определяне на процентното разпределение ще се влияе от обективната необходимост и вижданията на съответните ръководители [13].

Формирането на фонда от работна заплата във фирмите у нас не винаги се извършва обосновано. Заплатите на сътрудниците се определят често на базата на общата трудова конюнктура в страната. От практиката на фирми с охранителна дейност може да се види, че обикновен служител с неголям стаж получава месечно възнаграждение около 10-15% повече от минималната работна заплата за страната, а на служител от службите за техническо осигуряване – около 2 пъти минималната работна заплата, процентът на работната заплата варира от 15 до 60 % от общия бюджет на СС. Тези заплати са съизмерими със основната заплатата на полицай от 800 до 1000 лева. За сравнение, през 2017 год. средната заплата на полицай в Русия варира по региони от 450 до 480 долара (без допълнителното възнаграждение) [22]. Заплатите на полицаите в Германия са 2800-3000 долара [22].

За информация с цел определяне съотношенията на заплатите на отделните позиции в ФСС у нас, могат да се използват и данни за основните възнаграждения в руските частни служби за сигурност.

Образуването на фонда за работни заплати в руските корпоративни служби за сигурност също не се извършва винаги обосновано [15]. Размерът на заплатите в едно звено може да се различава с десетки проценти, при това не винаги в зависимост от извършената работа. Към 2018 год. средната заплата на служител от частните служби за сигурност варира от 800 долара в Москва, 645 долара в Санкт Петербург до 400 долара в градове като Казан, Уфа и Омск. Тези заплати понастоящем се определят както от фирмата, в която е службата, така и от географския район, в който се намира тя [23]. В

частните служби за сигурност се назначават служители най-малко със средно образование. Заплатата на служител без опит започва от 560 долара в Москва и 400 долара в Санкт Петербург.

Заплатите на служители с висше образование и опит на работа 1 година е от 645 до 800 долара в Москва и от 516 до 645 долара в Санкт Петербург. За специалистите с опит 3 години заплатата варира от 1080 долара в Москва до 806 долара в Санкт Петербург. По-голяма заплата получават служителите с опит над 5 години (обикновено бивши служители на полицията или държавните органи за сигурност) – 1612 долара в Москва и 1290 долара в Санкт Петербург. Рядко адекватна заплата получава и директорът на ФСС. Често това зависи не толкова до заплатата, а до позиционирането му във фирмата. Според руски специалисти той трябва да получава повече от мениджърите на компанията. Обаче според други експерти заплатата му не трябва да е по-висока от тази на главния счетоводител на компанията, който подписва основните финансови документи на корпорацията.

За ФСС у нас при определяне на заплата на ръководителя на контраразузнавателното звено, еквивалентна на 1400 долара, и средна заплата на служителите от звеното 700 долара, приблизителната оценка за фонда работна заплата на звеното е еквивалентна на около 11000 долара. Ако тя е 25 % от бюджета на звеното, то рамките на месечния бюджет на звеното са 44000 долара. Когато в компанията се изплащат премии на служителите от ФСС, то оптимален е варианта, когато на служителите по тримесечия или в друг режим се отпуска уговорена сума, която се разпределя между служителите в зависимост от приноса на всекиго в общата дейност [8].

Целесъобразно е в бюджета на ФСС да се заделят и определени средства за поощряване на работещите в корпорацията за сътрудничество със службата за сигурност. Целта е да създаде „мотивация към сътрудничество” посредством парични премии и гарантирана анонимност. На първо време средствата могат да бъдат трудни за осигуряване, но постигнатия ефект от намаляне на фактическите щети ще възстановят с лихви вложеното. По оценка на западните експерти всеки изплатен като „премия за сътрудничество” долар води до намаляне на щетите от четири до седем долара [15].

3. Заключение

Анализът на информацията от публични източници за другите страни, показва, че за разлика от тях, у нас не са налични отговори за конкретни рамки и препоръки за финансирането на службата за сигурност. С отчитане на всички посочени съображения може да се приложи подхода на аналогията, за да се определи какъв процент от годишния оборот на фирмата да се отделя за тази дейност.

На базата на посочените данни за държавни и частни фирми в областта на сигурността, може да се предложи предварителна оценка на размера на фонда работна заплата за фирмено КРЗ със структура от фиг.2.

Световната практика показва, че при недостатъчно финансиране на собствените служби за сигурност се повишава значително риска от опасности за компанията, от една страна, и за поява на недоволни инсайдери в самата служба за сигурност от друга. При работа в условия на нисък бюджет, не се препоръчва съвместяване на дейности от едни и същи служители поради липса на средства, това води до ниско качество и спадане на мотивацията на последните да изпълняват основните си функционални задължения.

Един от най-важните аспекти на работата на директора на ФСС е разработването на бюджета на неговата служба в съответствие с финансовата стратегия на фирмата, нейната обосновка (защита), контрола върху правилното изпълнение и корекции, ако е необходимо по време на работа. Това изисква познаването и на основните принципи на

финансовото управление от мениджъра по сигурността. Тъй като основната цел на бизнеса е да реализира печалба, програмата за сигурност трябва да бъде и икономически изгодна и измерима от гледна точка на финансите. Размерът на бюджета задава обща външна рамка на дейностите и възможностите на звеното за контраразузнаване на фирмата.

Определянето му трябва да бъде прецизно извършено, защото малки колебания в положителна или отрицателна посока от необходимостите могат да дадат големи разлики във възможностите. Те ще влияят пряко и основно върху променливата част от разходите, която от своя страна осигурява специфичните дейности на звеното за контраразузнаване на фирмата.

Предстоят конкретни проучвания и изследвания на фирми в Североизточна България от различни сфери на стопанския живот и с различни финансови възможности, относно въпросите за организираните служби за сигурност, начините за материално-техническо и финансово осигуряване на ФСС и формиране на бюджетите за дейността им.

ЛИТЕРАТУРА:

[1] Whitehead, St., Corporate counterintelligence – protecting business information.[онлайн].[прегледаномай2018]. http://www.cbr.co.za/ regular.aspx?pklRegularId=1390.

[2] Tucker, W., Counterintelligence in the Private Sector.[онлайн].[прегледано юни 2018]. https://worldview.stratfor.com/horizons/fellows/william-tucker/05122017-counterintelligence-private-sector.

[3] Комаров, В., Бюджет службыбезопасности, как эффективный инструмент управления.[онлайн].[прегледано май 2018] http://www.psj.ru/saver_people/detail.php?ID=68403 10 августа, 2011.

[4] Землянов В.М., Своя контрразведка. Практическое пособие.[онлайн].[прегледано май 2016].http://litresp.ru/kniga/ru/%D0%97/zemlyanov-valerij-mihajlovich/svoya-kontrrazvedka-prakticheskoe-posobie

[5] Hulnick, A., RiskyBusiness. Private Sector Intelligence in the United States. [онлайн].[прегледано юни 2018]. http://hir.harvard.edu/article/?a=1065.

[6] Доронин, А.,Бизнесразведка. (Система экономической контрразведки промышленного предприятия).[онлайн].[прегледаноюни 2018].http://www.nnre.ru/delovaja_literatura/biznes_razvedka/p12.php.

[7] Организация и эффективность экономической разведки.[онлайн].[прегледаномай 2018]. http://na-uroke.in.ua/31-61.html.

[8] Экономическая разведка и контрразведка. [онлайн].[прегледаномай 2018]. https://studbooks.net/930279/pravo/ekonomicheskaya_razvedka_kontrrazvedka.

[9] Христов, Х.,Организация и управление на противодействието срещу посегателства на фирмената сигурност. Дисертация. УНИБИТ, София.2012.

[10] Бугримов,С., Зенкин,Д., Борисов, К., (интервью). Служба безопасности — надежная опора бизнеса.[онлайн].[прегледано май 2018].http://www.top-personal.ru/issue.html?1980.

[11] За безопасность нужно платить, а за ее отсутствие расплачиваться.[онлайн].[прегледано юни 2018]. http://ohrana.ru/articles/53006/.

[12] Станев, С.,Стеганологична защита на информацията.Университетско издателство „Епископ К. Преславски“, Шумен, 2013.ISBN 978-954-577-825-4.

[13] Финансирование подсистемы экономической разведки предприятия[онлайн].[прегледано май 2018]. https://studwood.ru/1114569/menedzhment/finansirovanie_podsistemy_ekonomicheskoy_razvedki_predpriyatiya.

[14] Вайс,А. и Иванов, М., Конкурентно разузнаване с ограничен бюджет, Professional Бр.3,4.2013.

[15] Принципы финансирования системы экономической разведки предприятия.[онлайн].[прегледано юни 2018]. http://bzbook.ru/biznes-razvedka.12.html.

[16] Бюджет на безопасность.[онлайн].[прегледано май 2018].https://www.unirate24.ru/byudzhet-na-bezopasnost/.

[17] Миронов, Н.,Планирование бюджета службы безопасности малого предприятия.[онлайн].[прегледано май 2018]. http://www.amulet-group.ru/page.htm?id=645.

[18] [онлайн].[прегледано юни 2018]. https://theworldnews.net/ua-news/daniliuk-raskhody-na-sbu-i-genprokuraturu-nuzhno-umen-shit-a-na-kontrrazvedku.

[19] Бюджетные расходы на силовиков к 2019 году вырастут до 2 трлн руб.[онлайн].[прегледано юни 2018].https://www.rbc.ru/politics/23/10/2016/580a526d9a7947cb56546df8https://www.rbc.ru/politics/23/10/2016/580a526d9a7947cb56546df8.

[20] Бюджетна ДАНС за 2018 г.[онлайн].[прегледано май 2018]. http://www.dans.bg/images/stories/budget/Budget_2018/budjet_dans_2018.pdf.

[21] У истоков русской контрразведки. Сборник документов и материалов. [онлайн].[прегледано юни 2018]https://rutlib4.com/book/18323.

[22] Зарплата полиции в России.[онлайн].[прегледано юни 2018].https://visasam.ru/russia/rabotavrf/zarplata-policii-v-rossii.html.

[23] Специалист службы безопасности на предприятии.[онлайн].[прегледано юни 2018]. https://www.superjob.ru/research/articles/111894/specialist-sluzhby-bezopasnosti-na-predpriyatii/.

[24] Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

[25] Boyanov, P., Zhaneta, T., An unauthorized penetration into computer system with activated firewall and antivirus software, Anniversary Scientific International Conference 45 Years Computer Sciences and Engineering Department 30 Years Computer Systems and Technologies Speciality, 27-28 September, 2013, ISSN 1312-3335, Varna, Bulgaria, Section 1 Computer systems and Networks, pp.41-46.

[26] Hristov, Hr., Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies. Mathematical and Software Engineering, ISSN 2367-7449, Vol.4, No 1, 2018, pp. 1-6.

[27] Hristov, Hr., A modern survey on problems of business organization’s security. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 7, 2015, pp. 72-79.

[28] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security” № 1(3)-2013 УДК 004 (056.5+413.5).

[29] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[30] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[31] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски", ISBN 978-954-753-207-6, 2014 г.

[32] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

Име на автора: докторант Иван Иванов Кантарджиев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: ikant@abv.bg

Име на съавтора: проф. д-р инж. Станимир Стоянов Станев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: stan_stanev@yahoo.com
Име на съавтора: доц. д-р инж. Христо Атанасов Христов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Началник на катедра „Управление на системите за сигурност“
E-mail: hristov63@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 109 - 115 Problems of Security Systems

TOOLS FOR DEFENSING THE SENSITIVE COMPANY INFORMATION FROM INSIDER THREATS

LUCHEZAR T. HRISTOV, STANIMIR S. STANEV, HRISTO A. HRISTOV

ABSTRACT: *Some drawbacks of existing tools for defensing the insider threats to information security are analyzed. A description of the modern systems for protecting confidential data against insider threats is given, approaches to detecting confidential data in the information stream and the efficiency of these approaches as well as the basic requirements for such systems. Possible directions of research are specified with the aim to increase the efficiency of the methods for fighting insider threats.*

KEYWORDS:. *Information security, insider threats, contents analysis, context filtering, protection against the leaking of confidential data.*

СРЕДСТВА ЗА ЗАЩИТА НА ЧУВСТВИТЕЛНАТА ИНФОРМАЦИЯ НА ФИРМАТА ОТ ВЪТРЕШНИ ЗЛОЖЕЛАТЕЛИ (ИНСАЙДЕРИ) *

ЛЪЧЕЗАР Т. ХРИСТОВ, СТАНИМИР С. СТАНЕВ, ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *Анализират се недостатъците на съществуващите средства за защита срещу вътрешни заплахи за информационната сигурност. Описани са съвременните системи за защита на поверителни данни от вътрешни заплахи, подходи за признаване на поверителна информация в информационния поток и ефективността на тези методи, както и основните изисквания на такива системи. Възможните посоки на бъдещи изследвания са показани с цел повишаване на ефективността на средствата за борба с вътрешните заплахи.*

1. Въведение

Търговските тайни на компаниите, чувствителната корпоративна информация и личните данни са една от ценностите на днешната икономика, поради което са изложени на повишен риск [21]. Вътрешните заплахи са особено трудно разрешим проблем, защото има много начини вътрешните зложелатели във фирмата (т.нар. „инсайдери”, от англ. insiders) да откраднат информация от корпоративната мрежа. Проблемът на тези заплахи е толкова актуален, че той официално е поставен под номер 2 в списъка на най-трудните проблеми – HPL (Hard Problem List) на Американският съвет за изследване на сигурността на информационните системи – INFOSEC [1].

Според проучването на заплахите за информационната сигурност Global Data Leak Report 17, проведено от Infowatch на водещи корпорации за световните компании заплахата, идваща от вътрешността на корпорациите, посредством инсайдери, е с много по голяма стойност и значимост в глобален аспект в сравнение със заплахите, идващи от външна страна, като тези заплахи нарастват прогресивно във времето на изследвания период 2006-2017г. [2].

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Фиг. 1. Отношение на изтичания, причинени от инсайдери спрямо външни нарушители.

Тази ситуация се наблюдава не само в бизнес корпорациите в национален и световен мащаб. Данните сочат аналогични показатели и в частните (домашни) системи за информационна сигурност [13], [14], [15], [16], [17], [20]. През последните години страхът от вътрешни инциденти от представители на малки и средни предприятия значително се е увеличил. Изтичанията се толерират не само от представители на бизнеса, но и от правителствени агенции по целия свят [18], [19], [20]. „Инсайдерите" са напълно наясно за стойността на информацията, с която те работят, въз основа на ежедневната си дейност. Като резултат, вътрешните кражби на чувствителна информация се увеличават с обезпокоителни темпове, за целта инсайдерите може да използват всяко от стеганографските приложения, достъпни в Интернет като безплатен или Shareware софтуер. Повечето средства за мрежова сигурност и системи за предотвратяването на загуба на данни не откриват употребата на стеганография от вътрешни служители [3].

2. Изложение

Средства и методи за борба с вътрешните заплахи

Защитата на икономическата сигурност е функция на бизнес организацията като цяло и тя се осъществява от нейните структури за сигурност в рамките на тяхната компетентност и в съответствие с възложените им функции и предоставените им сили, средства и методи на дейноста. В тази връзка частните фирми и особено мощните корпорации създават свои специални отдели, които да се занимават с проблемите на сигурността на фирмата. Корпоративните служби за сигурност имат за своя основна цел да се противопоставят на видовете посегателства, нанасящи вреди на интересите на фирмата и поставящи в опасност нейното съществуване и успешно развитие.

Изборът на конкретни мерки за защита зависи до голяма степен от структурата на корпорацията, както и от икономическото състояние на защитаваната организация [4].

Могат да бъдат разграничени няколко вида системи за вътрешна сигурност [5].

Системите за мониторинг и одит са добър начин за разследване на инциденти. Модерните системи за одит позволяват регистрирането на почти всяко действие. Недостатъкът на тези системи е липсата на възможност за предотвратяване на изтичането, защото това изисква система за реагиране на събития и вземане на решения, като се разпознава коя последователност от действия е заплаха и коя не е. В края на краищата, ако отговорът на дадено нарушение не последва незабавно, то последствията от инцидента не могат да бъдат избегнати.

Силните системи за удостоверяване служат за защита срещу неразрешен достъп до данни. Те се основават на дву- или трифакторен процес на идентификация, в резултат на който потребителят може да получи достъп до исканите ресурси. Такива инструменти могат да защитят информацията от "непосветения" служител, но не от вътрешна информация, която вече има достъп до защитена информация [18], [19].

Системите за осигуряване на защитена комуникация служат за защита на предаваната чувствителна информация от неоторизиран достъп. В техния състав влизат различни модули за криптографска и стеганографска защита на информацията предавана между звената на организацията. Използването на надеждни криптографски алгоритми позволява да се осигури надеждно предаване на чувствителна информация [6,7], но от друга страна не скрива факта, че такъв тип информация се обменя между звената. За тази цел е необходимо да се използват програмни средства за стеганографска комуникация [8,9]. Скриването на факта, че се предава чувствителна информация увеличава защитеността на тази информация.

Системи за откриване и предотвратяване на изтичането на данни (Data Leakage Prevention, DLP). Тези системи контролират каналите за изтичане на данни в реално време. Има два основни вида решения - сложни (обхващащи много канали за изтичане) и точка (покриваща определен канал за изтичане). Тези системи използват проактивни технологии, така че не само да регистрират факта на нарушаване на информационната сигурност, но и да предотвратят изтичането на информация. Разбира се, качеството на този контрол директно зависи от способността на системата да разграничава поверителната информация от неповерителната информация, т.е. от алгоритмите за филтриране на съдържание или контекст. Повечето съвременни системи за защита от изтичане на информация имат функциите на криптиране на файлове (такива системи се защита и контрол на информацията (IPC)). Те могат да използват защитени хранилища за данни, по-специално крипто контейнери, които при достъпа до файл вземат предвид не само криптиращия ключ, но и различни фактори като ниво на достъп на потребителите и т.н. Те могат също така да водят поведенчески анализ на потребителя (въпреки че тази технология все още не дава високи резултати) и имат различни приложни функции.

Има фърмуерни средства за защита, които не могат да бъдат пряко отнесени към горните категории, като например външен хардуерен ключ и т.н., но тези инструменти обикновено не разграничават неповерителна информация от поверителна и се явяват реализация на отделни функции на съвременните системи за защита от вътрешни заплахи. Към днешна дата системата за защита от вътрешни заплахи е единственото решение, което помага за предотвратяване на течове в реално време, контролира действията на потребителите и процесите, и може да разпознава поверителна информация в информационния поток. За да се определи уязвимостта на защитата [18], осигурена от такава система, е необходимо да се разгледат по-подробно основните и функции и възможности, както и методите, използвани от тези системи за осъществяване на филтриране на съдържание / контекст.

Производителите на системи за защита срещу течове използват различни технологии за разпознаване на поверителна информация. Всеки производител твърди, че използваните в него продукти се отличават благоприятно от методите на аналоговите програми. Но всички тези методи в съвкупността се основават на синтеза на няколко фундаментално различни подхода.

Търсене на сигнатури. Най-простият метод за филтриране на съдържанието е да търсите последователност от знаци в потока от данни. Понякога забранената поредица от

символи се нарича "спираща дума". Техниката работи само за точни операции и лесно се заобикаля чрез просто заместване на символите в анализирания текст.

Търсене на регулярни изрази (метод на маски). С помощта на някои езици за регулярен израз се дефинира "маска", структура от данни, която е класифицирана като поверителна. Най-често този метод се използва за определяне на лични данни (номер на ЕГН, номер на сметка, документи и т.н.). Недостатък на метода е присъствието на голям брой фалшиви положителни данни, а също така е напълно неприложим за анализа на неструктурирана информация.

Езиков и морфологичен анализ. Техниката се основава на методи за анализ на съдържанието на текстове. Съществува количествен (отчитане на честотата на поява и тегловни коефициенти на думи) и качествен анализ (търсене на споменаване в текста на дадени теми). Морфологичният анализ дава възможност да се работи с езикови словоформи и дава възможност да се разглеждат предложения и да се потърси комуникация с думи. Предполага се, че информацията ще бъде анализирана чрез предварително зададени речници или ключови фрази. Основното предимство на метода е, че той може да открива поверителна информация, предавана в неформална форма. Методът е напълно нечувствителен към броя документи, т.е. базата за филтриране на съдържанието не се променя по размер от появата на нови документи или процеси в компанията. Също така методът е нечувствителен към промяната на отделните думи или тяхната пермутация и зависи от използвания език. За съжаление, използването на такива методи все още дава голям брой грешки от първи и втори вид.

Контейнерният анализ (или контекстуално филтриране) на базата, за разлика от по-горе описаните методи, не се основава на анализ на съдържанието, а на анализ на свойства или характеристики на контейнера с информация. Може да се анализира по вид приложение, подател, получател, както и свойствата на файла или друг контейнер, който съдържа информацията. Примери за този подход са решения, базирани на етикети, които маркират чувствителна информация. Всеки контейнер съдържа етикет, който уникално идентифицира вида съдържание, съдържащо се в контейнера. Тези методи изискват малко изчислителна мощ. Техният недостатък е, че системата се грижи само за маркираната информация: ако етикетът не е доставен, съдържанието не е защитено. Този подход често включва предварителна категоризация на данните, за да се присвоят на файловете атрибути (етикети) и степени на поверителност. Друг недостатък на този подход е изключителната сложност на ръчното изпълнение на категоризацията на файловете (практическа невъзможност с голямо количество информация), поради което е необходимо да се автоматизира процеса на категоризация. За тази цел, има много методи: Статистически (брои честоти думи), вероятността (на базата на теоремата на Бейс "), езикови алгоритми, с помощта на невронни мрежи, вектор (представителството на текста като вектор функция), категоризация на базата на онтологии (формални описания домейни използване на концепции и техните взаимоотношения).

Трябва да се отбележи, че всички горепосочени методи не позволяват да се открива поверителна информация, скрита чрез методите на стеганографията. Съществуват известни разработки в тази насока [10,11]. Съществуващите методи могат да открият случайно изтичане, но не могат да се борят с висококвалифицирани вътрешни лица.

Допълнение към технологиите, използвани за откриване на поверителна информация, системата за защита срещу вътрешни заплахи се характеризира с редица допълнителни изисквания (критерии за принадлежност към системи за защита срещу изтичане). Основните изисквания за този клас системи за защита могат да бъдат дефинирани по следния начин:

- *многоканалност* (възможност за наблюдение на множество канали за изтичане на данни);
- *единно управление* (наличие на за управление и политика по сигурността на информацията, възможност анализ на събитията на всички канали за мониторинг и подробно отчитане);
- *активна защита* (системата трябва не само да открива, но и да предотвратява нарушаване на информационната сигурност);
- *комбинация от анализ на съдържанието и контекста* (в този случай, в допълнение към анализа на контекста етикетите трябва да се възложи анализ на активността на потребителя и приложения).

Системите DLP, представени на пазара, нямат възможност да идентифицират потребителя чрез "типичен портрет на работата в системата". В съществуващите решения се извършва анализ на активността на потребителите, за да се идентифицират незаконни действия и не ви позволява да определите кой всъщност е на компютъра. За целта е необходимо да се пристъпи към видеонаблюдение, което не винаги е възможно на практика.

С течение на времето, технологията, използвана в областта на защитата срещу изтичане се подобри, както и всички използвани конфиденциални методи за разпознаване на информация и комбинации от тях, въз основа на съдържанието и контекста на горните методи, системи. Еволюцията на системите за защита срещу течове може да бъде разделена на три етапа. Първите системи за защита срещу течове използват главно методи за филтриране на съдържанието. Но тяхната ефективност е твърде ниска, защото на практика такива методи дават достатъчно голям процент грешки от първи и втори вид. По този начин максималната вероятност за правилно разпознаване на поверителна информация, използвайки алгоритмите за филтриране на съдържанието в потока от данни (документ, файл, трафик и т.н.) към днешна дата, не надвишава 0,8. И тази вероятност може да се постигне, като се използват всички подходи за анализ на съдържанието (регулярни изрази, подписи, езикови методи и т.н.). Този индикатор е нисък (много по-нисък от заявените характеристики на разработчика) и не отговаря на изискванията за сигурност на информацията.

Системите за защита от течове от второ поколение използват анализ на контейнерите. Този подход включва недвусмисленото определяне на поверителна информация в потока въз основа на файловия атрибут (етикет). Но, въпреки привидната детерминираност, подобна система ще вземе правилното решение, при условие че данните, категоризирани правилно от нея предварително с помощта на съществуващите методи, са правилно категоризирани. Но всички съществуващи методи за категоризация (вероятностни, лингвистични и т.н.) също се основават на методи за филтриране на съдържанието (анализ на съдържанието), които, както беше споменато по-горе, далеч не са съвършени. Необходимо е да се осигури и разработване на процедури за поставяне на етикети на нови и входящи документи, както и на системата за борба с прехвърлянето на информация от табелка контейнер в немаркирана и подсказване при създаване на файлове "от нулата". Всичко това е много сложна задача, също зависи от задачата за анализиране на съдържанието. Както можете да видите, концепцията за детерминистично филтриране не може да се използва отделно от филтрирането на съдържанието и дори теоретично не е възможно да се отървете от методите за филтриране на съдържанието. В идеализирания случай, с вероятността за правилно разпознаване на документ 0.99 и по-висок, можете да

изоставите детерминиращия подход (анализ на контейнера). Но съществуващите алгоритми не позволяват това да бъде направено (минималната сума на грешките от първия и втория вид е> 0,2). Може би с развитието на генетичните алгоритми и технологиите за изкуствен интелект ситуацията може да се промени.

Новото поколение на системи за защита от изтичане (MCC RSKD, информационно-аналитична система за вземане на поверителни данни) обещава да се отърве от недостатъците на съдържание и контекстуални методите за използване на всеки от тях в случаите, когато това е най-ефективен. Но комбинацията от две несъвършени и зависими технологии не може да направи значително подобрение.

3. Заключение

Бизнесът все по-ясно разбира значението на запазването на своите вътрешни секрети и последиците от несанкциониран достъп на конкуренти, терористични организации и чужди разузнавателни сили до тях. Несигурността за бъдещето на организацията пряко кореспондира с изпреварващото определяне и предвиждане на възможни заплахи и посегателства. Въпреки големия брой налични алгоритми за откриване изтичането на поверителна информация, те не са ефективни. Актуализирането на проблема с вътрешните заплахи се дължи на несигурността на техните организации и липсата на ефективно решение за борба с тях. Почти всички предприятия използват софтуерни и / или хардуерни средства за защита, които са предназначени за борба с външни заплахи (антивирус, защитна стена, IDS и т.н.) и са доста ефективни срещу тях. С нарастването на броя на инцидентите използващи методите на социалното инженерство и в частност корумпирането на важни за сигурността служители [12], все по голямо внимание трябва да се обръща на този тип заплахи. Що се отнася до защитата срещу вътрешни заплахи (системи за защита срещу течове), само малка част от фирмите ги използват, въпреки че необходимостта от тези средства обективно съществува. Пазарът на информационната сигурност все още не може да предложи пълно и цялостно решение за ефективна защита на чувствителната корпоративната информация.

ЛИТЕРАТУРА:

[1] Станев, С. и Х. Христов. Роля на фирмените служби за сигурност при организиране на противодействие срещу стеганографски атаки. Сборник трудове на Годишна университетска научна конференция на НВУ "Васил Левски".Секция 5 В.Търново, 2013.

[2] InfoWatch Analytics Center, Global Data Leakage Report, 2017, [онлайн]. https://infowatch.com/sites/default/files/report/Global_Data_Leak_Report_2017_ENG.pdf.

[3] Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. http://www.sarc-wv.com/news/press_releases/2013/steganography_insider_threat.aspx.

[4] Христов, Л. и Х. Христов. Обща характеристика и посегателства върху икономическата сигурност на корпорацията. Международна научна конференция „Политиката на ЕС по защитата на информацията и личните данни“, Шумен, 12-13 април 2018.

[5] Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[6] Kordov, K. M., Modified Chebyshev Map Based Pseudo-Random Bit Generator, AIP CP, 1629, 432-436, 2014.

[7] Kordov, K., Modified pseudo-random bit generation scheme based on two circle maps and XOR function, Applied Mathematical Sciences, Vol. 9, 2015, no. 3, pp. 129-135.

[8] Zhelezov, S., H. Paraskevov, H. Hristov, P. Boyanov, B. Uzunova, An architecture of steganological subsystem for information protection, Proceedings of 10-th International Conference ICBBM, Liepaya, Latvia, 2014, p. 123-128

[9] Zhelezov, S., H. Paraskevov, Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, Volume 8, Issue 20, ISSN:1313-6569, 2015.

[10] Zhelezov, Stanimir. "Modified Algorithm for Steganalysis." Mathematical and Software Engineering 1.2 (2016): 31-36.

[11] Станев, С., С. Железов, and И. Якимов. "Реализация на паралелен стеганализ с клъстерна система." Международна научна конференция" Съвременни методи и технологии в научните изследвания", Варна. 2012.

[12] Василева Р, Методиева Ц, "Международно сътрудничество срещу корупцията. Антикорупционни инструменти на Европейския съюз", Първа научна конференция "Образование, Наука и Иновации", 01-02 декември 2017 г., София.

[13] Добрев, Д., Европа – философия и политика. Издателство „Просвета-София", ISBN 978-954-01-3785-8, 2018 г.

[14] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

[15] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[16] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие "40 години Шуменски университет 1971 - 2011", Шумен, Университетско издателство „Епископ Константин Преславски", ISBN: 978-954-577-620-5, 2011, с. 122-128.

[17] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски", ISBN 978-954-753-207-6, 2014 г.

[18] Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

[19] Boyanov, P., Zhaneta, T., An unauthorized penetration into computer system with activated firewall and antivirus software, Anniversary Scientific International Conference 45 Years Computer Sciences and Engineering Department 30 Years Computer Systems and Technologies Speciality, 27-28 September, 2013, ISSN 1312-3335, Varna, Bulgaria, Section 1 Computer systems and Networks, pp.41-46.

[20] Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks; Information Technology and Security" № 1(3)-2013 УДК 004 (056.5+413.5).

[21] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

Име на автора: докторант Лъчезар Тодоров Христов
Месторабота: Шуменски университет „Епископ Константин Преславски", Факултет по технически науки, катедра „Управление на системите за сигурност"
E-mail: luchano@abv.bg
Име на съавтора: проф. д-р инж. Станимир Стоянов Станев
Месторабота: Шуменски университет „Епископ Константин Преславски"
E-mail: stan_stanev@yahoo.com
Име на съавтора: доц. д-р инж. Христо Атанасов Христов
Месторабота: Шуменски университет „Епископ Константин Преславски", Факултет по технически науки, началник на катедра „Управление на системите за сигурност"
E-mail: h.a.hristov@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 116 - 121 Problems of Security Systems

TENDENCES IN TRAINING POLICE OFFICERS ON SPECIAL POLICE TACTICS

DONCHO HR. TILEV

ABSTRACT: *The tendency of police officers training on a global scale is oriented to improve the practical abilities to work in different venture situations. This method offers assurance accumulation of actions, leading to lower risk situations for both the officers and the citizens. Within the use of more efficient methods for practical schooling of the police officers in Bulgaria will be given the answer of society expectations for more effective strong, professional, and inspiring respect police.*

KEYWORDS: *Compagnie republicaine de securite - police nationale „CRS”.*

ТЕНДЕНЦИИ В ОБУЧЕНИЕТО НА ПОЛИЦЕЙСКИТЕ СЛУЖИТЕЛИ ПО СПЕЦИАЛНА ПОЛИЦЕЙСКА ТАКТИКА*

ДОНЧО ХР. ТИЛЕВ

АБСТРАКТ: *Тенденциите в обучението на полицаите в световен мащаб са ориентирани към повишаването на практическите умения за работа в различни рискови ситуации. Така се дава възможност служителите на реда да натрупат по-голяма увереност в действията си, да се намали риска от неправилни или опасни за тях и гражданите действия. Чрез използването на по-ефективни методи за практическа подготовка на полицаите в България ще се отговори на очакванията на обществото за силна, професионално – компетентна, работеща и вдъхваща уважение и респект полиция.*

1. Въведение

В условията на усложнената международна обстановка, на засиления трафик на нелегални мигранти през българските граници, все по–често ставаме свидетели на неадекватно поведение на служители от правоохранителните органи. Все по–често научаваме за нападения срещу униформени служители. Всичко това ни провокира да изследваме ситуацията и да потърсим къде би могъл да е проблема в подбора на кадрите, в метода на обучение на полицаите или има причини, които водят до професионално прегаряне на служителите и нежелание за качествена работа [1], [2], [3], [4].

Един от основните проблеми на служителите от сектор сигурност е неумението или невъзможността своевременно и правилно да оценяват обстановката, в която трябва да работят и предприемат необходимите мерки за преодоляване на евентуални конфликти. Това неумение ги обрича на неуспех при евентуален сблъсък с нарушителите.

В момента обучението по специална полицейска тактика се извършва по стара френска програма за подготовка на полицаи, адаптирана за нашите условия. В нея е заложено обучение чрез изучаване на определени казуси, които френския научен институт към министерството на вътрешните работи е преценил, че са най–често срещани и на тяхна база следва да се извършва обучението. В момента в България обучението на

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

изпълнителския състав от полицията се извършва в центровете към Академията на МВР, по утвърдена програма [1], [2], [3], [4].
Етапите на първоначалното професионално обучение са базов и специализационен, включващи самостоятелни теоретични и теоретико-практически модули и практически стажове [1], [2], [3], [4].

През базовия етап се придобиват фундаментални теоретико-практически знания за изпълнение на задачите и дейностите на основното структурно звено.

През специализационния етап се придобиват знания и умения за изпълнение на длъжностните задължения на длъжностите от професионалното направление, за което е спечелен конкурсът [1], [2], [3], [4].

Методите които трябва да се използват при обучението на служителите са лекции, упражнения, практически занятия, сюжетни и ролеви игри, консултации, самоподготовка и други. (учебно-планова документация за първоначално професионално обучение на ново постъпили държавни служители – стажанти от НС "полиция" – МВР по противодействие на престъпността, опазване на обществения ред и превенция 2007г.)

2. Изложение

Основните знания и умения се придобиват през базовия етап на обучение, когато се разглеждат споменатите по–горе казуси. Някои от тях са: проверка на документи, проверка на автомобил, запазване на местопроизшествие и др. В лекционния материал се дават основните моменти на които трябва да се обърне внимание, като избор на място, представяне и др., които са в съответствие с действащото законодателство. В стремежа си да бъдат прилежни, много от обучаемите наизустяват лекцията и на практическото занятие, при отиграването на дадения казус , направо цитират казаното от преподавателя. Тези действия водят до шаблонизиране действията на служителите и ако те попаднат в по различна ситуация от тази наизустена от лекцията, се стига до невъзможност своевременно и правилно да оценяват обстановката в която трябва да работят и да предприемат необходимите мерки за преодоляване на евентуални конфликти. Това неумение ги обрича на загуба при евентуален сблъсък с нарушителите или най–малко ги поставя в неловко положение пред извършителите и обществеността. За да излязат от създалата се ситуация някои от служителите прибягват до необоснована агресия – използване на физическа сила и помощни средства, а от там се стига и до жалби за полицейско насилие, или остават безучастни когато видят правонарушение, за да не изпадат в неловко положение [1], [2], [3], [4].

В пресконференция пред медиите на 29.09.17г. по повод изнесена статистика , че с 27% са се увеличили нападенията над униформени служители, министърът на вътрешните работи Валентин Радев заявява" Нашето задължение и това, което ние можем да направим, е да обучим, да акцентираме на полицаите точно как да използват, включително оръжие, когато се самоотбраняват. Или други помощни средства, или дори без средства". Това негово изказване, присъствал журналист коментира: „Защо полицаите имат нужда от подобно обучение, след като то е основна част от професионалната им характеристика, не стана ясно. Те би трябвало да получават такава подготовка преди да излязат на улиците, и опреснителни курсове по време на цялата си кариера". Нападенията са се увеличили не защото криминогенната обстановка се е влошила или защото престъпниците са станали по дръзки, а защото полицаите са по - неподготвени. Такава констатация правят и членове на СФСМВР в интервю от поредицата "Цената на сигурността", която се реализира в партньорство между най-големия синдикат на работещите в системата на МВР СФСМВР и Actualno.com - там се дискутират проблемите свързани с обучението и професионалната

подготовка на служителите в МВР. Разглеждат се възможностите за подобряване на условията на работа и повишаване на квалификацията на кадрите. Според Нелсън Мандела, именно образованието е най-силното оръжие за промяна. Това важи в пълна сила и за системата на МВР. Ако искаме по-квалифицирани кадри и повече ефективност, именно адекватното обучение на служителите е начинът да го постигнем. Известният писател Айзък Азимов твърди, че образованието не е нещо, което може да бъде завършено. Този ключов аспект се оказва неглижиран от управляващите МВР с години, които не създават условия, позволяващи подобряване на уменията и компетенциите на работещите в системата. В това интервю председателят на УС на СФСМВР Валентин Попов, зам.-председателят на УС на СФСМВР Илия Кузманов, зам.-председателят на УС на СФСМВР Радка Павлова, зам.-председателят на УС на СФСМВР Илия Хрисимов, Евгени Крумов, учредител на СФСМВР, председателят на СД37 на СФСМВР Емилиян Недялков посочват следните проблемите свързани с обучението и професионалната подготовка във ведомството [1], [2], [3], [4]:

1. Обучението е формално. В МВР и към настоящия момент се провеждат обучения на служители, но те са формални. Събират се и провеждат някаква форма на дискусия или ако е физическа подготовка – разходка в планината. Горе-долу с това се изчерпва обучението на действащите служители. Формалното изпълнение не позволява придобиване на нови умения, което е от съществено значение за ефективността на служителите. В същото време има служители, които не са получавали възможност за допълнителна квалификация с десетилетия.

2. Проблеми с първоначалното обучение – когато един служител постъпи на работа в МВР, има задължително първоначално обучение от 6 до 9 месеца, което трябва да премине. За съжаление, то също е сведено до абсолютния минимум. Липсва необходимото ниво на подготовка по отношение на стрелба, физическа и теоретична подготовка, което да позволи на служителя да е ефективен при изпълнение на служебните си задължения. Това води до процес на обучение, който продължава паралелно с практиката и отнема 1-2 години, в които служителят не е пълноценен.

3. Обучението по стрелба – истината е, че в МВР се стреля много по-малко, отколкото трябва да се стреля. В същото време, доброто боравене с оръжие е основна предпоставка за спасяване, а не за отнемане на човешки живот. Стрелбите се провеждат в добрия случай веднъж в месеца и с много ограничено количество боеприпаси. Всички тези фактори водят до лоши резултати при боравенето с оръжие от страна на служителите.

4. Физическата подготовка – Следващия път, когато видите полицай с наднормено тегло се замислете, че този човек работи на ненормирано работно време, няма достъп до адекватни съоръжения за поддържане на физическа форма на работа и често работи и извънредно поради дефицита на кадри в системата. Изпити обаче се провеждат, макар да няма условия за подготовка. Още по-трагичното е, че тези изпити имат нормативи, които са еднакви за всички, независимо от възрастта им [1], [2], [3], [4].

5. Кариерното развитие и обучението. Теоретично, кариерното израстване в МВР би следвало да е свързано с допълнителната квалификация и умения придобити от служителите. Обучението би трябвало да разширява възможностите и да увеличава капацитета на служителя. За съжаление това не е така. Няма реална връзка между кариерното развитие в МВР и обучението на кадрите.

Експертите говорят за стрелкова и физическа подготовка, защото са специалисти в това направление, но проблемите са същите и с полицейската тактика, която се явява обединител на цялостната подготовка на полицая. Не е възможно служител със слаба стрелкова, физическа, психологическа или правна подготовка да покаже отлични

резултати по полицейска тактика. В цитираната по- горе наредба е регламентирано, че след първоначалното обучение за придобиване на професионална компетентност, следва и продължаващо обучение, но докато за стрелковата и физическа подготовка е регламентирано колко часа месечно да се провеждат, то полицейската тактика влиза в специализираната полицейска подготовка и дели шестте часа месечно/ регламентирани в програмата за обучение на полицейските служители по специализирана полицейска подготовка без откъсване от работа/с административната, правната и психологическа подготовки, което е крайно недостатъчно. Освен това поне две теми са спуснати от старшата структура, които задължително трябва да бъдат разгледани. Вече е ясно, че часове за полицейска тактика няма, или ако има някакъв инцидент, се прави показ на определени действия от служителите от „групите за задържане" и с това приключва всичко [1], [2], [3], [4].

Чрез използването на по-модерни и ориентирани към практиката методи на обучение може да се повиши ефективността на полицейската подготовка. Например, чрез сюжетните ролеви игри обучаемите ще се научат да мислят и действат съобразно обстановката, а не да се придържат строго към определени статични положения.

Сблъсквайки се с проблема за шаблонното действие на обучаемите и неумението им да действат при различна ситуация, ни провокира в един от центровете за професионална подготовка да въвеждам в обучението на курсистите „ролевата игра". Играта е ситуационна, свързана с определени полицейски правомощия. За целта се разпределяха ролите между обучаемите, като се избираха „полицаи", нарушители и наблюдатели. На всички участници се поставяха конкретни задачи. Всички участници в ролевата игра притежаваха необходимите теоретични знания свързани с конкретната ситуация. .При това подбирахме за ролята на „нарушителите" по–темпераментни , будни и комбинативни курсисти. Целта бе да се създаде максимално реалистична обстановка която да даде възможност на обучаемия да разкрие напълно своите знания и умения. Изпълнението на роли е импровизация, тъй като ситуацията е отворена. Обучаемият се ръководи от действията на своя партньор и натрупаните теоретични знания. Какъв ще бъде нейният край е само предположение. Независимо от това, обаче, играта дава възможност обучаемият да погледне от друга гледна точка и да оцени своето отношение към игровата ситуация, да провери доколко неговите действия се покриват с действията на неговите колеги . След подходящия инструктаж и умелото ръководене на ролевата игра резултатите не закъсняха. Обучаемите бяха разделени на три групи - нарушители , които с действията си насочваха в каква посока ще продължи да се развива играта, полицаи , които изпълняваха определена задача/проверка на документи или автомобил, съобразно изискванията на вътрешно ведомствените документи и действащото законодателство и последната група – наблюдатели. Когато имаше възможност играта на обучаемите се заснемаше с видеокамера [1], [2], [3], [4]. След приключване на играта се провеждаше обсъждане при което „полицаите „пояснявaха защо по този начин са отработили задачата и въз основа на кои нормативни документи. Нарушителите казваха как са почувствали въздействието на „полицаите" върху себе си, могли ли са да избягат, ако искат или контрола е бил качествен, имало ли е прекомерна агресия, или използване на физическа сила. Наблюдателите от своя страна казваха какви грешки са видели в действията на своите колеги. Последни думата вземаха преподавателите, които посочваха слабости или обобщаваха резултата. Отначало имаше доза субективизъм в изказванията на обучаемите, породена от приятелски отношения или други причини, но в последствие курсистите, осъзнаха, че обективната оценка на ситуацията им помага да повишат своите знания и да подобрят уменията в чисто практически план. След това ролите се разменяха. По този

начин възможностите на ролевите симулации се осъществяват напълно. Смяната на ролите позволява светът да се погледне от различен ъгъл, „да влезеш в обувките на другия…[1], [2], [3], [4]”

С всяка следваща смяна на ролите, обучаемите започваха да допускат все по–малко грешки и все по уверено да аргументират своите действия. Чрез ролите се насочваше вниманието на полицаите към нов начин на мислене, а от там се променяше тяхното поведение, отношение към ситуацията и очакванията. Поставени в различна обстановка обучаемите имат възможност да усъвършенстват комуникативните си способности, правилното и точно мислене, изразяване и действие. В последствие при нестандартно променена ситуация полицаите не се стъписваха вече, а търсиха подходящия начин да решат ситуацията и регламентиращ документ, обуславящ техните действия при документалното оформяне на случая. Използването на физическа сила и помощни средства се сведе до минимум, обучаемите станаха по уверени в своите знания и умения, придобиха самочувствие и с държанието си вдъхваха респект в „нарушителите”. Изпълнявайки различни роли полицаите започнаха по бързо да възприемат конкретната ситуация, оценяваха обстановката, и предприемаха правилните действия за да решат случая . По този начин скъсиха времето за наблюдение, оценка, решение и действие /НОРД/ цикъла и действията им станаха по оперативни. Какво представлява НОРД цикъла [1], [2], [3], [4]?

Сърцевината на специалната тактика е тактическото мислене.

Използването на определен модел за мислене, осигурява предимство във високорисковите ситуации. В основата на този модел е умението бързо да се възприеме действителността, да се направят необходимите изводи, да се вземе решение и да се приведе в действие. Този модел е известен от 60-те години на XX век и е известен със съкращението НОРД описан в книгата на И. Станчев „ Тактически действия при високо рискови ситуации”[8]. Съкращението е от началните букви на думите наблюдение, оценка, решение, действие. Тази последователност от дейности са елементите на разглеждания мисловен модел, приложим във високорисковите-ситуации. Във всеки потенциален или реален сблъсък се наблюдава обстановката, за да се получи информация за местоположението и състоянието на извършителите на престъпления и обкръжаващата среда. Събраната информация дава възможност да се направи оценка, оценка на престъпника; на служителите от действащия екип; на мястото, времето и други елементи (фактори) на обстановката, които влияят върху действията. Въз основа на тази оценка се взема решение какво и как трябва да се направи. Следва изпълнение на решението чрез извършване на определено действие – това представлява един цикъл: Наблюдение, Оценка, Решение, Действие.

След действието обстановката отново се променя, което налага НОРД-цикълът да започне отново. Този цикъл е непрекъснат. Динамиката на промените в обстановката налагат наблюдението, оценката, решението и действията да се извършват с максимална бързина [1], [2], [3], [4].

Ако в определена конфронтация (високо-рискова ситуация) една от противоборстващите страни може по-бързо и по-ефективно да наблюдава, да оценява, да взема решение и да действа по-динамично може да се каже, че е налице тактическо предимство. По-високата скорост на провеждане на циклите дава възможност да се поддържа по-високо темпо на действията. Страната (дори и по-силната, физически или технически), която реагира по-бавно не успява да реализира пълноценно своите възможности, тъй като не е в състояние да се ориентира в настъпващите промени. Чрез използването на ролеви игри в обучението на полицаите и поставянето им в

нетрадиционни ситуации се постигна повишаване на скоростта на НОРД цикъла им , а от там се осигури и по голямо тактическо предимство при решаване на поставените им задачи [1], [2], [3], [4].

3. Заключение

Тенденциите в обучението на полицаите в световен мащаб са ориентирани към повишаването на практическите умения за работа в различни рискови ситуации. Така се дава възможност те да натрупат по-голяма увереност в действията си и да се намали риска от неправилни или опасни за тях и гражданите действия.

Би следвало професионалното обучение на полицаите в България да следва тези тенденции като това е въпрос на желание и воля от страна на всички заинтересовани полицията да биде реален и ефективен стожер на реда и сигурността в страната.

ЛИТЕРАТУРА:

[1] "Цената на сигурността" - Actualno.com

[2] „НАРЕДБА № 8121з-433 МВР

[3] Учебно-планова документация за първоначално професионално обучение на ново постъпили държавни служители – стажанти от НС “полиция” – МВР по противодействие на престъпността, опазване на обществения ред и превенция 2007г.

[4] Станчев И. „Тактически действия при високорискови ситуации” В. техника 2003г.

Име на автора: докторант Дончо Христов Тилев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail:

GDPBZN ACTIVITIES OF SAFETY AND PROTECTION

DONIKA V. DIMANOVA

ABSTRACT: *Protection of the population from disasters is a complex activity which is planned and conducted by the executive authorities. In case of danger or occurrence of disasters, GDPBZN performed coordination constituent parts of the rescue system, through its operating centers managing and coordinating rescue and restoration works. The Directorate is one of the main structural units, related to the protection of the population and the national economy.*

KEYWORDS:. *Protection of the population, disasters, unified rescue system, preventive activities, emergency restoration works.*

ДЕЙНОСТИ НА ГДПБЗН ПО БЕЗОПАСНОСТ И ЗАЩИТА*

ДОНИКА В. ДИМАНОВА

АБСТРАКТ: *Защитата на населението при бедствия е комплексна дейност, която се планира и провежда от органите на изпълнителната власт. В случай на опасност или възникване на бедствия, ГДПБЗН извършва координацията на съставните части на единната спасителна система, чрез оперативните си центрове, като ръководи и координира спасителните и аварийно-възстановителните работи. Дирекцията е една от основни структурни звена, свързани със защитата на населението и националното стопанство.*

1. Въведение

След промените в Закона за МВР от 1 януари 2011 г. Главна дирекция „Пожарна безопасност и спасяване” и Главна дирекция „Гражданска защита” са обединени. Функциите по осигуряване на пожарна безопасност, спасяване и защита при бедствия се извършват от обособената специализирана структура на МВР – Главна дирекция „Пожарна безопасност и защита на населението“ (ГДПБЗН), при условията и по реда на Закона за МВР и Закона за защита при бедствия (ЗЗБ).

В случай на опасност или възникване на бедствия, ГДПБЗН извършва координацията на съставните части на единната спасителна система, чрез оперативните си центрове, като ръководи и координира спасителните и аварийно-възстановителните работи. Дирекцията е една от основни структурни звена, свързани със защитата на населението и националното стопанство.

В тази връзка целта на изложението е да се направен анализ на дейността на ГДПБЗН, свързана с безопасността и защита на населението при пожари, бедствия и извънредни ситуации.

2. Дейности на ГДПБЗН по защита при пожари, бедствия и извънредни ситуации

ГДПБЗН е национална специализирана структура на МВР за осъществяване на дейности по осигуряване на пожарна безопасност и защита при пожари, бедствия и

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

извънредни ситуации, при условията и по реда на закона за МВР и на Закона за защита при бедствия.

Дейностите на ГДПБЗН по осигуряване на пожарна безопасност и защита при пожари, бедствия и извънредни ситуации се определят с наредби на министъра на вътрешните работи (Закон за МВР, чл.17, ал.2.) и се осъществяват чрез [1,4,8]:

- Превантивна дейност и превантивен контрол;
- Държавен противопожарен контрол;
- Пожарогасителна и спасителна дейност;
- Разрешителна и контролна дейност на търговци, извършващи дейности по осигуряване пожарната безопасност на обекти и/или поддържане и обслужване на уреди, системи и съоръжения, свързани с пожарната безопасност;
- Оценяване на съответствието и контролната дейност на продукти за пожарогасене;
- Методическа и експертна помощ;
- Информационно-аналитична дейност;
- Неотложни аварийно-възстановителни работи, оперативна защита при наводнения, операции по издирване и спасяване, химическа, биологическа и радиационна защита;
- Ранно предупреждение и оповестяване при бедствия и при въздушна опасност на органите на изпълнителната власт и населението [9], [10];
- Методическа и експертна помощ на териториалните органи на изпълнителната власт по отношение на защитата при бедствия и при организиране на дейността на доброволните формирования;
- Определяне на пожарните характеристики на продукти и техническите и експлоатационните показатели на пожаротехническо оборудване и продукти за пожарогасене.

Превантивна дейност и превантивен контрол. Превантивната дейност се осъществява от органите на ГДПБЗН към МВР съвместно с органите на държавната власт, местното самоуправление, юридическите лица и гражданите при оказване на експертна и методическа помощ. Основната ѝ цел е намаляване на риска от бедствия. Превантивната дейност е регламентирана в Закона за защита при бедствия и включва [1,2,3,8]: анализ и оценка на рисковете от бедствия; картографиране на рисковете от бедствия; планиране намаляването на риска от бедствия; разработване и изпълнение на програми и проекти за намаляване на риска от бедствия [9], [10]; категоризиране на населените места в зависимост от броя на потенциално засегнатото население; установяване на критичните инфраструктури и обектите им и оценка на риска за тях; мерки за защита на критичните инфраструктури; планиране на защитата при бедствия; определяне на норми за устройственото планиране на територията, проектирането, изпълнението и поддържането на строежите във връзка с намаляване на риска от бедствия; изграждане и поддържане на системи за наблюдение, ранно предупреждение и оповестяване; осигуряване на места и условия за временно настаняване на пострадали (засегнати) при бедствия; осигуряване на колективни и индивидуални средства за защита; обучение и практическа подготовка на централните и териториалните органи на изпълнителната власт, силите за реагиране, доброволните формирования и населението [9], [10].

Освен изброените, превантивната дейност обхваща ѝ планирането, подготовката и провеждането на учения и обучение на населението, детските градини и училищата, за защитата при пожари, за формиране на необходимото поведение при бедствия и извънредни ситуации и за прилагане на необходимите защитни мерки.

Превантивния контрол е комплекс от мероприятия за контрол по спазването на нормативната уредба, свързана със защитата при бедствия. Чрез него се извършват мероприятия за контрол по спазване на изискванията за защита при бедствия, регламентирани в Закона за защита при бедствия, издадените въз основа на него подзаконови нормативни актове и в случаите, предвидени в други закони.

За осъществяване на превантивен контрол органите на ПБЗН извършват [6]:

• контрол за спазване на нормативната уредба при одобряването на устройствени схеми и планове, съгласувателни процедури на обекти, осъществяващи дейност с рискови вещества и материали, и участие в държавни приемателни комисии;

• контрол по изготвяне и съгласуване на аварийни планове;

• контрол на дейностите по защита и на средствата за защита на работещите в обекти представляващи строежи първа и втора категория. Това са обекти, криещи опасност от взрив, от значително вредно въздействие върху околната среда или от разпространение на отровни или вредни вещества. Към строежите първа категория спадат и хидротехнически съоръжения, криещи опасност от наводнения, в т.ч. големи язовири и язовири от първа степен на потенциална опасност и прилежащите им съоръжения и временно строителство. Към строежите втора категория са включени сгради и съоръжения за обществено обслужване с капацитет над 1000 места за посетители;

• контрол за спазване изискванията на Закона за защита при бедствия и издадените въз основа на него подзаконови актове;

• контрол за спазване на инженерно-техническите правила за защита от бедствия и аварии на строежи и на въведени в експлоатация обекти.

Държавен противопожарен контрол. Държавния противопожарен контрол е дейност на ПБЗН, при който дирекцията извършва основно проверки за спазване на правилата и нормите за пожарна безопасност при проектиране, строителство и експлоатация на различни обекти, както и на дейности в земеделските земи. В правомощията на ПБЗН е да издават писмени разпореждания или уведомления, и да изисква документи и сведения, за осигуряването на пожарната безопасност от държавни органи, организации, юридически лица и граждани. При упражняването на държавния противопожарен контрол, структурите на ПБЗН участват в експертни съвети и държавни приемателни комисии, като дават становища и оценка за съответствие с правилата и нормите за пожарна безопасност на инвестиционните проекти, както и на строежите във връзка с въвеждането им в експлоатация. Те имат право да издават сертификати и други документи свързани с пожарната безопасност, когато това е предвидено в нормативен акт.

Държавният противопожарен контрол включва [3,4,5,8]:

• контрол за спазването на правилата и нормите за пожарна безопасност при проектиране, строителство и експлоатация на обектите, при тяхната реконструкция, основно обновяване, основен ремонт или промяна на предназначението, както и при поставяне на премествaеми обекти за търговски и други обслужващи дейности - павилиони, кабини, маси, зарядни колонки за електрически превозни средства, както и други елементи на градското обзавеждане (спирки на масовия градски транспорт, пейки, осветителни тела, съдове за събиране на отпадъци, чешми, фонтани, часовници и други);

• контрол за съответствието на влаганите в строежите и обектите продукти с нормативните изисквания за пожарна безопасност;

• контрол по спазване на изискванията за пожарна безопасност при други дейности, които създават опасност за възникване на пожари и застрашават живота и здравето на

гражданите, както и в случаите, предвидени в други закони, министърът на вътрешните работи съвместно със съответния министър издават наредби.

Пожарогасителна и спасителна дейност. Пожарогасителната и спасителна дейност се организира и осъществява от териториалните структури на ГДПБЗН, секторите „Специализирани оперативни дейности“ към РД, самостоятелно или съвместно със специализираните сили и средства на органите на изпълнителната власт, организациите, юридическите лица, гражданите, търговците или с доброволните формирования.

Пожарогасителната дейност включва [1,8]:

• определяне на способите, начините и средствата за пожарогасене и спасяване;

• разработване на планове за ликвидиране на бедствия и аварии;

• незабавно изпращане на сили и средства при пожари, бедствия и аварии;

• спасяване на хора и имущество;

• ограничаване и ликвидиране на пожари, както и последствията от бедствия и аварии;

• оказване на първа медицинска помощ на пострадалите и транспортирането им до болничните заведения.

За осъществяване на пожарогасителни и спасителни дейности, органите на ПБЗН е необходимо да работят на непрекъснат сменен режим, да разработват планове за пожарогасене, да изучават оперативната обстановка на обектите, да поддържат в готовност налична техника, специализирано оборудване и спасителни екипи за провеждане на дейности за защита на населението и оказване на първа медицинска помощ. Важен фактор е взаимодействието с органите на държавната власт, местното самоуправление, юридическите лица и гражданите.

Таблица 1. Обучение и подготовка на централните и териториални органи

	ГОДИНА	ОБЛАСТНО НИВО						ОБЩИНСКО НИВО						ОБЕКТОВО НИВО					
		Учебни сборове	Комплексни учения	Тренировки на щаба за координация	**Общ брой мероприятия**	Участвали от ГДПБЗН	Участвали от ЕСС (брой)	Учебни сборове	Комплексни учения	Тренировки на щаба за координация	**Общ брой мероприятия**	Участвали от ГДПБЗН	Участвали от ЕСС (брой)	Учебни сборове	Комплексни учения	Тренировки на щаба за координация	**Общ брой мероприятия**	Участвали от ГДПБЗН	Участвали от ЕСС (брой)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Регионални дирекции общо за страната	**2017**	64	9	40	113	461	1089	139	22	246	407	449	3568	278	287	618	1183	689	800
	2016	47	7	41	95	559	1220	168	41	298	507	475	3212	246	457	655	1358	545	754
	2015	70	6	39	115	394	1426	173	31	285	489	546	5166	318	461	574	1353	460	429
	2014	50	9	43	102	428	1039	138	30	250	418	389	2954	167	233	650	1050	398	419
	2013	47	3	36	86	474	1216	166	28	195	389	559	2348	56	157	340	553	358	494
	2012	45	5	51	101	363	1436	155	63	228	446	435	2100	95	166	177	438	475	507
	2011	38	5	32	75	315	1184	149	26	227	402	474	2310	104	134	139	377	434	610
РДПБЗН ШУМЕН	**2017**	1	0	2	3	10	8	12	0	17	29	29	8	2	65	12	79	130	0
	2016	0	1	1	2	0	0	12	0	4	16	7	160	3	58	2	63	180	240
	2015	1	0	1	2	5	0	7	1	6	14	15	60	2	0	12	14	58	0
	2014	1	0	0	1	2	9	8	1	4	13	20	15	2	2	22	26	13	0
	2013	1	0	0	1	2	0	7	0	3	10	10	0	6	5	53	64	35	0
	2012	1	1	0	2	7	41	1	2	1	4	10	114	4	8	14	26	36	0
	2011	0	1	3	4	3	25	1	0	3	4	3	56	0	1	4	5	7	39

Спасителната дейност включва [1,8]:
• начините и средствата за извършване на дейността;
• незабавно изпращане на сили и средства при бедствия, аварии и катастрофи;
• ограничаване и ликвидиране на последствията от бедствия, аварии и катастрофи;
• спасяване на хора и имущество;
• оказване на първа медицинска помощ на пострадалите;
• организиране транспортирането на пострадалите до лечебните заведения.

Методическа и експертна помощ от органите на ПБЗН се оказва на териториалните органи на изпълнителната власт по отношение на защитата при бедствия и при организиране на дейността на доброволните формирования. В таблица 1 е представен броя и видовете обучения и подготовка по ПБЗН на областно, общинско и обектово ниво, а в таблица 2 видовете и броя проведени обучения на населението за периода 2011-2017 г.

Таблица 2. Проведени обучение и занятия с населението

	ГОДИНА	Занятия с деца, ученици и студенти		Занятия със служители от системата на МОМН		Занятия с ДА и общинска адм.		Занятия в обекти от КИ		Занятия в други обекти		Занятия с ДФ		Занятия с неработещо население и пенсионери	
		БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ	БР. ЗАНЯТИЯ	БР. УЧАСТНИЦИ
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Регионални дирекции общо за страната	**2017**	6045	268055	1799	27293	481	13712	226	6442	2069	36070	849	3428	486	9695
	2016	4495	247363	1496	26823	553	13192	272	7140	2615	41870	427	3151	231	8277
	2015	4362	148239	1196	23864	447	13701	187	6277	1938	32389	362	2423	151	11925
	2014	4285	205694	1205	24082	6157	15808	2192	4155	1555	32002	1450	7451	128	12911
	2013	4699	644075	952	16256	406	12428	312	5126	1884	28879	1470	3026	193	17986
	2012	4831	218634	1277	16923	426	8099	388	5437	2213	31965	131	1859	351	11414
	2011	5362	139189	1476	14601	360	10464	686	10332	2171	25845	277	2152	270	13182
РДПБЗН ШУМЕН	**2017**	184	2829	26	982	11	354	0	0	97	904	11	120	2	18
	2016	197	2301	25	621	21	726	2	280	134	957	10	120	10	144
	2015	168	1703	27	524	15	561	3	320	14	416	11	96	1	67
	2014	217	2201	26	503	17	519	11	329	75	590	18	107	1	67
	2013	165	4831	106	1358	24	896	55	276	88	1443	125	70	0	0
	2012	254	4834	39	331	7	187	65	423	184	1436	0	0	4	114
	2011	435	5082	99	389	3	157	6	82	57	768	2	59	6	936

Лицата, които не са служители на МВР или военнослужещи от МО и желаят доброволно да участват в дейности, свързани със защита на населението при бедствия, пожари и извънредни ситуации, могат да станат доброволци. Кандидатстването, набирането и обучението на доброволци е уредено със закон (Закон за МВР, Закон за защита при бедствия, Наредба за реда за създаване и организиране на дейността на доброволните формирования за предотвратяване или овладяване на бедствия, пожари и извънредни ситуации и отстраняване на последиците от тях и др.).

Информационно-аналитична дейност на ГДПБЗН. Информационно-аналитичната дейност включва събиране, обработване, съхраняване и анализиране на информация от системите за наблюдение на Националния оперативно комуникационно-информационен

център, Центъра за аерокосмическо наблюдение, оперативните комуникационно-информационни центрове на МВР и др., с цел управлението на риска от бедствия и координацията на съставните части на единната спасителна система. Информацията се използва и предоставя за [1,8]:

• възникнали пожари, аварии, бедствия, катастрофи, други инциденти и извършената дейност от службата;

• превантивните и административно наказателните мерки;

• стратегическите и особено важните обекти;

• противопожарната и спасителната техника, въоръжение и гасителни средства;

• плановете за ликвидиране на последиците от пожари, аварии, бедствия и катастрофи;

• издадените разрешения на търговци, извършващи пожарогасителна или аварийно-спасителна дейност или противопожарно обследване на обекти.

Събраната статистическа информацията при необходимост се предоставя за нуждите на ръководството на МВР, ГДПБЗН, другите държавни институции и държавни органи, юридически лица и граждани, които имат законен интерес и основание да я получат. За целта в ГДПБЗН се поддържат няколко автоматизирани информационни системи.

Една от основните е Автоматизирана информационна система „Произшествия” в РДПБЗН. В нея се въвеждат, съхраняват и обработват данни за пожари, промишлени аварии, бедствени ситуации, катастрофи, в ликвидирането на които или отстраняването на последиците от тях са участвали структурните звена на ГДПБЗН към МВР.

В таблица 3 са представени данни за броя произшествия и излизания на противопожарна и спасителна техника в периода 2011-2017 г. общо за ГДПБЗН, съгласно информацията от АИС "Произшествия".

Таблица 3. Брой и видове произшествия на противопожарна и спасителна техника в периода 2011-2017 г.

Регионални дирекции общо за страната	ГОДИНА	ПОЖАРИ			СПАСИТЕЛНИ ДЕЙНОСТИ ПРИ:										ВСИЧКО ПРОИЗШЕСТВИЯ (пожари и спасителни дейности)	ПОМОЩ НА ДР. РСПБЗН
		ПОЖАРИ С МАТЕРИАЛНИ ЗАГУБИ	ПОЖАРИ БЕЗ МАТЕРИАЛНИ ЗАГУБИ	ОБЩО ПОЖАРИ	ОКАЗВАНЕ ПОМОЩ НА ПОСТРАДАЛИ ГРАЖДАНИ	БЕДСТВИЯ	АВАРИИ	БИТОВИ / ПРОМИШЛЕНИ ИНЦИДЕНТИ	ИНЦИДЕНТИ С ОПАСНИ ВЕЩЕСТВА И МАТЕРИАЛИ	ИНЦИДЕНТИ С ИЗТОЧНИЦИ НА ЙОНИЗИРАЩИ ЛЪЧЕНИЯ	ОКАЗВАНЕ НА ПОМОЩ, ИЗДИРВАНЕ И/ИЛИ СПАСЯВАНЕ	КАТАСТРОФИ С ТРАНСПОРТНИ СРЕДСТВА	ТЕХНИЧЕСКА ПОМОЩ	ОБЩО СПАСИТЕЛНИ ДЕЙНОСТИ		
	2017	9120	26362	35482	227	43	141	236	205	5	270	1352	11937	14416	49898	1837
	2016	9058	28304	37362	292	190	101	269	273	4	297	1652	11242	14320	51682	2021
	2015	8656	21353	30009	303	269	114	308	357	15	390	1558	14392	17706	47715	1563
	2014	7781	15417	23198	420	703	207	469	465	16	587	1423	16313	20603	43801	1494
	2013	8503	24401	32904	332	70	218	419	487	11	376	1306	10019	13238	46142	1828
	2012	9728	35203	44931	571	700	170	415	648	18	456	1201	13688	17867	62798	2454
	2011	9487	32403	41890	605	153	10	556	681	0	0	1362	9030	12397	54287	1629

За подпомагане при вземането на информирани управленски решения при природни бедствия, големи промишлени аварии и транспортни катастрофи в ГДПБЗН към МВР са внедрени ГИС и CAD информационни системи. Чрез тях могат да се анализират и визуализират географски и пространствени данни, които да моделират и създадат карта на

конкретно природно бедствие. Така се увеличава възможността за незабавна реакция на основните сили и средства за защитата на гражданите, стратегическите и потенциално опасни обекти от националното стопанство.

Неотложни аварийно-възстановителни работи. Те се извършват от ГДПБЗН и териториалните ѝ звена самостоятелно или съвместно със специализираните сили и средства на органите на изпълнителната власт, организациите, юридическите лица, доброволните формирования и гражданите. НАВР започват с въвеждането в изпълнение на съответния план за защита при бедствие или авариен план и се провеждат по решение на ръководителя на операцията, непрекъснато до завършването им или до отмяната на бедственото положение в случай, че такова е обявено [1]. При тях приоритетно се извършват дейности за осигуряване на живота и здравето на населението.

Оперативна защита при наводнения. Защитата при наводнения е регламентирана в Инструкцията за условията и реда за осъществяване на оперативна защита при наводнения. Тя се осъществява от органите на ГДПБЗН на общинско, областно и национално ниво. Обособени са три фази: непосредствена опасност от наводнение, наводнение и след наводнение. Дейностите по оперативна защита се координират от ръководителя на съответното звено на ПБЗН към МВР, който организира взаимодействието между частите на ЕСС.

Операции по издирване и спасяване. Тези операции включват откриване на местонахождението на хора, попаднали в беда и извеждането им на безопасно място. Най-често обхващат операции по издирване и спасяване във водна среда, по суша (използване на алпийски техники) и при авиационни произшествия. Основните дейности по издирване и спасяване са регламентирани с Инструкция за условията и реда за осъществяване на операции по издирване и спасяване.

Химическа, биологична и радиационна защита. Дейностите по химическа, биологична и радиационна защита се извършват от ГДПБЗН на МВР и териториалните ѝ звена съгласно Националния план за защита при бедствия и Закона за защита при бедствия. Те се организират от ръководител на операцията, който организира взаимодействието между частите на ЕСС. Химическата, биологичната и радиационната защита включват: мерки за предотвратяване или намаляване на последиците от инцидента и аварията за населението и околната среда, оказване на помощ на пострадалите и ликвидиране на последиците от инцидента и аварията.

Ранно предупреждение и оповестяване при бедствия и при въздушна опасност на органите на изпълнителната власт и населението. Тази дейност е регламентирана в Наредбата за условията и реда за функциониране на НСРПО на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност. Тя се осъществява чрез Националната система за ранно предупреждение и оповестяване, която по същество е комуникационно-информационна система, състояща се от две подсистеми. Едната е насочена към населението на страната, а другата към органите на изпълнителната власт и съставните части на ЕСС.

Ранно предупреждение и оповестяване се извършва от оперативните дежурни в националният оперативен център на ГДПБЗН - МВР или в оперативния център на РДПБЗН и от дежурните длъжностни лица в областните и общинските администрации, кметствата и в обекти, чиито производства са свързани с рискови вещества и материали [2].

3. Заключение

Защитата на населението при бедствия е комплексна дейност, която се планира и провежда от органите на изпълнителната власт. Чрез своята дейност те организират и координират [3, 7]:

- Анализа, оценката и прогнозата за характера и последствията от най-често проявяващите се бедствия;
- Разработване и актуализиране на планове за защита при бедствия;
- Провеждане на мероприятия за усвояване на плановете;
- Поддържане на непрекъснато денонощно дежурство;
- Формиране и поддържане на сили и средства за провеждане на СНАВР във възникналите огнища на поражения (заразяване) на територията на страната;
- Създаване на организация за действие и взаимодействие между органите за управление и силите за провеждане на мероприятия по защитата на населението и извършване на СНАВР;
- Поддържане в добро състояние на общинските и местните пътища;
- Защита на водоизточниците, поддържане на готовност при недостиг на питейна вода за осигуряване на допълнителни пунктове за снабдяване с вода и включване във водоснабдителната система на допълнителни водоизточници;
- Осигуряване (в министерствата, ведомствата и в техните структури) на финансови и материални средства за комплектуване, обучение и поддържане в постоянна готовност на органите за управление и силите за реагиране при бедствия;
- Дейности по осигуряване на производството и доставката на основни строителни материали за нуждите на неотложните аварийно-възстановителни работи;
- Участие на дружествата със строително-монтажна и пътно строителна дейност във възстановителните работи и по осигуряване и поддържане на пътища;
- Организиране на експертни и проектантски екипи за участие в работата по планиране на защитата и инженерното осигуряване на спасителните и аварийните дейности;
- Информиране на населението за възможните бедствия на територията на страната, както и за правилата за действие и поведение при възникването им.

Дейностите на ГДПБЗН по безопасност и защита се извършват и в съответствие със стратегическите цели и приоритети, произтичащи от пълноправното членство на България в Европейския съюз, НАТО и други международни организации. Международното сътрудничество се реализира в рамките, определени от националното законодателство и международните договори, по които Република България е страна.

ЛИТЕРАТУРА:

[1] Диманова, Д., Защита при бедствия, аварии и катастрофи. УИ Епископ Константин Преславски, Шумен (2016).

[2] Kuzmanov, Z., Kuzmanova, E. Public order and public security. Annual of Konstantin Preslavski University of Shumen, Vol. VII E, Faculty of Technical Sciences, ISSN 1311-834X (2017).

[3] Закон за защита при бедствия, изм. и доп. ДВ. (бр.97/5.12.2017).

[4] Закон за МВР, изм. ДВ. (бр.55/3.07.2018).

[5] Наредба № 8121з-882 за реда за осъществяване на държавен противопожарен контрол, обн. ДВ, бр. 100/5.12.2014, изм. ДВ. (бр. 15/16.02.2018).

[6] Наредба № 8121з-758 за осъществяване на превантивна дейност от органите за пожарна безопасност и защита на населението на МВР, обн. ДВ. (бр. 90/30.10.2014).

[7] Национален план за защита при бедствия, с.23, МС София (2010).

[8] http://www.nspbzn.mvr.bg/Za_NSPBZN/Deinost (26.08.2018).

[9] Христо А. Христов. Координация, взаимодействие и сътрудничество при преодоляване на кризи, породени от бедствия и аварии. Научна конференция с международно участие „Облачните структури и защитата на информацията“ НВУ „Факултет А,ПВО и КИС“ –Шумен, 12-13 май 2016 г., ISSN: 1314-3921, т. 2, 2016, стр. 210-216.

[10] Христов, А., Андреев, А., Оптимизиране дейността на структурите за бърза реакция при кризи, чрез използване на екипи по TASK-FORCE принцип. Научна конференция с международно участие „MATTEX“, ШУ „Еп. К. Преславски“ 11-13ноември 2016 г., ISSN: 1314-3921, т. 2, 2016, стр. 72-76.

Име на автора: доц. д-р инж. Доника Величкова Диманова
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: d.dimanova@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 131 - 138 Problems of Security Systems

INTERNATIONAL SECURITY STANDARDS

DONIKA V. DIMANOVA, ZDRAVKO YU. KUZMANOV

ABSTRACT: *Standardization is an essential part of the economy of countries and plays an important role in integrating it into the single European market. Standards harmonize requirements for goods and services, which facilitates international trade. Applying the different standards helps ensure consistent product quality and improves productivity. This in turn helps to increase consumer confidence. The report will analyze key international security standards, particularly those relating to information security.*

KEYWORDS:*.International, standards, ISO, ITU, NIST, ETSI, security, information security.*

МЕЖДУНАРОДНИ СТАНДАРТИ ЗА СИГУРНОСТ*

ДОНИКА В. ДИМАНОВА, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *Стандартизацията е съществена част от икономиката на държавите и играе важна роля за нейното интегриране в единния европейски пазар. Чрез стандартите се уеднаквяват изискванията към стоките и услугите, което улеснява международната търговия. Прилагането на различните стандарти съдейства за осигуряване на постоянното качество на продуктите и подобрява производителността. Това от своя страна спомага за по-голямото доверието на потребителите. В доклада ще бъдат анализирани основните международни стандарти свързани със сигурността и в частност с информационната сигурност.*

1. Въведение

Стандартът [1,4] е документ, който предвижда изисквания, спецификации или характеристики, които да гарантират, че продуктите, процесите и услугите са безопасни, надеждни и с добро качество. Стандартите се изработват доброволно от национални органи по стандартизация от различни страни, обединени в Международната организация по стандартизация ISO (International Organization for Standardization).

Съгласно Директива (ЕС) 2015/1535 на Европейския парламент и на съвета от 2015 стандартът е *„…техническа спецификация, одобрена от призната организация по стандартизация за многократно или непрекъснато приложение, съответствието с който не е задължително и която има една от следните разновидности: международен стандарт-стандарт, приет от международна стандартизационна организация и предоставен на разположение на обществеността; европейски стандарт-стандарт, приет от европейски орган по стандартизация и направен достояние на обществеността; национален стандарт-стандарт, приет от национален орган по стандартизация и предоставен на разположение на обществеността”.*

Националният орган за стандартизация в България е Българският институт за стандартизация (БИС).

Освен международните, европейските и националните стандарти, за да се осигури по-голяма гъвкавост се разработват и други видове стандартизационни документи. Това са

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

технически спецификации, технически доклади, споразумения и ръководства. Разработването и одобряването на тези документи също става от стандартизационни органи, но процедурите са по-опростени и това позволява своевременно да бъдат удовлетворени нуждите на пазара по отношение на технически изисквания и информация.

Разработват се само стандарти, които се изискват от пазара и които в последствие ще бъдат прилагани. До момента са публикувани над 20500 международни стандарта. За бизнеса, те са стратегически инструменти, чрез които могат да се намалят разходите, да се увеличи производителността и конкурентоспособността. Издаването на международните стандарти от Международната организация по стандартизация, представлява постигане на международен консенсус за състоянието на технологиите или съответните дейности.

В тази връзка целите на изложението са да бъдат анализирани стандартите свързани със сигурността (екологичната, мрежова, интернет сигурност, както и защита на критичната информационна инфраструктура) и в частност с информационната сигурност.

2. Международни стандарти свързани със сигурността

През 90-те години на XX век проблемите, свързани с околната среда и заплашването на човечеството с екологични катастрофи, стават причина за започването на работа на Международната организация по стандартизация и разработването на стандарта за управление на околната среда BS8800 (по-късно преобразуван в ISO 14001:1996). Следват разработки на много други стандарти, определящи изискванията за система за управление на здравето и безопасността при работа OHSAS 18001:1999, стандарти, свързани с IT сектора и защита на информационната сигурност BS 7799 (по-късно преобразуван в ISO 27001), докато се стигне до модели на стандарти, базирани на управлението на риска ISO 31000.

Освен Международната организация по стандартизация съществуват и други организации и институти, които са признати и разработва стандарти, препоръки и ръководства свързани със сигурността [8], [9], [10]. На някои от тях ще бъде направена кратка характеристика.

ITU - Международния съюз по далекосъобщения (*International Telecommunication Union*), подобно на ISO издава препоръки в областта на киберсигурноста. Като най-популярни сред тях могат да се отбележат: X.1205 - Преглед на киберсигурноста; E.408 - Изисквания за сигурност на телекомуникационните мрежи; X.509 – Наръчник: публичен ключ и рамка на атрибутите на сертификат; X.805 - Архитектура на сигурността за системите, предоставящи комуникации от край до край; X.1500 – Рамка обмен на информация, свързана с киберсигурността и др.

NIST - Националния институт за стандарти и технологии на САЩ (*National Institute of Standards and Technology*) разработва стандарти, ръководства за измерване и тестване и на програми за валидиране. Отделът на NIST за компютърна сигурност публикува стандарти и насоки за сигурно IT планиране, изпълнение, управление и експлоатация.

ETSI - Европейският институт за стандартизация на далекосъобщенията (*European Telecommunication Standardization Institute*) издава препоръки в областта на сигурността на мрежите и телекомуникациите. Института е световен лидер в създаването на криптографски алгоритми и протоколи за предотвратяване на измами и неоторизиран достъп до ИКТ и електронните мрежи, както и за защита на неприкосновеността на личния живот на клиентите.

Интернет общество играе водеща роля в решаване на въпроси, свързани с използването на Интернет. Тази организация има групи, които отговарят за стандартите за инфраструктурата на Интернет, както и за Internet Engineering Task Force (IETF) и Internet

Architecture Board (IAB). Интернет общество организира най-популярните стандарти в тази област – RFC (*Requests for Comments*), които включват стандартите на Интернет-протокол и Наръчника за сигурността на Уеб-сайтовете RFC-2196.

Форумът по сигурността на информацията е организация, в която участват водещи организации в областта на финансови услуги, производството, телекомуникациите, търговия с потребителски стоки, правителствени органи и др. Тя организира провеждане на научни изследвания в практиката, свързани с информационната сигурност и предлага консултации в стандарта на добри практики, както и консултации.

BSI - Германското федерално управление за сигурност в информационните технологии (*Bundesamt für Sicherheit in der Informationstechnik*) издава колекции от документи свързани със защитата. Базови каталози или ръководства за защита са особено полезни за откриване и премахване на слаби точки в защитата на IT среди.

Както вече бе отбелязано Международната организация по стандартизация е основната организация отговаряща за разработването на стандартите. Тя е подразделение на Организацията на обединените нации и консорциум от националните институти по стандартизация на 157 страни, координирани в Женева, Швейцария.

По-известни международни стандарти свързани със сигурността и приети от Международната организация по стандартизация са:

1) ISO/IEC 10181:2006 Информационни технологии - Отворена система за взаимно свързване - Рамки за сигурност за отворени системи: Рамка за контрол на достъпа.

Този стандарт определя обща рамка за осигуряване на контрол на достъпа. Целта на контрола е противодействие на заплахата от неразрешени операции, включващи компютърна или комуникационна система.

2) ISO 14000 – семейство стандарти, осигуряващи практически инструменти за фирми и организации, които искат да управляват своите екологични отговорности в различни аспекти на околната среда.

Стандарта ISO 14001:2015 и свързания с него ISO 14006:2011 се фокусира върху системите за управление на околната среда като средство за намаляване негативните въздействия от дейността на организациите. Другите стандарти в семейството акцентират върху специфични подходи, като например одити, комуникации, оценяване и управление на рисковете, анализ на жизнения цикъл, както и екологичните предизвикателства като изменението на климата.

3) Друг стандарт, отнасящ се към управлението на околната среда и базиран на ISO 14001, е EMAS (Схемата за управление по околната среда и одитиране). Стандартът е приложим за всички видове организации, като спомага за рационалното използване на ресурсите, минимизиране на замърсяването, участието на служителите и печелившия бизнес. EMAS цели да направи управлението по околна среда един непрекъснат процес, водещ до непрекъснато подобряване на резултатността спрямо околната среда.

4) ISO 15408:2009 Информационни технологии - Техники за сигурност - Критерии за оценка на IT сигурност. Стандарта е предназначен да служи като основа за оценка на сигурността на IT продуктите. Той регламентира създаването на зони на сигурност в информационната система. В ISO/IEC 15408-1 се установяват общите понятия и принципи за оценка на IT сигурността и се определя общия модел за оценка. Той дава насоки за специфициране на целите за сигурност (ST) и предоставя описание на организацията на компонентите в целия модел.

5) BS OHSAS 18001 [3] е стандарт, определящ изискванията за Система за управление на здравето и безопасността при работа. BS OHSAS 18001 е приложим към всяка организация, която желае да намали или отстрани напълно рисковете, свързани със

здравето и безопасността при работа за своя персонал и други външни заинтересовани страни.

6) ISO 27000:2017 Information technology – Security techniques – Information security management systems – Overview and vocabulary [7]. Това е семейството стандарти, подпомагащи организациите да поддържат информационните активи защитени. Използването на тези стандарти управляват сигурността на финансовата информация, интелектуална собственост, информация на работниците и служителите или информация, която е поверена на организациите от трети страни.

7) PCI DSS (Payment Card Industry Data Security Standard) е световен стандарт за сигурност на данните за търговци и процесори на платежни карти. Този стандарт е жизнено важен за прилагането на информационната сигурност и най-добрите практики в индустрията с кредитни карти.

8) Payment Application Data Security Standard (PA-DSS) [1] е стандарт на PCI организацията, поставящ изисквания и определящ процедури за оценка на сигурността към производителите на софтуерни приложения, които участват в разплащания с кредитни карти. PA DSS се използва от одобрените оценители на платежни приложения (Payment Application Qualified Security Assessors (PA-QSAs)), за да се потвърди, че съответният софтуер отговаря на изискванията на PCI DSS.

9) ISO 28000:2007 Международен стандарт за система за управление на сигурността на веригата на доставки. Стандарта предоставя рамка за организации или тези разчитащи на логистични фирми, да намалят до минимум риска от инциденти, свързани със сигурността и така да помогне за безпроблемни и навременни доставки. ISO 28000 е стандарт, основан на системите за управление на риска, който се основава на модела „планиране – изпълнение - проверка – действие“, подобен на стандартите ISO 9001, ISO 14001 и OHSAS 18001.

10) ISO/IEC 7498:2002 Информационна технология - Отворена система за взаимно свързване - Основен референтен модел: Наименуване и адресиране (OSI - Open System Interconnection). Този стандарт определя OSI модела, като описва архитектура за сигурна комуникация чрез услуги за сигурност (контрол на достъпа, проверка на автентичността, на интегритета на данните, на конфиденциалността на данните и недопускане на отхвърляне) и чрез механизми за сигурност (шифриране, електронни подписи, автентификация на обмен, контрол на маршрутизацията и нотаризация).

11) ISO 31000 [1] е международен стандарт, определящ изискванията към управление на риска. ISO 31000 замества AS/NZS 4360 стандарта за управление на риска, който е широко разпространен и изпробван в Австралия и Нова Зеландия. Стандартът е приложим за всякакъв тип организация – частна, публична, обществена организация, сдружение, група или лице. Рискове, засягащи организации, могат да имат последствия по отношение на икономическата ефективност, професионална репутация, околната среда, безопасността и социални резултати. В тази връзка ISO 31000:2009 [1] дава общия подход, принципите и указанията, които трябва да бъдат прилагани, за да бъде ефективно управлението на риска. Стандартът касае всякакъв тип риск, като препоръчва организациите да разработват, внедряват и непрекъснато да подобряват организационната рамка, за да се интегрира процеса на управление на риска в процеса на цялостното управление на организация, в нейната стратегия за управление чрез планиране, създаване на отчети, ценностите и организационната култура.

Редица други стандарти също се отнасят към управлението на риска. Това са:

- ISO Guide 73:2009 Възможност за управление на риска (*Risk Management Vocabulary Guidelines for Use in Standarts*), който допълва ISO 31000 като предоставя

единна терминология свързана с управлението на риска. В „анекс А“ на стандарта са описани термини и дефиниции за управлението на риска в сферата на сигурността;

- стандартът ISO 31010:2009 Risk Assessment Techniques, съдържащ насоки за подбор и прилагане на техники за оценка на риска;

- FERMA (*Federation of European Risk Management Associations*). Стандарт по управление на риска, разработен от експертни екипи от водещите организации по управление на риска във Великобритания – Институт по управление на риска (IRM), Асоциацията на застрахователните и риск мениджъри (AIRMIC) и Националния форум по управление на риска в обществения сектор (ALARM).

Следва да бъдат анализирани семейството стандарти ISO/IEC 270XX, регламентиращи информационната сигурност. Най-известният стандарт в семейството е ISO/IEC 27001. Той предоставя изисквания за система за управление на информационната сигурност (*Information Security Management System*, ISMS). Стандартът е приложим за търговски дружества, държавната администрация, неправителствени институции, които притежават и желаят да подобрят сигурността на важна за тях информация. Система за управление на сигурността на информацията е част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията [6].

Необходимо е да се отбележи, че групата включва и някои преди това разработени стандарти, като:

- ISO/IEC 27005 Управление на риска за информационната сигурност, преразглежда и отменя стандартите ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000 за Управление на сигурността на информационните и комуникационни технологии (*Management of Information and Communications Technology Security*);

- ISO/IEC 27033 Сигурност на мрежата (в 6 части) е замяна на стандарта за мрежова сигурност ISO/IEC 18028;

- ISO/IEC 27035 Управление на инциденти по сигурността на информацията, заменя стандарта за управление на инцидент ISO/IEC TR 18044.

Семейството стандарти ISO 270XX предоставя доказана рамка за управление на информационната сигурност, като използва интегриран набор от препоръчителни правила, процедури, документи и технологии под формата на ISMS. Основните концепции по внедряването и сертифицирането на ISMS се основава и подпомага от следните стандарти [5]:

- ISO/IEC 27000:2018 Информационни технологии - Техники за сигурност - Системи за управление на информационната сигурност – Общ преглед и речник;

- ISO/IEC 27001:2015 Информационни технологии - Техники за сигурност - Системи за управление на информационната сигурност – Изисквания;

- ISO/IEC 27002:2015 Информационни технологии - Техники за сигурност - Кодекс на практиките за контрол на информационната сигурност;

- ISO/IEC 27003:2017 Информационни технологии - Техники за сигурност - Ръководство за прилагане на системата за управление на информационната сигурност;

- ISO/IEC 27004:2016 Информационни технологии - Техники за сигурност - Управление на информационната сигурност - Мониторинг, измерване, анализ и оценка;

- ISO/IEC 27005:2018 Информационни технологии - Техники за сигурност - Управление на риска за информационната сигурност;

- ISO/IEC 27006:2015 Информационни технологии - Техники за сигурност - Изисквания към органите, предоставящи одит и сертифициране на системите за управление на информационната сигурност;

- ISO/IEC 27007:2017 Информационни технологии - Техники за сигурност - Насоки за одит на системите за управление на информационната сигурност;
- ISO/IEC TR 27008:2011 Информационни технологии - Техники за сигурност - Насоки за одиторите относно контрола на информационната сигурност;
- ISO/IEC 27009:2016 Информационни технологии - Техники за сигурност - Секторно специфично приложение на ISO/IEC 27001 – Изисквания;
- ISO/IEC 27010:2015 Информационни технологии - Техники за сигурност - управление на информационната сигурност за между секторни и вътрешно-организационни комуникации;
- ISO/IEC 27011: 2016 Информационни технологии - Техники за сигурност - Насоки за управление на информационната сигурност за телекомуникационни организации въз основа на ISO/IEC 27002;
- ISO/IEC 27013:2015 Информационни технологии - Техники за сигурност - Ръководство за интегрирано прилагане на ISO/IEC 27001 и ISO/IEC 20000-1;
- ISO/IEC 27014:2013 Информационни технологии - Техники за сигурност - Ръководство за информационна сигурност;
- ISO/IEC TR 27015:2012 Информационни технологии - Техники за сигурност - насоки за управление на сигурността на информацията за финансовите услуги;
- ISO/IEC TR 27016:2014 Информационни технологии - Методи за защита - Управление на информационната сигурност - Организация на икономиката;
- ISO/IEC 27017:2015 Информационни технологии - Техники за сигурност - Кодекс на практиките за контрол на информационната сигурност въз основа на ISO/IEC 27002 за облачните услуги;
- ISO/IEC 27018:2014 Информационни технологии - Техники за сигурност - Кодекс за защита на лична идентификация (PII) на обществени облаци, действащи като PII процесори;
- ISO/IEC 27023:2015 Информационни технологии - Техники за сигурност - Картографиране на ревизираните издания на ISO/IEC 27001 и ISO/IEC 27002;
- ISO/IEC 27031:2011 Информационни технологии - Техники за сигурност - Насоки за готовност на информационните и комуникационните технологии за непрекъснатост на бизнеса;
- ISO/IEC 27032:2012 Информационни технологии - Техники за сигурност - подобряване състоянието на кибер сигурността (сигурност на информацията, мрежова сигурност, интернет сигурност, защита на критичната информационна инфраструктура);
- ISO/IEC 27033:2013 Информационни технологии - Техники за сигурност - Мрежова сигурност (VPNs), части 6;
- ISO/IEC 27034:2015 Информационни технологии - Техники за сигурност - Сигурност на приложенията, части 5;
- ISO/IEC 27035:2016 Информационни технологии - Техники за сигурност - Управление на инцидентите на информационната сигурност, части 2;
- ISO/IEC 27036:2016 Информационни технологии - Техники за сигурност - Информационна сигурност за взаимоотношенията с доставчиците, части 4;
- ISO/IEC 27037:2012 Информационни технологии - Техники за сигурност - Насоки за идентифициране, събиране, придобиване и съхранение на цифрови доказателства;
- ISO/IEC 27038:2014 Информационни технологии - Техники за сигурност - Спецификация за цифрово редактиране;
- ISO / IEC 27039: 2015 Информационни технологии - Техники за сигурност - Избор, внедряване и експлоатация на системи за откриване на проникване (IPDS);

- ISO/IEC 27040:2015 Информационни технологии - техники за сигурност - сигурност при устройствата за съхранение на данни;
- ISO/IEC 27041:2015 Информационни технологии - Техники за сигурност - Ръководство за осигуряване на пригодност и адекватност на методите за разследване на инциденти;
- ISO/IEC 27042:2015 Информационни технологии - Техники за сигурност - Насоки за анализ и тълкуване на цифрови доказателства;
- ISO/IEC 27043:2015 Информационни технологии - Принципи и процеси за разследване на неоторизиран достъп, повреждане на данни, системни сривове или корпоративни нарушения на сигурността на информацията, както и всякакви други цифрови разследвания;
- ISO/IEC 27050:2016 Информационни технологии - Техники за сигурност - Електронно откриване, части 3;
- ISO 27799:2016 Здравна информатика - Управление на информационната сигурност в здравеопазването, използвайки ISO / IEC 27002.

Системата ISMS се основава на резултатите от оценката на риска. Организациите трябва да изготвят набор от мерки за контрол, за да бъдат сведени до минимум идентифицираните рискове и да не бъде компрометирана тяхната информационна сигурност.

Контролите препоръчани от ISO 27001, са не само технологични решения, но хора и организационни процеси. Съществуват 114 контрола, обхващащи управлението на информационната сигурност, включително области като физически контрол на достъпа, политики за защитна стена, програми за повишаване на информираността на персонала по сигурността, процедури за наблюдение на заплахи, процеси за управление на инциденти и криптиране.

3. Заключение

Сигурността на информацията е от особено важно значение за всяка една организация, от където произтича и необходимостта от определено ниво на защита. С развитието на технологиите през последните години е нужно основно обновяване на правилата и стандартите за сигурност в Европа. Тъй като последствията при пробив в базата данни често са сериозни и трайни, в интерес на всяка организация е да защити информацията на бизнеса и клиентите си по най-добрия начин.

Една от възможностите е внедряването на система за управление сигурността на информацията, съгласно изискванията на стандарт ISO 27001. Системата ISMS не само предоставя набор от подходящи технически контроли, политики и процедури, процеси за мониторинг и непрекъснато усъвършенстване, но също така популяризира културата и осведомеността свързана със сигурността на информацията.

Чрез стандарта ISO 27001 се очертава рамката за изграждане на система за защита на чувствителната бизнес информация. Целта е постигане на определено ниво на защита, като се осигури поверителност на съответната информация, цялостност на информацията и достъпност на оторизираните служители до същата. Спазването на стандарта ISO 27001 гарантира, че дадена организация е създала механизми за редовно идентифициране и управление на рисковете за сигурността на данните и е в състояние да се справи с постоянно развиващите се заплахи за сигурността на информацията.

ЛИТЕРАТУРА:

[1] Диманова, Д., Управление на риска. УИ Епископ Константин Преславски, Шумен (2016).

[2] ДИРЕКТИВА (ЕС) 2015/1535 на Европейския парламент и на съвета установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество, Брюксел (2015).

[3] http://www.consejo.bg.

[4] www.iso.org.

[5] https://www.itgovernance.eu/en-ie/iso-27001-ie.

[6] http://www.mscservices.eu/kop3.php.

[7] http://www.mscservices.eu/kop9.php.

[8] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 386-391.

[9] Boyanov, P., Analysis and assessment of several security vulnerability databases, Third international scientific conference science, Education, innovation, dedicated to the 145th anniversary of Bulgarian Academy Of Sciences and to the 35th anniversary of Georgi Ivanov's flight, Konstantin Preslavsky University Press, ISBN 978-954-577-969-5, vol. II, Shumen, Bulgaria, 21-23 May 2014, pp. 118-122.

[10] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

Име на автора: доц. д-р инж. Доника Величкова Диманова
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: d.dimanova@shu.bg
Име на съавтора: гл. ас. д-р Здравко Юриев Кузманов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: z.kuzmanov@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 139 - 145 Problems of Security Systems

RISK MANAGEMENT IN INFORMATION SECURITY

DONIKA V. DIMANOVA, ZDRAVKO YU. KUZMANOV

ABSTRACT: *Information security is one of the most pressing problems, which organizations in Europe today face. With the improvement of technology It needs major update rules and security and risk management standards. The best way to protect information is the application of good practices and procedures security organization.*

KEYWORDS: *Management and risk assessment, information security, ISO 270001.*

УПРАВЛЕНИЕ НА РИСКА В ИНФОРМАЦИОННАТА СИГУРНОСТ*

ДОНИКА В. ДИМАНОВА, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *Информационната сигурност е един от най-належащите проблеми, пред които са изправени организациите в Европа днес. С усъвършенстване на технологиите е нужно основно обновяване на правилата и стандартите за сигурност и управление на риска. Най-добрият начин за защита на информацията е прилагането на добри практики и процедури за сигурност в организация.*

1. Въведение

Информационната сигурност е дейност свързана със защита на информацията. Много организации съхраняват информация в своите бази данни, която е поверителна и от голямо значение за тях. Тази информация може да бъде от лични данни на служители и клиенти до банкова информация и чувствителни фирмени данни. Колкото по-значителни са данните, толкова по-голямо ще бъде въздействието от загубата им.

За да защитят информацията си все повече компании стават сертифицирани по ISO 27001, т. к. оценката и управлението на рисковете от информационна сигурност са в основата на този стандарт. Стандарта се приема като уверение, че организациите спазват най-добрите практики за информационна сигурност, предоставят независима и експертна проверка, ангажирани са да изпълняват задълженията си към клиентите и бизнес партньорите.

Пред системите за управление на информационната сигурност (ISMS) се поставят изисквания за контроли за сигурност на информацията на базата на редовни оценки на риска. Това дава гаранция че, заплахите пред които е изправена организацията са съобразени с рисковия апетит.

Извършването на оценка на риска за информационната сигурност е сложен процес, който изисква значително планиране и специализирани познания, за да бъдат покрити всички рискове, свързани с хора, процеси и технологии.

Във връзка с това целта на изложението е да бъде анализирана оценката на риска в информационната сигурност на база стандарта ISO 27001:2013, осигуряващ рамка за ефективно управление на риска.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

2. Оценка на риска за информационната сигурност съгласно ISO 27001

Стандарта е приложим към всички типове организации, които желаят да управляват сигурността на информацията. В стандарта се подчертава значението на систематичния подход за разработване и поддържане на процеса за управление на риска по отношение на информацията.

Оценката и управлението на рисковете от информационна сигурност са в основата на ISO 27001, където се посочва, че процесът на оценка на риска трябва да установи и поддържа определени критерии за риск за информационната сигурност.

Оценките на риска за информационната сигурност включват пет етапа: създаване на рамка за управление на риска, идентификация на риска, анализ и оценка на рисковете и избор на опции за въздействие (третиране) на риска.

Създаване на рамка за оценка на риска. Изпълнението на ISMS, започва с анализ на организацията - нейните бизнес, специфични нужди и законови, регулаторни и договорни задължения. Процесът на оценка на риска е разработен така, че да произтича от това разбиране и получената среда за сигурност да е подходяща за ситуацията на организацията.

Рамката за оценка на риска включва правила, регламентиращи [2]:

- Как ще бъдат идентифицирани рисковете;
- Целите и принципите за реализиране на информационната сигурност;
- Кои законови, стандартизационни, бизнес изисквания и договорни задължения за сигурност ще удовлетворява;
- Какъв стратегически контекст за управление на риска на организацията ще отговаря;
- По кои показатели и критерии ще се оценява риска;
- Дефиниране на подхода за оценка на риска (изчисляване на очакваното въздействие и вероятността от възникване на риска).

От това произтича необходимостта да се направи описание на обекта за защита, да се определят елементите на системата и дейностите, които се извършват в тях. Освен това трябва да бъдат дефинирани и активите на организацията, които са обект на защита.

Когато се говори за информационна сигурност, тя се свързва с определена съвкупност от уязвимости, заплахи и рискове. Когато възможната загуба е неприемливо голяма, е необходимо да се приемат икономически оправдани мерки за защита и периодична оценка на риска. От количествена гледна точка рискът се явява функция на вероятността за реализиране на определена заплаха, използваща дадена уязвимост на системата и определя големината на възможната загуба.

Управлението на риска включва [1,3,5]:

- Анализ и оценка размера на риска (измерване на риска);
- Третиране на риска чрез внедряване на ефективни и икономични механизми за намаляване на риска (минимизиране на риска);
- Определяне нивото на остатъчния риск и постигне на убеденост от организацията, че рисковете се намират в допустими граници и остават такива (остатъчен приемлив риск).

Управлението на риска включва основно два вида дейности, които се редуват циклично през целия жизнен цикъл на системата [1,5]:

- Оценка (измерване) на риска;
- Избор на ефективни защитни средства за неутрализиране на рисковете.

Избора на метод за оценката на риска трябва да бъде одобрен от висшето ръководство и да отговаря на следните въпроси: „Кои са основните критерии за сигурност?“, „Каква скала на риска ще бъде използвана?“, „Какъв е апетита към риска?“ и „Как ще бъде извършена оценката на риска – на база сценарий или активи?“

На този етап от изключителна важност е определянето критериите за нивата на „приемливия риск”.

Идентификация на рисковете. Идентифициране на рисковете, които могат да засегнат поверителността, целостта и достъпността на информация е най-трудоемката част от процеса на оценка на риска.

Идентифицирането на риска може да се раздели на три компонента, без които рисковете не могат да съществуват. Това са:

- Актив, който има стойност и изисква защита;
- Заплаха, за всеки от дефинираните активи, която може да го нарани;
- Уязвимост – слабост или място, което позволява заплахата да се достигне до актива [7], [8], [9], [10], [11].

Препоръчително е да се извършва оценка на риска на базата на активи. Активите могат да бъдат разделени на множество видове, за да се гарантира, че всички съответни активи са идентифицирани и техните собственици са определени.

Типовете активи, които трябва да бъдат разгледани, включват:

- Информация и данни (хартиени или цифрови записи);
- Хардуер и софтуер (IT активи и бизнес приложения);
- Физически местоположения и съхранение (сайтове и офиси);
- Системи и услуги (захранване, вода, газ, асансьори, телефония);
- Хора и организации (персонал, трети лица, доставчици и др.);
- Нематериални активи (марка, репутация, цена на акции и др.).

Процесът на идентифициране на активите гарантира, че всичко ценно в организацията е определено. При определянето на ценността на активите е необходимо данните да се класифицират в съответствие с последствията от нарушаване на конфиденциалността им.

Активите могат да имат множество заплахи, които от своя страна могат да достигнат до актива чрез множество уязвими места. Важно е да бъдат направени консултации с притежателите на активи, за да се гарантира, че идентифицираните рискове са уместни и адекватни, но не прекомерни по отношение на дейността на организацията.

В случаите, когато организациите не могат да установят собственици на активи, мениджърите стават притежатели на активите.

Анализ на рисковете. След като бъдат идентифицирани всички рискове, следващият етап е те да бъдат анализирани. За всяко събитие, което е идентифицирано като рисково, трябва да се определи вероятността от всяка заплаха и уязвимост, както и да им бъдат присвоени стойности (въз основа на рисковите критерии на конкретната организация) [7], [8], [9], [10]. Следователно чрез анализа се систематизират и класифицират идентифицираните рискове. Това дава възможност да се даде приоритет на определени рискове.

Рисковете са резултат от бизнес последиците и вероятността, или от въздействието и вероятността. Това е мястото, където повечето оценки на риска се различават в тяхната методология - от гледна точка на оценката на риска.

Има няколко подхода за измерване на риска. В зависимост от конкретната методология се различават количествени, качествени, едномерни, многомерни подходи и комбинации от тях. Изборът на подход е строго специфичен и се определя от вида на

изследването, наличието и вида на данните за изследвания обект [1]. Всяка организация сама определя нивата на въздействие и вероятност, които са от значение за бизнеса ѝ. В ISO 27001 и ISO 27005 не се посочва дали тези нива трябва да бъдат количествени или качествени, високи до ниски, от 1 до 5 или по друг начин.

Резултатът от този процес указва степента на риска, свързан с определени ценности. На база този резултат се избират средствата за защита и решения за минимизация на риска. Когато собствениците на рискове смятат, че са в състояние да приемат риск от определена скала, те трябва да са готови да приемат бизнес ситуация, при която загубата е с определени финансови измерения, а не по-малко въздействие. На практика съществува връзка между въздействието и заплахата и уязвимостта и вероятността, тъй като сходни заплахи оказват въздействие върху бизнеса и подобни уязвими места създават подобни вероятности. Като типове въздействия могат да се посочат човешки, финансови, правни, регулаторни, репутационни и оперативни.

Оценка рисковете. След като възможните рискове и рискови фактори бъдат идентифицирани и анализирани, е необходимо да се направи оценка на всеки един от тях. По своята същност този етап е най-сложен и продължителен, тъй като оценката не е еднократно действие, а се извършва периодично в хода на управлението. Чрез нея:

- Се подпомага решението за въздействие върху риска;
- Изготвят се варианти, описващи желаните възможности и рисковите събития, изискващи отговор;
- Определят се възможностите за пренебрегване или приемане на определени рискови събития, без това да надхвърля допустимото ниво за риск.

При оценката на риска се определя областта, в която попадат рисковете – област с висок приоритет, област с нисък приоритет и област за наблюдение. Така рисковете се подреждат по приоритет, като се определят тези от тях, които следва да бъдат управлявани.

Като приемливи се определят рисковете, които не изискват прилагане на мерки за редуциране на тяхното влияние. При тях продължава да се следи изменението им поне веднъж годишно (област на допустим риск) и се анализира вероятността и влиянието, което биха имали при промени във вътрешните и външните фактори.

Като отхвърлени рискове се определят тези, които са несъществени или несъществуващи.

Като значими рискове се определят тези, които трябва да са с висок приоритет (област на недопустим риск). Те задължително подлежат на управление. В някои случаи е възможно рискът да бъде много висок и да се наложи преоценка на дейността като цяло.

В практиката за сложни информационни системи, често се прилага комбиниран подход за оценка на риска, който се заключава в осигуряването на едно базово ниво на защита за определен кръг от елементи и преференциална защита за компоненти, изложени на по-голям риск, които са определящи за дейността на организацията [2].

След като се идентифицират и оценят възможности за въздействие върху риска, се прилагат подходящи механизми за контрол. Всичко описано до тук представлява план за въздействие върху риска, който представя управленските действия, ресурси, отговорности и приоритети за управлението на рисковете, свързани със сигурността на информацията.

Избор на възможности за управление на риска (въздействие на риска). След като всички рискове бъдат оценени и подредени по приоритет, следващият етап е да се вземе решение как да бъдат управлявани. Основната цел е минимизиране на риска до приемливи нива.

Мерките за въздействие на риска могат да бъдат насочени към намаляване на вероятността за проява на риска, намаляване честотата на въздействие, ограничаване размера на очакваните последици или трите фактора едновременно.

За всеки риск стандарта предлага използването на един от четирите основни метода за въздействие (третиране) [1,3]:

Приемане на риска – рискове, при които организацията е в състояние да понесе последиците от евентуално нежелано събитие (остатъчни и непроявени рискове). Не е необходимо да се предприемат специални действия за контролирането му. Това е възможно само ако оценката на остатъчния риск е в рамките на приемливо ниво или ако възможностите за предприемане на ефективни действия са ограничени.

- Намаляване на риска (ограничаване) – прилагат се механизми, чрез които да се намалят размера на щетите до определено приемливо ниво в рамките на общите изисквания към дейността. Въвеждат се контролни дейности свързани със сигурността, насочени към понижаване на вероятността от реализиране на риска и намаляване на последствията, ако рискът се материализира.

- Трансфер (прехвърляне) на риска – ако рискът е неприемливо висок, може да се търсят възможности за пренасянето му или споделянето му към външен субект, който разполага с по-големи възможности да го контролира. Това са застрахователи, клиенти, охранителни фирми. Докато избягването е свързано с усилия да не се случи нежеланото събитие, то прехвърлянето на риска е насочено към неутрализация на негативните последици при евентуално случване на събитието. Трансферирането може да се извърши и чрез хеджиране, застраховане и диверсификация.

- Избягване на риска – осъществява се чрез прекратяване на дейността, свързана с риска или чрез алтернативна дейност за постигане на целите. Прилагането му означава да се вземат решения, които ограничават вероятността и премахват източниците на риск, като не се предвиждат специални действия за неговото третиране.

Мерките за въздействие са специфични за всяко рисково събитие и могат да доведат до поява на вторични рискове, които следва също да се идентифицират и анализират. Поради това за разработването им е необходимо сътрудничеството на различни вътрешни и външни за организацията структури. Във връзка с това се разработва „План за въздействие на риска”. В този план следва да се подберат подходящите управленски действия, ресурси, отговорности и приоритети за управлението на рисковете на информационната сигурност.

Мониторинг на риска. Това е дейност за систематично и непрекъснато наблюдение и оценяване на прилаганите техники за въздействие на риска. Чрез мониторинга се осъществяват съответните коригиращи и превантивни действия спрямо управляваните рискове и самата система за управление на риска, което всъщност представлява контролът. Следва да бъдат преценени съществуващите контроли за сигурност, да бъдат отстранени евентуално пропуските според нуждите и да се приложат контролите последователно според критериите за приемане/въздействие на риска от организацията.

Приложение А към ISO 27001 определя 114 контрола за сигурност на добри практики, групирани в 14 области на информационната сигурност. При подбора на тези практики следва да се отчетат постановките на ISO 27002, които препоръчват приложимите механизми за контрол за намаляване на рисковете до приемливо ниво и гарантират нормалното функциониране на ISMS [6].

Основните обекти на системата могат да бъдат: информацията, служителите, материалните активи, клиентите и финансите на организацията. В техен интерес трябва да се разработи и прилага адекватна политика за сигурност, съответстваща на мисията на

организацията, класифициране на активите, подсистема за организационна сигурност, подсистема за управление непрекъснатостта на бизнеса, система за контрол на достъпа, подсистема за сигурност на комуникациите, подсистема за физическа сигурност, подсистема за сигурност на персонала, поддържане жизнения цикъл на системата [2].

Важен момент е да се изберат и внедрят цели по контрола и механизми за контрол, които да отговарят на изискванията на процесите оценка на риска и въздействие на риска. При избора трябва да се вземат в предвид критериите за приемане на риска, законови, нормативни и договорни задължения.

За контрол на риска се препоръчват следните процедури:

- Технически мерки (мониторинг, анализ на системните дневници и извършване на проверки);
- Анализ от страна на ръководството;
- Независими вътрешни одити.

Фазата на оптимизация на риска съдържа преоценка на риска и съответно:

- Преразглеждане на политиката;
- Ръководството по управление на риска;
- Коригиране и обновяване на механизмите за сигурност.

След като са определени контролите, е необходимо да се изготви декларация за приложимост (Statement of Applicability - SoA). Това е един от най-важните документи на ISO 27001. Тя трябва:

- Да определя избраните контроли, за да се минимизират идентифицираните рискове;
- Да дава обяснение защо са избрани тези контроли;
- Да посочва дали контролите са изпълнени или не;
- Да дава обяснение защо са били пропуснати всички контроли по ISO 27001.

Записите в декларация за приложимост SoA подпомагат с допълнителна информация за всеки контрол и връзка със съответната документация за изпълнението на същия. Докладът за оценка на риска може да бъде много дълъг, така че SoA е много полезен документ за ежедневна оперативна употреба. Той показва, че контролът е бил приложен и дава полезна връзка със съответните политики и процеси, които са били приложени като въздействия на всеки идентифициран риск.

Важен момент на всеки етап от управление на риска е прилагането на принципа на осведоменост, който предвижда информиране на всички участващи в процедурите по управление на сигурността, както и фиксиране на събитията от ISMS.

3. Заключение

Основните движещи сили за сигурността без съмнение са глобализацията, правителствените директиви, регулаторните изисквания, терористичните дейности и ескалирането на кибернетичните заплахи. Поради това управлението на риска трябва да бъде непрекъснат и постоянен процес, за да се гарантира висока ефективност.

Процесът на оценка на риска трябва да:

- Създава и поддържа определени критерии за риск за информационната сигурност;
- Гарантира, че повторните оценки на риска дават последователни, валидни и съпоставими резултати;
- Идентифицира рисковете, свързани със загубата на поверителност, целостта и наличността на информация в рамките на обхвата на системата за управление на информационната сигурност;
- Идентифицира собствениците на тези рискове;

- Анализира и оценява рисковете за сигурността на информацията съобразно определени критерии.

Процесът на управление на риска за сигурността (ISRM) преминава през оценка на заплахите за активите на конкретната организация, разпознаване на риска от тези заплахи, определяне на ефективни възможности за неговото предотвратяване и документиране от собствениците на риска, че същия е оптимизиран до приемливо ниво (остатъчен риск).

В някои рискови области не се изисква пълен и подробен анализ на риска, докато в други, където рисковете се проявяват като значителни, е необходима по-подробна оценка на риска. Ефективният процес на управление на риска за сигурността (ISRM) изисква непрекъснат мониторинг на активите, стойностите на активите, заплахите, уязвимостта, контрола и увеличените странични влияния, като нови законови регулации или по-голяма зависимост от конкретен актив. Чрез разработване на структуриран процес на ISRM, всяка организация може да гарантира, че управлението на риска е съобразено с нейната култура, бизнес цели и стратегии, в условията на променящите се пазарни и законови регулации.

ЛИТЕРАТУРА:

[1] Диманова, Д., Управление на риска. УИ Епископ Константин Преславски, Шумен (2016).

[2] Млеченков, М., Методика за разработване на система за информационна сигурност. Шумен (2010).

[3] ISO/IEC 27001:2015 (ISO27001) Information technology – Security techniques – Information security management systems – Requirements (2015).

[4] ISO/IEC 27005:2018 (ISO 27005) Information technology - Security techniques - Information security risk management (2018).

[5] http://www.tuj.asenevtsi.com/Sec2009/Sec30.htm, 23.09.2018, 11:16.

[6] https://www.itgovernance.eu/en-ie/iso-27001-ie.

[7] Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

[8] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 386-391.

[9] Досев, Н., Томов Г., Кибертероризъм и противодействие. Учебник за дистанционно обучение, Издателски комплекс на Национален военен университет "Васил Левски",ISBN 978-954-753-207-6, 2014 г.

[10] Желев, Ст. Информационно осигуряване на статистическия синтез на адаптивна система за контрол на комутационната апаратура. Научни трудове - Русенски университет „Ангел Кънчев“, ISSN 1311-3321 (print), 2003 г.

[11] Добрев, Д., Философия на западния модел за сигурност през 21. век. Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-619-201-076-8, 2016 г.

Име на автора: доц. д-р инж. Доника Величкова Диманова
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: d.dimanova@shu.bg
Име на съавтора: гл. ас. д-р Здравко Юриев Кузманов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: z.kuzmanov@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 146 - 156 Problems of Security Systems

CORRUPTION IN THE STATE ADMINISTRATION AND ECONOMIC CORRUPTION IN THE CONTEXT OF THE MEMBERSHIP OF BULGARIA IN THE EUROPEAN UNION

GALIN I. ISAEV

ABSTRACT: *Bulgaria is a country - member of the European Union, which by preference of the European committee has achieved unsatisfactory results in relation to the counteraction and the fight against corruption. In a result of this preference Bulgaria has been included in a specially created Mechanism for cooperation and verification regarding certain areas, within which the committee comes out with an annual report, reporting the condition of the country in the mentioned areas. The essential part of the problem with corruption in Bulgaria is the corruption in public administration and the associated with it - economic corruption. The Mechanism for cooperation and verification plays a significant disciplining role regarding the authorities in Bulgaria for taking actions targeted into the counteraction against corruption.*

KEYWORDS:. *Mechanism for cooperation and verification, corruption in public administration, economic corruption, counteraction against corruption.*

КОРУПЦИЯТА В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ИКОНОМИЧЕСКАТА КОРУПЦИЯ В КОНТЕКСТА НА ЧЛЕНСТВОТО НА БЪЛГАРИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ*

ГАЛИН И. ИСАЕВ

АБСТРАКТ: *България е държава член на Европейския съюз, която по преценка на Европейската комисия е постигнала незадоволителни резултати във връзка с противодействието и борбата с корупцията. В резултат на тази преценка България е включена в специално създаден Механизъм за сътрудничество и проверка (МСП) по отношение на определени области, в рамките на който Комисията излиза с ежегоден доклад, отчитащ състоянието на държавата в посочените области. Съществена част от проблема с корупцията в България са корупцията в държавната администрация и свързаната с нея икономическа корупция. Съществуващият МСП играе значителна дисциплинираща роля по отношение на властите в България за предприемане на действия, насочени към противодействие на корупцията.*

1. Въведение

Актуалността на изследвания проблем се обуславя от факта, че България, наред с Румъния, е държава член на Европейския съюз, която по преценка на Европейската комисия е постигнала незадоволителни резултати във връзка с функционирането на съдебната си система, както и противодействието и борбата с корупцията и организираната престъпност.

В резултат на тази преценка България е включена в специално създаден Механизъм за сътрудничество и проверка (МСП) по отношение на посочените области, в рамките на който механизъм Комисията излиза с ежегоден доклад, отчитащ постиженията на

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

държавата, както и респективно – неуспехите. За съжаление в изготвените до момента доклади, макар и с дипломатически тон, се констатира, че извършеното от парламента и администрацията е крайно недостатъчно. От общия тон се вижда, че Комисията констатира необходимостта от значително по-решителни усилия за минимизиране на негативните последствия от анализираните крайно отрицателни явления, касаещи цялостното функциониране на обществото.

България, като част от Европейския съюз е призвана да осигури върховенство на закона и правов ред, гарантиращи правилното разходване на европейски средства, стабилност на вътрешните и чужди инвестиции, просперитет на гражданите си и като цяло доближаване на икономическия стандарт на държавата до средния за съюза.

Проблемите, предмет на анализ в настоящия доклад, са недостатъчно разработени през последните години от началото на членството на България в Европейския съюз, които години от своя страна се характеризират със специфични проблеми, породени от това членство и специфични изисквания за принадлежност на България към общността. Факт е, че приемането на България и Румъния в ЕС беше съпроводено със сериозни компромиси от страна на последния именно в областите, предмет на настоящото изследване.

Целта на настоящия доклад е да обоснове тезата, че съществуващият МСП играе значителна дисциплинираща роля по отношение на властите в България за предприемане на действия, насочени към противодействие на корупцията в изследваните области.

2. Корупционни фактори, свързани с държавната администрация

Държавната администрация функционира, за да подпомага дейността на органите на изпълнителната власт (Министерски съвет, министерства и други ведомства, общини, кметства). Изпълнителната власт от своя страна е призвана да реализира изпълнението на законите директно и като автор на подзаконови нормативни актове в изпълнение на законите. Нормативната йерархия на подзаконовите нормативни актове се определя от вида обществени отношения, които се регулират с тях, както и от органа който ги издава, а това от своя страна също зависи от степента на важност и конкретизация на съответните регулируеми обществени отношения. Подробни правила в тази насока съдържа Законът за нормативните актове, обн. ДВ, бр. 27 от 1973 г., посл. изм. бр. 46 от 2007 г.[4].

Кънева и Йорданова[9] очертават широк кръг корупционни фактори, относими към работата на държавната администрация.

Администрацията, призвана да осигури технически прилагането на законите, осъществява на практика една вторична, подзаконова дейност, която от една страна е свързана твърде често с прилагане на несъвършено законодателство, а от друга – с ежедневен и пряк контакт с граждани и юридически лица, адресати на правните норми.

Лошият закон в съчетание с прекия контакт често провокират корупционно поведение от страна на заинтересованите. Невинаги функцията на отделните звена в администрацията и на съответните държавни служители е ясно дефинирана като често се наблюдава дублиране на функции. В много случаи процедурите по реализация на правата и задълженията на правните субекти са изключително и ненужно усложнени, а това от своя страна е предпоставка за корупционен натиск. Най-често механизмите за вътрешен контрол в съответните агенции и звена са анахронични и на практика неработещи.

Кръгът от информацията, с която администрацията разполага по отношение на заинтересуваните от съответните административни услуги граждани и юридически лица е широк и представлява самостоятелен провокиращ фактор за стремеж към извличане на материални и други облаги от страна на държавните служители. Също така

администрацията има санкционни функции, а често предвидените административни санкции са необосновано завишени и несъответстващи с вредоносната дейност на санкционирания субект.

Обстоятелството, че държавната администрация подпомага органите на изпълнителната власт при осъществяване на техните правомощия предопределя висока степен на зависимост на държавните служители от политическите промени. Честите „чистки“ в администрацията в резултат на конкретни политически промени, касаещи управлението на държавата, създават у служителите убеждение, че тяхното положение е несигурно, а това ги прави по-склонни да се възползват от своето служебно положение.

От друга страна цялостният статут на държавните служители не предоставя на последните възможности, които да са конкурентни на условията в частния сектор. Липсата на ясни критерии за кариерно израстване не поощрява служителите да се задържат задълго в държавната администрация.

В резултат на изложените фактори се наблюдават практики, при които срещу договорена облага се влияе върху вземане на определени нормативни решения в подзаконови нормативни актове, необосновано се намаляват, избягват, отлагат или отменят административни наказания, по целесъобразност се извършват действия или се издават актове в полза на гражданин или юридическо лице, които не му се следват по закон, ускоряват се срещу облага административни процедури, неправомерно се предоставя на заинтересован субект служебна информация, получава се не по установения за това ред назначение в администрацията или кариерно израстване. В общи линии тези случаи се определят като т. нар. „малка корупция“.

Вече четвърт век остава незадоволително решен въпросът за провеждане на административна реформа, която да доведе до минимизиране на рисковите фактори и изложените по-горе резултати от тяхното съществуване като въвеждането на т.нар. „електронно правителство“.

В Доклад на Европейската комисия за борба с корупцията до Съвета и Европейския парламент [1] се отбелязва, че широко разпространената корупция се счита за основен проблем и представлява сериозно предизвикателство за българските власти и тя несъмнено се отразява на желанието на предприятията да инвестират в България. Според Комисията би било полезно ползването на независим външен експертен опит в процеса на разработване на мерки за справяне с проблема. Като цяло резултатите от вече положените в тази насока усилия към този момент са отчетени като много ограничени. Общото впечатление е за слаба и некоординирана реакция на вече системен проблем във всички области на публичната администрация.

През последните години бяха извършени редица институционални промени, но има тенденция тези инициативи да се натъкват на проблеми или просто да не дават никакви видими резултати.

В областта на обществените поръчки сложната и непрекъснато променяща се законодателна уредба затрудни още повече изграждането на култура на обективност и стриктност. Чуват се гласове из стопанските среди, които започват да губят надежда, че е възможно да се противодейства на манипулациите на търговете и конкурсите.

Факт е, че усилията за борба с корупцията в държавната администрация са разпокъсани, като нито един антикорупционен орган не разполага с правомощията и с независимостта да предизвика промяна. Опитът показва, че от основно значение за доверието в антикорупционните действия е успешното преследване на корупцията по високите етажи на властта за да е видно, че за извършени нарушения се подвеждат под съдебна отговорност съответните лица. Липсата на доказан успех в преследването на

случаи на корупция на висококо властово ниво остава пречка за това българската обществеост да бъде убедена, че се полагат сериозни усилия за справяне с този проблем [9], [10], [11].

В икономически аспект държавните органи определят правната рамка, в която функционира икономиката на една държава. Правните норми в стопанската област се прилагат от държавната администрация. От друга страна държавните структури купуват и произвеждат различни стоки и услуги.

На следващо място държавните структури осъществяват т.нар. „трансферни плащания“, които не са свързани с плащането на стоки и услуги и като такива не се отчитат при измерването на брутния вътрешен продукт. Такива плащания са пенсиите, помощите за безработица, социалните помощи и др.[7].

Правителствата заплащат придобиваните от тях стоки и услуги. Като цяло с помощта на разходите, които правят и данъците, които събират, те играят водеща роля в разпределението и преразпределението на блага в икономиката. По един или друг начин правителството участва в избора на това какво да се произвежда (разходи за отбрана, образование, наука и култура), как да се произвежда (посредством регулативната политика и правната система) и за кого да се произвежда – чрез данъците и трансферните плащания то изземва доход от едни свои граждани и прехвърля доход върху други.

Освен това пряко въздействие, правителствата оказват и косвено влияние върху разпределението на ресурсите чрез данъците и субсидиите. В основата на регулативната функция на държавата стоят следните няколко фактора:

а. нормативните актове, върху които се базира регулативната намеса на държавата;

б. държавните органи, контролиращи спазването на тези закони;

в. контролиращите институции на държавните органи.

Регулативната функция на държавата обаче дава възможност за получаване на доходи и богатство от определени групи от обществото, които са свързани с администрирането на икономиката и обществения живот. Един от начините за ограничаване на влиянието на политиците и администрацията е въвеждането на прозрачни правила за функционирането на икономиката.

Тази регулативна функция на държавата създава естествена среда за корупционни практики. При общества със значителна степен на държавно вмешателство в икономиката, широки са и правомощията на администрацията за прилагане на правителствени разпоредби, а това от своя страна е фактор, който стимулира стопанските субекти в частния сектор да „разрешават“ своите проблеми чрез плащане на подкупи.

Търговските ограничения са основен източник на предпоставки и за корупционни практики в стопанската сфера. Протекционистичната политика на правителството по отношение на дейността на местните стопански субекти стимулира последните да генерират облаги, плащайки подкупи.

Съществен източник на корупция са и държавните субсидии. Контролът върху цените също е потенциален източник на облаги и следователно стимулира определен тип корупционно поведение. Ниските заплати на държавната администрация в съпоставка с тези в частния сектор са също потенциален корупционен фактор.

Мощен корупционен фактор, който заема специално място е наличието на държавни или частни монополни структури. Монополът в икономиката изкривява действието на пазарните сили и съсредоточава значителни ресурси в много малък кръг стопански субекти, което е доказано сериозна предпоставка за корупция. От една страна контролът на държавата върху определен ресурс стимулира администрацията сама да търси подкупи

от желаещите да получат достъп до този ресурс. От друга страна самите монополисти са стимулирани да предоставят подкупи, за да запазят възможно най-дълго съществуващото в тяхна полза статукво.

3. Икономическата корупция и нейната корелация с корупцията в държавната администрация

Корупцията в икономическата сфера е подчинена на класическия пазарен принцип на търсенето и предлагането. Колкото по-голям ресурс контролира държавната администрация под формата на средства и регулации, толкова по-голям е рискът от корупция в стопанския живот.

Държавата се намесва в икономиката чрез правилата за регулиране на бизнеса, които самата тя създава. За множество дейности правителствата въвеждат редица ограничения с цел охраняване на правата на гражданите – здраве, околна среда, сигурност и др. От друга страна всяко ограничение предпоставя предоставяне на властови ресурс на администрацията, което само по себе си е потенциален източник на корупция.

Наличието на сложна, скъпа и недобре структурирана система на разрешителните и лицензионни режими е корупционен фактор, който освен корупция влече със себе си и забавяне на икономическия растеж.

Едно сериозно и балансирано ограничаване на разрешителните и лицензионни режими в случаите, в които това е възможно, от една страна би облекчило дребния бизнес, който е най-потърпевш, от друга страна ще ограничи инструментите на администрацията да получава облаги, които не ѝ се следват. Дори и в случаите, при които липсата на разрешителен или лицензионен режим е обществено неоправдана, целесъобразно е инстанциите, от които той зависи да бъдат възможно най-малко и да работят по възможно най-опростената и прозрачна процедура.

При отчитане на гореизложеното се констатира, че в настоящия момент най-масовата предпоставка за корупция, отнасяща се както за дребния и среден бизнес, така и за най-големите инвестиционни проекти и концесии е институтът на обществените поръчки. Той е универсалният начин, по който държавни средства се насочват към частния сектор. Поради огромния размер на трансферираните средства чрез провеждане на обществени поръчки, последните се явяват вероятно най-значимия корупционен фактор в областта на икономиката.

Под формата на обществени поръчки годишно се преразпределят милиарди левове държавен ресурс, а през последното десетилетие – и огромни средства от бюджета на Европейския съюз от предприсъединителните и другите фондове на съюза. Въпреки положителните промени в правната уредба на обществените поръчки през последните години те продължават да бъдат основен обект на корупционен натиск.

Когато държавата или община се нуждаят от стока или услуга имат две алтернативи – да се направи или да се купи[8]. Градът например сам може да предложи стоката или услугата, както и да я достави от частния сектор.

Общинските паркинги могат да се стопанисват директно от общината или от търговско дружество с общинско участие, но могат да бъдат отдадени под наем в резултат на проведена обществена поръчка. Сметосъбирането и снегопочистването могат да се осъществяват като дейности от общината, но по-често се възлагат на външни фирми. В съдебен процес общината може да бъде представлявана от юрисконсулт, но може и от външен адвокат или адвокатско дружество.

Формите на корупция основно са свързани със случаите, при които се ангажират услугите на външни за общината или държавата субекти, като в основните случаи се касае за проведени обществени поръчки.

В огромния случай дейности от общодържавен или местен интерес се възлагат на външни компании след проведени обществени поръчки или различни форми на пряко договаряне. Договарянето при обществените поръчки често се отнася до големи парични средства и засяга обществено известни хора и компании в и извън властта или свързани по някакъв начин с лица, упражняващи власт на централно или местно ниво. Така този вид корупция може да е особено вредна за обществото, тъй като става дума за разходване на значителни по обем обществени средства.

Вредата възниква при порочно упражняване на властта, свързано с тайно договаряне на по-високи цени от приемливите, подкупи от участващите субекти, насочени към отговорните за поръчката фактори с цел уреждане на определена дейност.

Възлагането на обществена поръчка започва при установена нужда за извършване на определена работа или доставяне на услуга, които държавата или общината не са в състояние да осъществят със собствени ресурси извън финансовите такива. Самият процес преминава през няколко основни стъпки:

а. първа стъпка – обявяване на обществена поръчка или покана за пряко договаряне;

б. втора стъпка – подаване на предложения (оферти);

в. трета стъпка – оценяване на офертите, избиране на спечелил поръчката и сключване на договор с него;

г. четвърта стъпка – изпълнение на договора.

Всяка от изложените стъпки генерира корупционен потенциал.

На първия етап е възможно органът с компетенции за провеждане на обществени поръчки да бъде мотивиран неправомерно да открие процедура за обществена поръчка за доставка на стоки, предоставяне на услуги или извършване на определени дейности без да е налице нужда от тези дейности или в случаите, когато възложителят разполага с потенциал да ги извърши със свой ресурс.

Често срещани са случаите, когато между потенциалния възложител и потенциалния изпълнител се обменя предварителна информация или се споделя от страна на възложителя с определен потенциален кандидат вътрешна информация, която дава изначално нечестно предимство на този кандидат при подаване на офертата.

Най-често практикуваната корупционна схема е при определяне на критериите за участие да се заложат такива критерии, на които отговарят точно определени кандидати, въпреки, че тези критерии не са от определящо значение за провеждане на процедурата и участие в нея. Така се извършва предварително пресяване на кандидатите в полза на определен кандидат, извършил необходимото за „мотивиране“ на възложителя.

При втората стъпка е възможно група от кандидати тайно да се договорят или да манипулират офертата, за да се осигури спечелването на поръчката на един от тях.

Клитгард, Маклейн-Абароа и Парис[8] систематизират четири различни форми на тръжна манипулация:

а. Скрито наддаване – фирмите предоставят формални оферти, обикновено твърде високи, с цел да осигурят предварително избран член на картела да спечели договора. Отношенията помежду им са уредени предварително като най-често става дума за разпределение на изпълнението при различни обществени поръчки в съответния сектор.

б. Задържане на наддаването – фирмите се въздържат при наддаването или спират надпреварата, за да оставят свободна пътека за предварително избрания доставчик.

в. Ротация при наддаването – фирмите правят ротация на печелившите оферти помежду си и чрез странични плащания осигуряват всяка да спечели „достатъчен“ дял от бизнеса след време.

г. Разделяне на пазара – фирмите разделят пазара според региона, производството на уникален продукт или други параметри като се въздържат от участие (конкуренция) извън определените граници.

На третия етап на обществените поръчки според предложената схема – процесът на оценяване, най-често става дума за получаване на подкупи и комисионни или търговия с влияние. Може би точно на този етап корупцията се проявява в най-чист вид.

На четвъртия етап – изпълнение на договора, най-често става дума за измамно завишено отчитане на разходите, промяна на спецификациите или претенции въз основа на фалшиви режийни разходи. Често тези възможности са заложени още по време на стъпки едно и две. Например корумпиращите кандидати могат да занижат първоначално подадената оферта, за да спечелят поръчката, като е налице предварителна договорка с възложителя за бъдещо признаване на „непредвидени“ разходи.

Другата типична форма на корупция на този етап касае признаване от корумпирани инспектори, следящи за изпълнението на договора, на качество, което е по-ниско от обещаното. По този начин изпълнителят реализира неследващи му се икономии на средства.

Проблем, който малко или много засяга всяка икономика, но е силно изразен в България и е в пряка корелация с корупционни практики е наличието на сива икономика и контрабанда. Както отбелязва Илиев[7] „…сивата икономика като цяло лишава държавния бюджет от постъпления и създава сериозни препятствия пред утвърждаване на пазарна икономика.“

Сивата икономика и контрабандата от една страна и организираната престъпност от друга вървят ръка за ръка. Сивата икономика е реално социално-икономическо явление, както отбелязахме, съпътстващо стопанския живот на всяка една страна, като тя, разбира се на пръв поглед изпълнява и социална функция в едно бедно общество каквото е нашето. „Благодарение“ на нея определен контингент от населението, разполагащ със силно ограничени ресурси, в някои случаи на ръба на оцеляването, има достъп до евтини ресурси, включително и от първа необходимост. По тази причина управляващите често предпочитат да си затварят очите пред заобикалянето или директното нарушаване на закона от „играчите“ в сивия сектор като механизъм да се „тушира“ народното недоволство от ниските доходи.

От друга страна именно сивата икономика е един от основните фактори за ниския икономически растеж в страната, за хроничния недостиг на средства в публичния сектор, за изкривената представа за състоянието на икономиката и в крайна сметка се явява болестно състояние, при което се лекуват симптомите на заболяването, но не и неговите предпоставки [9], [10], [11].

Сивата икономика дефинитивно може да бъде разгледана като неофициална, нерегистрирана икономика, която включва доходи от иначе законна дейност, но укрити от официалните власти и съответно необложени с налози.

От важно значение е, че в тази сфера се включват и доходи от незаконна дейност (контрабанда, кражби и др. престъпни дейности). Най-общо става дума за доходи от дейности, които или са незаконни, или самите доходи не са публично достояние и съответно не се облагат с налози и за които не се плащат осигуровки. Във всички случаи това са дейности, които не се обхващат от официалната статистика.

Основна причина за съществуването на сивия сектор в икономиката са високите разходи, свързани с осъществяването на дейностите в рамките на закона. Икономисването на всеки един от тези разходи води след себе си навлизане в сивия сектор, а цената за това са корупционните практики.

Корупцията, свързана със сивия сектор на икономиката се открива в няколко направления:

а. корупционни практики, свързани с избягване на заплащането на данъчни или осигурителни задължения и неправомерно ползване на данъчен кредит по ДДС;

б. използване на силови структури за обезпечаване на функционирането на съответния бизнес в сферата на сивия сектор;

в. нерегламентирани плащания при сключване на договори, обезпечаващи функционирането на съответния бизнес.

Особено място по отношение на корупционната дейност заема сферата на контрабандата, която се характеризира с незаконното прехвърляне през държавната граница на стоки, валутни ценности и други предмети в нарушение на митническото законодателство с цел избягване на плащането на мита, данъци, акцизи или други налози на държавата. Пряката цел е обогатяване на осъществяващите тази дейност, а косвения резултат – ощетяването на фиска.

Можем най-общо да разграничим трансфера на стоки, търговията с които изначално е забранена и трансфера на стоки, търговията с които (внос или износ) поначало е разрешена, а единствената цел е избягването на налози.

4. Ролята на механизма за сътрудничество и проверка като дисциплиниращ фактор за противодействие на корупцията

Препоръките на ЕК в Доклада по МСП от 2015 г.[2] по отношение на борбата с корупцията се свеждат до следното: „Борбата с корупцията изисква продължителни и последователни усилия за превенция, но и за наказателното преследване на нарушенията и демонстриране на това, че извършването на престъпления води до санкции. В тази област България следва:

а. Да повери на една-единствена институция задачата да координира борбата с корупцията, да подпомага и координира усилията в различните сектори.

б. Да прегледа и актуализира националната стратегия за борба с корупцията след консултация с организациите на гражданското общество.

в. Да предприеме стъпки за намаляване на риска от корупция в процедурите за възлагане на обществени поръчки, като ги направи по-прости и по-прозрачни.

г. Да прегледа процедурите във връзка с конфликта на интереси, за да гарантира тяхната ефективност и безпристрастност, както и надеждността на механизма за налагане на санкции.“

В контекста на изложеното е редно да се отбележи, че МСП е инструмент на Европейската комисия за регистриране и подпомагане на напредъка на България и Румъния за постигане на специфични цели в областта на съдебната реформа, борбата с корупцията и организираната престъпност, установен непосредствено преди присъединяването на България към Европейския съюз като съпътстваща мярка към Акта на присъединяване, представляваща развитие и продължение на подхода, използван от ЕС по време на преговорите за присъединяване.

Целта е да се мотивират държавите кандидатки да извършат промени чрез поставяне на условия. Европейската комисия преди присъединяването на България констатира, че въпреки решението за присъединяване в страната остават неразрешени редица проблеми и

в този смисъл самото присъединяване е плод на известен компромис. В този смисъл целта на МСП е да се стимулира управляващата класа в България да извърши реформи, необходими и полезни за функционирането на българското общество. Тези констатации важат в най-пълна степен за предизвикателствата пред България, свързани с корупцията в държавната администрация и икономическата корупция.

Първите реални действия, съобразени с препоръките по МСП за противодействие на корупцията се предприеха, когато през 2015 г. Министерският съвет внесе в Народното събрание законопроект за Закон за предотвратяване на корупцията сред лицата, заемащи висши публични длъжности[6]. В мотивите към законопроекта е констатирано, че с Решение № 230 от 09.04.2015 г. Министерският съвет прие Национална стратегия за превенция и противодействие на корупцията в Република България 2015 – 2020 г. и, че водещ приоритет в стратегията е противодействието на корупцията по високите етажи на властта.

Внесеният законопроект беше в изпълнение на тези мерки, предвидени в Националната антикорупционна стратегия. Той даде законодателен израз на идеите, залегнали в стратегията и отговаря на необходимостта от създаване на по-ефективен механизъм за противодействие на корупцията по високите етажи на властта, намерила отражение и в препоръки, съдържащи се в докладите на Европейската комисия за напредъка на България по Механизма за сътрудничество и проверка.

Основната цел на проекта за закон според вносителите е да създаде работеща система за проверка на имуществените декларации и за установяване на конфликт на интереси чрез създаването на нов единен антикорупционен орган. Предложените решения се основават както на извършения анализ на действащата институционална рамка за противодействие на корупцията, така и на проучен чужд опит и препоръки на български и чуждестранни организации, работещи задълбочено по проблемите на борбата с корупцията.

Внесеният законопроект беше съществена стъпка в правилната посока. За съжаление в Народното събрание не беше формирано необходимото мнозинство за приемане на закона, което отново потвърди очевидният факт на липса на политическа воля за ефективна борба с корупцията, основно по отношение на висшия ешелон на властта.

След отхвърлянето в пленарна зала на 03.09.2015 г. на Законопроекта за Закон за предотвратяване на корупцията и за отнемане на незаконно придобито имущество и в съответствие с изискванията на Правилника за организацията и дейността на Народното събрание беше внесен нов законопроект, съдържащ промени в сравнение с отхвърления през септември вариант, свързани преди всичко с изразените в хода на дискусията в Народното събрание аргументи за неподкрепа на законопроекта.

Както е отбелязано в мотивите към този законопроект[6] важна промяна в сравнение с първоначалния вариант е обединяването на единния орган с Комисията за отнемане на незаконно придобито имущество. Целта според вносителите беше да се концентрират допълнително усилията за борба с корупцията като се свържат още по-пряко с производството за отнемане на незаконно придобито имущество.

На фона на скромните реални опити за налагане на правила, които да доведат поне до задоволителни резултати на антикорупционната политика Европейската комисия на 25.01.2017 г. излезе с поредния си доклад до Европейския парламент и Съвета за напредъка на България по механизма за сътрудничество и проверка[3].

В раздела за корупцията, разбирана като корупция по високите етажи на властта, но и като корупцията в по-общ план, по-специално на местно равнище и по границите, Комисията за пореден път констатира, че в засегнатата област продължава да съществува

очевиден дефицит на доверие, за който свидетелства българското обществено мнение, както и че досега в България броят на конкретните дела за корупция по високите етажи на властта, завършили с влезли в сила осъдителни присъди е много ограничен, а увеличаването на броя на тези присъди е най-ясното доказателство, че борбата срещу корупцията е реален приоритет. България продължава да е сред държавите членки на ЕС, с най-високи равнища на възприятие на корупцията и гражданите и представителите на бизнеса продължават да считат корупцията за значителен проблем.

В контекста на борба с корупцията и организираната престъпност към настоящия момент България, макар и мъчително и като резултат на сериозен политически дебат, изпълни част от отправените препоръки. На 19.01.2018 г. беше обнародван Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество[5].

3. Заключение

България беше приета за член на Европейския съюз с известни компромиси, касаещи функционирането на съдебната система, както и противодействието и борбата с корупцията и организираната престъпност, поради което беше включена в специално създаден Механизъм за сътрудничество и проверка (МСП) по отношение на посочените области. В рамките на този механизъм Комисията излиза с ежегоден доклад, отчитащ постиженията неуспехите на страната в тази насока. В досегашните си доклади Комисията констатира необходимостта от значително по-решителни усилия за минимизиране на негативните последствия явления.

Съществена част от отправените препоръки касаят корупцията в държавната администрация, в частност по високите етажи на властта, както и свързаната икономическа корупция.

България, макар и бавно и мъчително предприе мерки в насока отправените препоръки, които в крайна сметка към момента доведоха до приемането на Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество, чийто анализ е предмет на отделно изследване.

Изводът, който може да бъде направен е, че МСП играе съществена дисциплинираща роля по отношение на усилията на политиците, законодателя и администрацията, насочени към противодействие на корупцията.

ЛИТЕРАТУРА:

[1] Доклад на ЕС за борбата с корупцията. http:// ec. europa. eu/ dgs/ home- affairs/ e-library/ documents/ policies/ organized- crime- and- human- trafficking/ corruption/ docs/ acr_2014_bg.pdf. 10. 01. 2014.

[2] Доклад на Комисията до Европейския парламент и Съвета относно напредъка на България по механизма за сътрудничество и проверка. http// ec. europa. eu/ cvm/ docx/ com 2015 36 bg. pdf. 12. 12. 2015.

[3] Доклад на Европейския парламент и Съвета за напредъка на България по механизма за сътрудничество и проверка от 25. 01. 2017г. https://ec.europa.eu/info/sites/info/files/com- 2017- 43_bg.pdf.

[4] Закон за нормативните актове. http://www.lex.bg/laws/ldoc/2127837184. 21. 01. 2016.

[5] Закон за противодействие на корупцията и за отнемане на незаконно придобитото имущество. https://www.lex.bg/bg/laws/ldoc/2137180227.

[6] Законопроект за Закон за предотвратяване на корупцията сред лицата, заемащи висши публични длъжности. http://www.parliament.bg/bg/bills/ID/15451. 27. 01. 2016.

[7] Илиев, П. (2003) Държавно регулиране на икономиката и антикорупционни стратегии, Учебно помагало Антикорупция. София.

[8] Клитгард, Р., Маклейн- Абароа, Р., Линдзи Парис, Х. (2006). Корумпирани градове. Практически наръчник за оздравяване и превенция. София.

[9] Кънева Н., Йорданова М. (2003). Борбата с корупцията в държавната администрация, Учебно помагало Антикорупция. София.

[10] Марков, Ю., Христов, Х., „Проблемни области в превенцията и борбата с измамите по проекти, съфинансирани от ес и националния бюджет на Република България – манипулирани оферти в тръжни процедури", Научно-практическа конференция на тема „Право и сигурност", на Центърът по юридически науки на Бургаския свободен университет 29-30 септември 2017 г. Бургас.

[11] Кръстев, К. и Христов, Х., Еволюция в схващанията за сигурността. Научна конференция „Новата парадигма за сигурност в киберпространството", НВУ „В. Левски" , Факултет „Артилерия, ПВО и КИС", 5-6.06.2014 г.

Име на автора: д-р Галин Исаев Исаев
Месторабота: Катедра„Управление на системите за сигурност", Факултет по технически науки, Шуменски университет „Епископ Константин Преславски".
E-mail:

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 157 - 163 Problems of Security Systems

PLACE AND ROLE OF DIRECTORATE – GENERAL FOR SECURITY IN THE NATIONAL SECURITY

GEORGI HR. ZHEKOV

ABSTRACT: *In this article, it analyzes the professional framework of the basic activities of Directorate General Security and some concepts and national strategic documents in the field of National Security. The aim is to present evidence how Directorate – General for Security ensuring National Security.*

KEYWORDS: *National security, strategic documents, Directorate – General for Security, national interests, magistrate's security.*

МЯСТО И РОЛЯ НА ГЛАВНА ДИРЕКЦИЯ „ОХРАНА" В СИСТЕМАТА НА НАЦИОНАЛНАТА СИГУРНОСТ[1]

ГЕОРГИ ХР. ЖЕКОВ

АБСТРАКТ: *В обществения живот на Република България Главна дирекция „Охрана" има не леката задача да гарантира сигурността на представителите на съдебната власт, а целта на настоящия доклад е чрез анализ на дейността на дирекцията от една страна и анализ на основни понятия и някои доктринални документи свързани с националната сигурност, от друга, да се покаже приносът ѝ в Системата на националната сигурност.*

1. Въведение

Сигурността на всяка система, в това число и на системата за национална сигурност, е такова състояние, при което е гарантирано нейното нормално съществуване и са надеждно защитени жизненоважните ѝ интереси [4]. Ако възникне заплаха за тези интереси, системата може да започне да изпитва недостиг на сигурност и да премине в състояние на несигурност. За защита на жизненоважните интереси се жертват огромни ресурси, особено тогава, когато само по този начин системата може да гарантира своето съществуване и развитие.

Системата за национална сигурност обхваща всички онези елементи, които трябва да доведат до състояние, характеризиращо се като „националната сигурност". В България определение за национална сигурност е дадено в чл.2 от закона за управление и функциониране на системата за защита на националната сигурност[3]: "Национална сигурност е динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети". Именно постигането на това състояние е функция на системата на националната сигурност.

[1] Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

2. Изложение

Национална сигурност и система за национална сигурност

Основните компоненти на системата на национална сигурност са четири [1]. Това са: стратегическите документи, нормативната база, дейността на специализираните държавни структури и органи и техните способности и, на четвърто място, взаимодействието между обществото и специализираните структури и органи. Последното често е подценявано, но за функционирането на системата е необходимо обществото да е убедено, че тя работи за гарантиране на националната сигурност. Това е особено важно при съвременните рискове за сигурността, когато се разчита на информация и съдействие от гражданите. Без доверие това взаимодействие не може да се реализира.

Доктриналните основи на системата са този елемент, който трябва да дефинира сигурността като динамично понятие и да постави всички останали елементи във взаимодействие.

Като общи документи може да посочим приетата през 1998 г. Концепция за националната сигурност или Стратегията за национална сигурност от 2011 година, актуализирана с Решение на НС от 14.03.2018 г.,обн., ДВ, бр. 26 от 23.03.2018 г. В сферата на отбраната стратегически документи са Военната доктрина и Бялата книга за отбрана.

Нормативната база на системата на национална сигурност е изключително важен елемент, особено в демократичното общество. Към настоящия момент са приети всички основни документи, регламентиращи отношенията в сферата на националната сигурност(Закона за защита на класифицираната информация, Закона за Държавна агенция „Национална сигурност“ , Закон за управление и функциониране на системата за защита на националната сигурност, Закон за Държавна агенция „Разузнаване“, Закон за НСО, Закон за военното разузнаване).

Според стратегията за национална сигурност на Република България приета от Народното събрание през 2018г. *Жизненоважни интереси са* [6]:

гарантиране на правата, свободите, сигурността и благосъстоянието на гражданина, обществото и държавата;

- запазване на суверенитета, териториалната цялост на страната и единството на нацията;
- защита на конституционно установения ред и демократичните ценности;
- защита на населението и критичната инфраструктура при кризи, бедствия, аварии, катастрофи и други рискове и заплахи;
- съхраняване и развитие на националната идентичност, изграждаща се на основата на единно гражданство;
- гарантиране интегритета на българското гражданско общество;
- преодоляване на негативните демографски процеси, на значителните диспропорции в развитието на регионите и изграждане на социално-икономическа среда, осигуряваща условия за развитието на поколения български граждани, способни да гарантират на Република България достойно място в ЕС и в световните политически, икономически, финансови и социални процеси.

Други важни интереси са:

- благоприятната и предвидима среда за сигурност;
- ефективно функциониране на българските институции заедно с тези на ЕС и НАТО за постигане на колективната ни сигурност и подобряване на нейното състояние чрез развитие на оперативната съвместимост;

- поддържане на добросъседски отношения и осигуряване на регионална сигурност и стабилност;
- развитие на регионалното сътрудничество в зоната на Черноморския регион;
- гарантиране на енергийната сигурност чрез диверсификация на видовете енергия, източниците и трасетата на доставка на енергийни и други стратегически суровини;
- развитие на образованието, възпитанието, науката и научно-приложните дейности в духа на националните и общоевропейските ценности;
- гарантиране на икономическа, финансова и социална стабилност и икономически просперитет; превенция и противодействие на корупцията и организираната престъпност;
- ограничаване на посегателствата срещу личността и собствеността;
- запазване високо качество на околната среда и природните ресурси.

Защитата на тези интереси е регламентирана именно чрез системата за защита на националната сигурност, която включва различни органи, осъществяващи националната политика за сигурност [4]. Системата за защита на националната сигурност на Република България се състои от държавни органи и структури, които осъществяват дипломатическа, отбранителна, разузнавателна, контраразузнавателна, оперативно-издирвателна, правоохранителна и охранителна дейност и които са представени в Съвета по сигурността към Министерския съвет. Такива органи са Министерство на отбраната, Министерство на външните работи, Министерство на финансите, Министерството на вътрешните работи, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Служба „Военна информация“; Националната служба за охрана. Посочените органите и структури при защита на националната сигурност осъществяват:

- взаимодействие и координация при извършване на дейностите си и при изпълнение на конкретни задачи;
- сътрудничество с другите държавни органи и организации, с органите на местното самоуправление, с юридически лица и граждани;
- сътрудничество със сродни институции в други държави и международни организации.

Както става ясно от всичко казано до тук ГДО не е включена, нормативно, в системата за защита на националната сигурност.

От друга страна, тази година актуализираната с Решение на НС от 14.03.2018 г.,обн., ДВ, бр. 26 от 23.03.2018 г Стратегията за национална сигурност [6], ГДО е спомената в т.129 от Раздел Политика за правосъдие и вътрешен ред, а именно:

„129. Службите на Република България за сигурност и обществен ред, както и специализираните структури за охрана на съдебната власт и изпълнение на наказанията в състава на Министерството на правосъдието развиват взаимодействието помежду си и сътрудничеството с частните стопански субекти, гражданите и техните организации. В международен план те устойчиво развиват сътрудничество със структури на международни организации и на държави, с които са установени съюзнически или партньорски отношения.“

Основните дейности на ГДО

Създаването на Главна дирекция „Охрана” е резултат от изискванията поставени от Европейския съюз в глава „Правосъдие и вътрешен ред”, за усъвършенстване съдебната система, съобразно утвърдените демократични норми и ценности в държавите от съюза.

Дейността на ГД „Охрана” е неразривно свързана с осъществяване на част от приоритетите в политиката за сигурност на Република България [6], а именно:

- осигуряване пълно и надеждно функциониране на съдебната власт за успешна превенция и ограничаване на престъпността;
- повишаване индивидуалната сигурност на гражданите;
- запазване на позитивния международен имидж на Правителството на Република България пред партньорите от Европейския съюз, останалите международни партньори и организации като Европол, Интерпол и други чуждестранни структури;
- утвърждаване на Република България като надежден съюзник и партньор в сектора за сигурност в рамките на Европейския съюз и други държави извън него.

Нормативната основа на структурата, статута и правомощията на ГД „Охрана” и териториалните й звена се намират в Закона за съдебната власт /ЗСВ/ [2] и Правилника за устройството и дейността на Главна дирекция „Охрана” [7].

Съгласно Закона за съдебната власт/ [2], ГД „Охрана” е със статут на юридическо лице и е второстепенен разпоредител с бюджетни кредити към министъра на правосъдието, на която се възлагат следните функции:

1. организира и осъществява охраната на съдебните сгради;
2. осигурява реда в съдебните сгради и сигурността на органите на съдебната власт при осъществяване на техните правомощия;
3. организира и осъществява охраната на съдии, прокурори и следователи - при условия и по ред, определени с наредба на министъра на правосъдието, съгласувано с пленума на Висшия съдебен съвет;
4. оказва съдействие на органите на съдебната власт при призоваване на лица в случаите, когато се пречи за изпълняване на това задължение;
5. довежда принудително лица до орган на съдебната власт, когато това е постановено от орган на съдебната власт;
6. конвоира обвиняеми и подсъдими, за които се иска или е постановена мярка за неотклонение задържане под стража, или лица, изтърпяващи наказания в местата за лишаване от свобода, до органите на съдебната власт;
7. изпълнява разпореждания на прокурор за привеждане в изпълнение на влезли в сила присъди с наложено наказание лишаване от свобода, като при необходимост търси съдействие от органите на Министерството на вътрешните работи;
8. извършва проверки и контролира спазването на правилата и нормите за охраната и безопасността при проектиране, строителство и експлоатация на сгради на съдебната власт;
9. извършва съгласуване на проекти и дава становища за въвеждане в експлоатация на сгради на съдебната власт по отношение на охраната и безопасността;
10. изгражда и поддържа за нуждите на своята дейност информационни фондове, в които събира, обработва, съхранява и използва информация, придобита при или по повод изпълнение на функциите й;
11. получава от Министерството на вътрешните работи информация, свързана с изпълнението на функциите й.

*През януари 2003 г. се п*риема се Наредба № 1 за структурата, организацията и дейността на охраната на съдебната власт. През *март 2003 г.* се обнародва Постановление № 48 на Министерския съвет, ДВ, бр.21 от 07.03.2003 г. за създаване на Главна дирекция “Охрана” към министъра на правосъдието.

ГД„Охрана” започва да функционира през м. март 2003 г. с отпуснатите й 400 щатни бройки, които през годините плавно нарастват. Към момента щатната численост е 1338 бройки.

Структурата на Главна дирекция „Охрана” се организира в дирекции, отдели, сектори и териториални звена.

Основните дейности на ГДО са :

✓ Организиране и осъществяване охраната на магистрати.

В съответствие с чл. 391, ал. 3, т. 3 от ЗСВ, ГД „Охрана” организира и осъществява охраната на съдии, прокурори и следователи.

Дейността по охраната на магистрати е регламентира в Наредба № 1 от 21 април 2011 г. за условията и реда за организиране и осъществяване охраната на съдии, прокурори и следователи.

В българското общество имиджа на професиите „прокурор” и „съдия” е много висок [5] и в този смисъл гарантирането на тяхната сигурност в много голяма степен се асоциира с гарантиране на сигурността на отделния гражданин и на държавата.

✓ Охрана на сгради и обекти на съдебната власт.

Една от основните функции на дирекцията е да организира и осъществява охраната на сгради и обекти на съдебната власт, да осигурява реда в тях и да обезпечава сигурността на органите на съдебната власт при осъществяване на техните правомощия. Дейността по осигуряване на съдебните сгради се осъществява чрез физически и технически способи за охрана. Към настоящия момент общият брой на обектите поетите под охрана е 186.

✓ Призоваване, принудително довеждане и задържане на лица.

Основните задължения на служителите по това направление са заложени в чл. 391от Закона за съдебната власт, а организацията, изпълнението, контролът и отчетността са регламентирани в „Правила за призоваване, принудително довеждане и задържане на лица”, утвърдени от министъра на правосъдието.

✓ Конвойна дейност.

Функционалните задължения на служителите от ГД „Охрана”, осъществяващи конвойна дейност, са регламентирани в чл. 391, ал.3, т.6 и чл.393 ал.1 от ЗСВ.

Организацията, изпълнението, контролът и отчетността са разписани в утвърдени от министъра на правосъдието „Правила за условията и реда за осъществяване на конвойната дейност от служителите на ГД „Охрана”.

✓ Екстрадиции и трансфери.

ГД „Охрана” осъществява функционални задължения по организацията и изпълнението на европейска заповед за арест, екстрадиции и трансфери на лица, приети от чужди държави или предавани на чужди държави, на основание разпореждане от орган на съдебната власт, в изпълнение на Закона за екстрадицията и Европейската заповед за арест /ЗЕЕЗА/ и международни договори ратифицирани от Р България.

Главна дирекция „Охрана” в системата на националната сигурност

След направения анализ на основните дейности на ГДО могат ясно да се открият следните основни приноси, които пряко кореспондират със защитата на жизненоважни национални интереси:

1. Опазване сигурността и живота на застрашени магистрати и техните близки, във връзка с изпълнение на функционалните им задължения.

2. Въвеждане ред и сигурност в съдебните сгради при провеждане на съдебния процес и административното обслужване на гражданите, както и недопускане на терористични актове и нападения на територията им.

3. Бързо изолиране на лица с влезли в сила присъда и предаването им на затворническите власти в местата за лишаване от свобода, с цел прекъсване на тяхната престъпна дейност.

4. Бързо приключване на съдебните процеси, посредством призоваване и своевременно принудително довеждане на лица, участници в наказателно производство.

5. Превеждане на задържани лица от помещенията на затворите и следствените арести до органите на съдебната власт, при недопускане на нападения върху конвойните наряди за освобождаване на конвоирано лице, както и недопускане на бягства на задържани лица от конвойния наряд. Изпълнение на съдебни поръчки по международни договори по екстрадиция и трансфер на лица, укриващи се от наказателно преследване.

Дейността на Главна дирекция „Охрана“ към министъра на правосъдието е много специфична част от осигуряването на вътрешния ред в държавата, изключително важен за ефективния съдебен процес и не на последно място за имиджа на Република България като надежден съюзник и партньор в сектора за сигурност в рамките на Европейския съюз и други държави извън него.

Всичко казано до тук не само показва, че ГДО има своето място в системата за национална сигурност, но и играе съществена роля в нея.

3. Заключение

По принцип стратегическите документи са динамични по своя характер, каквато динамика е характерна както за развитието на България, така и на международната система. Ето защо, тези документи трябва да дават ясна насока на развитие, като отчитат постоянните промени. От тази гледна точка и вземайки предвид приносът на Главна дирекция „Охрана” към системата на националната сигурност естествено следва идеята за възможни бъдещи промени в Закона за управление и функциониране на системата за защита на националната сигурност, както и създаването на отделен закон, регламентиращ дейността на Главна дирекция „Охрана“.

ЛИТЕРАТУРА:

[1] Божилов, Й. Доктринални основи на ситемата за национална сигурност. http://www.sofiaforum.bg/front/rtf.php?cid=8

[2] Закон за съдебната власт, Държавен вестник, бр. 49 от 12.06.2018 г;

[3] Закон за управление и функциониране на системата за защита на националната сигурност, в сила от 01.11.2015г.;

[4] Казаков, К. Управление на системата за защита на националната сигурност, София (2016)

[5] Николова, К. Набиране и задържане на персонала в професионалната армия (резултати от емпирично изследване)В: Приложна психология и социална практика, Варна, ВСУ”Черноризец Храбър”(2009).

[6] Стратегия за национална сигурност на Република България, Държавен вестник, бр. 26 от 23.03.2018 г;

[7] Правилник за устройството и дейността на Главна дирекция „Охрана”. http://www.gdo.bg/.

[8] Кръстев, К. и Христов, Х., Еволюция в схващанията за сигурността. Научна конференция „Новата парадигма за сигурност в киберпространството”, НВУ „В. Левски“ , Факултет „Артилерия, ПВО и КИС”, 5-6.06.2014 г.

Име на автора: докторант Георги Хр. Жеков
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: g.jekov@gdo.bg

TENDENCES IN TRAINING POLICE OFFICERS ON SPECIAL POLICE TACTICS

IVELIN G. KATSEV, HRISTO A. DESEV

ABSTRACT: *In the exhibition was carried out a quantitative analysis of the system of training of specialists in administrative and information security and the results are compared with the requirements of the international standards and practices. Conclusions have been made regarding the change of the programs for the direction of business direction, increasing the laboratory sessions using simulation models and modern software and optimization of the training programs according to the requirements of the modern certification systems.*

KEYWORDS: *System of training, certification, simulation models.*

ПРОБЛЕМИ НА ОБУЧЕНИЕТО, ПОДГОТОВКАТА И СЕРТИФИЦИРАНЕТО НА СПЕЦИАЛИСТИ ПО ИНФОРМАЦИОННА СИГУРНОСТ

ИВЕЛИН Г. КАЦЕВ, ХРИСТО А. ДЕСЕВ

АБСТРАКТ: *В изложението е извършен количествен анализ на системата на подготовка на специалисти по административна и информационна сигурност и резултатите са съпоставени с изискванията на международните стандарти и практики. Формулирани са изводи свързани с промяна на програмите по направление за бизнес насоченост, увеличаване на лабораторните занятия с използване на симулационни модели и съвременно програмно осигуряване и оптимизиране на програмите за обучение в зависимост от изискванията на съвременните системи за сертификация.*

1. Въведение

Информационната безопасност е важен и актуален проблем на IT индустрията и по-голямата част от ръководствата на корпоративните компании съзнават важността на проблема. Той се фокусира не толкова върху наличието на технологии и продукти, а в изграждането на високо професионално ниво на съответни специалисти. Показател за качеството на специалистите се явява тяхната сертификация по информационна безопасност. Проблемно е до колко тя изразява реалната способност и качества на специалиста, но за сега не съществува по-добър механизъм за оценка. Широкия практически опит и съществуващите процедури за сертифициране (изисквания, изпити и допълнителни обучения) се приема за достатъчна гаранция за възможностите на притежателя на сертификата. Създаването на специалисти със специално образование е комбинация три елемента „знания“, „навици“, и „опит“. Последователността на такъв тип изграждане е фокусирано през призмата на изискванията на стандартите за политика по информационна безопасност и ценности на такава безопасност.

Значението на повишаването на квалификацията и сертификацията на специалисти по информационна сигурност се потвърждават и от сравняването на финансовите показатели. По данни от IDC около 40% от топменижърите причисляват информационната безопасност към главните приоритети на своите бюджети, а заплатите на IT специалистите са в първите редове на ведомостите за заплати. Статистиките

показват, че 80% от фирмите вложили средства за обучение на персонала и 70% от фирмите отделили средства за сертификация на специалисти по IT сигурност са увеличили ранга на сигурност и са снижили нивото на риск и заплаха на корпоративната защита на информацията. За изминалите години 2012-2017 средно с 10% се е увеличило количеството на IT специалистите, постъпващи на работа.

2. Изложение

Основните модели прилагани при сертификациите са два, потребителски и независим.

Потребителските сертификации възникват, като сегмент от маркетинговите програми и поддържат стабилно позиции на пазара. Производители на технологични защити като Cisco, ISS, Symantec поддържат собствени три степени на сертификация. По престиж лидират сертификациите на Cisco, те и останалите производители на софтуер предлагат сетифициране в рамките на собствените продукти предназначени за редовите администратори и инженери, а не на конкретни специалисти. Необходимо е да отбележим, че такъв модел на сертифициране не е достатъчен в съвременни условия.

Независимите сертификации показват, че IT специалистът е способен да организира оптимално комплексна информационна безопасност на организацията. Такова ниво изисква знания от технически и управленски аспект на защитата на информацията и знания в по-широк спектър от криптографията до елементите на физическата защита. В обзор на Comp TIA 68% от потребителите определят този тип сертификация на IT специалисти за основен, а останалите го приемат за следващо ниво и надграждане на потребителските модели.

Лидерство в IT сертификаците има Comp TIA Security (Computing Technology Industry Association) около 22 хил. специалисти за 115 страни по света. Това е начално ниво и изискванията не са високи – 2 годишен опит в областта на мрежовите технологии.

Сертификациите от средното ниво SANS GSEC (SANS — SysAdmin, Audit, Network, Security; GSEC — Global Security Essentials Certification) е програма насочена към начинаещи IT специалисти, които вече имат опит в работата на системи и продукти.

Високите рангове на сертификации, CISA (Certified Information Systems Auditor), SANS GIAC Specialist и CISSP (Certified Iinformation Systems Security Professional) са тясно свързани с техническите аспекти за информационна сигурност.

CISM (Certified Information Security Manager) изисква от специалиста знания, опит и способности ефективно да управлява защитата на информацията в организацията. Тя е мениджмънт сертификация за определена област фокусирана върху управлението на риска в информационните системи. Изпитът е от 200 въпроса за време от 4 часа и съдържа тематики от информационната безопасност, управление на риска, управление на защитата на информация, управление на програми за защитата на информация и управление на реагирането. Изискванията са 5 годишен опит от които 3 в системата за сигурност на информацията. Такава сертификация се потвърждава ежегодно при проведени не по-малко от 20 часа обучение.

CISSP сертифицира експерти от държавните структури, институти, големи корпорации банки и др. Сертификатът потвърждава висша квалификация на специалист по комплексна безопасност на информационни системи и е свидетелство за позиция от най-високо ниво CISO (Chief Information Security Officer). Изискванията са 4-5 годишен опит в системата за киберзащитата на позииция в определен аспект от информационната защита. Изпитът се провежда по методиката Common Body of Knowledge (CBK), в нея са

застъпени най-добрите принципи и практики на защитата и управление на достъпа и обхваща 10 области (домейна [4]

За да обобщим прегледа на сертификационните модели следва да отбележим обвързаността между съществуващите рангове и нива на придобиване на такива валидации и строгата система от изисквания, норми и правила за тяхното получаване и поддържане.

Проблемите с вързани с обучението, подготовката и сертифицирането на специалисти по информационна сигурност възникват в няколко направления.

Подготовката на специалисти от сферата на сигурността е сложен и продължителен процес. Завършващият випускник, който получава тази квалификация „специалист по защита на информацията“ трябва да бъде служител с богат набор от знания, устойчиви навици и определен опит в своята област.

Съвременната подготовка на такива кадри трябва да се съгласува с Национална квалификационна рамка на Република България, съществуващите стандарти в областта на информационната сигурност и съответните изисквания за баланса в часовото разпределение. В стандартите са посочени минимални изисквания, които дават основа при необходимост да се разширят с липсващите приложения.[3]

Сравняването на съществуващите стандарти в редица държави подсказва изисквания за средно количество на часовете по специалността посочено в таблица 1.

Таблица 1

№	Дисциплина	Среден брой часове за целия курс на обучение
1.	Сигурност на операционните системи	150
2.	Сигурност на мрежите	150
3.	База данни	150
4.	Основи на информационната сигурност	80
5.	Компютърна сигурност	200
6.	Организация на информационната сигурност	100
7.	Правни аспекти на информационната сигурност	100
8.	Криптография	150
9.	Средства и методи за защита на информацията	150
10.	Програмни и апаратни мерки за защита на информацията	200
11.	Сигурност на автоматизираните мрежи	100

Ако сравним тези стандарти със съществуващите учебни планове от специалностите „АИС“ (Административна и информационна сигурност) и „КСТ“ (Компютърни системи и технологии) ще открием следното количество часове поместени в таблица 2.

Таблица 2

№	Дисциплина	АИС	КСТ
1.	Сигурност на операционните системи	-	-
2.	Сигурност на мрежите	45	45
3.	База данни	60	60
4.	Основи на информационната сигурност	-	-
5.	Компютърна сигурност	-	-
6.	Организация на информационната сигурност	75	-
7.	Правни аспекти на информационната сигурност	45	-
8.	Криптография	60	45

9.	Средства и методи за защита на информацията	45	-
10.	Програмни и апаратни мерки за защита на информацията	60	60
11.	Сигурност на автоматизираните мрежи	-	-

Значително по малко са предвидените за изучаване дисциплини в специалността „ККТ“ (Комуникационна и компютърна техника) свързани с информационната сигурност.

Анализът на учебните планове показва, че учебната натовареност по дисциплини свързани с изучаване на информатика и информационна сигурност е средно 3,5 пъти по-малко, по стандарт 1530 часа, а по учебни планове съответно 385 и 210 часа. От учебните планове липсват дисциплини пряко свързани със сигурността „Автоматизираните мрежи“, „Сигурност на операционните системи“ и „Компютърна сигурност“.

В магистърските програми насочени директно към информационна сигурност част от тези несъответствия се коригират. Те имат обща продължителност за специалисти от два семестъра или около 600 часа, с което изоставането намалява до 30% от необходимото.

Достатъчно ли са часовете по тези дисциплини за да се формират експерти (специалисти) в сферата на информационната сигурност? Макар и не еднозначно отговорът е „**не**“. Количествения анализ показва дефицит от часове необходими за основни способности в областта на информационната безопасност, което в последствие задълбочава проблема с невъзможност за израстване и прилагане на някои от моделите за сертификация. Допълнително би трябвало да се изучават „Защита на населението“, „Методи за програмиране“, „Технически средства за защита“ и др.

Не са обхванати и редица информационни приложения свързани със сигурността, (ERP, CRM, SCM, Билинг и др.), Web сървиз, комуникации и системи за съхранение на данни (SAN, NAS, DAS) – технологии без които функционирането на съвременното производство е немислимо.

Друг проблем в изоставането се разкрива от косвени признаци свързани с давността на използваните и препоръчвани за нуждите на учебния процес пособия. Те са от 5-7 години и по стари с което условно съответстват на изискванията, но в тях не са отразени тенденциите в съвременната кибербезопасност, засегнатите теми са развити в теоретичен план и сравнително малко практически занятия.

Следващият проблем визира слабата възможност получените знания по работа с криптографските модели да се прилагат поради неяснотата в държавните стандарти за ведомствените системи или за търговските дружества. На практика всеки специалист прилага и използва закупената, сертифицирана криптографска система и дори когато открива нейните слабости не е оторизиран да я променя.

Обучението създава основа на знанията, разширява кръгозора на своите випускници, което се оказва излишно за неговата пряка дейност освен ако не работи във фирма за разработване на софтуер.

Организационен проблем са слабостите на обучението, които не създават умения за представяне пред ръководствата на фирмите и организациите необходимостта от инвестиции в безопасността и обвързване на политиките по информационната сигурност със общата стратегия за развитие на бизнеса. Презентации на ценностите на сигурността за фирмата, разясняването на способите за реагиране на инциденти, мобилността на безопасността, аутсорсинг на безопасността сигурност на системите за съхранение на данните са част от способностите, които трябва да създава системата на образованието.

Маркираните проблеми свързани със систематичната подготовка на специалисти в сферата на информационната сигурност, които да придобиват квалификация и

възможности за сертификация по международните стандарти следва да имат национално, концептуално решение.

В стратегията „Киберустойчива България 2020“ са формулирани важни изисквания към обучението и изграждането на специалисти по информационна сигурност. Те визират осъвременяване и модернизация на програмите в професионалното и университетско образование в две основни направления,като:

- създаване на специалисти за ИКТ, софтуерна и технологична индустрия, и в различните сфери на мрежова и информационна сигурност и киберустойчивост – покриване на изисквания за дизайн и разработване на киберсигурни и устойчиви информационни системи;
- дигитални лидери (е-лидери) и кадри за развиващата се дигитална икономика и интелигентна специализация на България, съобразно новите технологични тенденции и изискванията за киберустойчивост на дигитално зависимите бизнес модели, производства и услуги;

Засегнати са и идеи за ефективно използване на формите на продължаващо обучение, допълнителна квалификация и преквалификация на всички нива за допълване и актуализиране на компетентностите в сферата на киберсигурността и използване на ИКТ във връзка с бързото развитие на технологии и платформи и произтичащите нови отговорности и заплахи, функционална и тематична квалификация в съответствие с установените стандарти и сертификация. [1]

3. Заключение

Набелязани са мерки за повишаване на киберкултурата и отговорното използване на дигитален обмен на информация, предоставяне и използване на електронни услуги по цялата верига на доставки (малък, среден и голям бизнес, граждани) и ефективно използване на механизмите и платформите за споделяне на информация.

Стратегията демонстрира желанието на държавата ни да се адаптира към съвременните тенденции за информационна сигурност. Сърцевината на тази дейност е в образованието и подготовката на кадри, които да умеят да прилагат световните практики по информационна сигурност. Доктриналните виждания за повишаване нивото на подготовка трябва да се приведат в практическа програма ориентирана за решаването на следните задачи:

- създаване на екипи от млади преподаватели;
- създаване на лаборатории със съвременно оборудване и програмно осигуряване;
- привличане на водещи специалисти, сертифицирани и с богат опит за практическите занятия;
- обвързване на учебните планове с продължаващо обучение насочено към водещите системи за сертификация;
- коригиране на учебните планове с реална бизнес ориентация;

Представените проблеми и начините за тяхното овладяване представят отделни страни от подготовката на специалисти по информационна сигурност и тяхното решаване е предмет на дългосрочни изменения в изискванията, стандартите за обучение и програмите за подготовка.

ЛИТЕРАТУРА:

[1] Национална стратегия за киберсигурност „Киберустойчива България 2020“.

[2] International Strategy for Cyberspace USA 2013.

[3] European Internet Security Strategy, European Union, April 2013.

[4] Gordon A., Hernandez C., Official (ISC)² Guide to the CISSP CBK.

[5] Държавна комисия по сигурността на информацията, Рискове за интересите на Република България в областта на защитата на класифицираната информация.

Име на автора: докторант Ивелин Г. Кацев
Месторабота: НВУ „В. Левски“, Факултет „А, ПВО и КИС“ гр. Шумен
E-mail: katsev.i@abv.bg
Име на съавтора: доц. д-р Христо А. Десев
Месторабота: НВУ „В. Левски“, Факултет „А, ПВО и КИС“ гр. Шумен
E-mail: hristo.desev@gmail.com

DATA FUSION IN SECURITY

KONSTANTIN K. KAZAKOV

ABSTRACT: *The paper focuses on the data fusion in security. A process dealing with the association, correlation, and combination of data and information from single and multiple sources to achieve refined position and complete and timely assessments of situations and threats, and their significance. The process is characterized by continuous refinements of estimates, assessments and the evaluation for the need of additional sources, or modification of the process itself, to achieve improved results in security.*

KEYWORDS: *Data fusion, security, security services.*

СЛИВАНЕ НА ДАННИ В СИГУРНОСТТА*

КОНСТАНТИН К. КАЗАКОВ

АБСТРАКТ: *Докладът се фокусира върху сливането на данни в областта на сигурността. Процес, който се занимава с свързването, корелацията и съчетаването на данни и информация от един или няколко източника, за да се постигне рафинирана позиция, пълна и навременна оценка на ситуации, заплахи и тяхната значимост. Процесът се характеризира с непрекъснато усъвършенстване на оценката на ситуацията, и преценяване за нуждата от допълнителни източници или промяна на самия процес, за да се постигнат по-добри резултати в сигурността.*

1. Въведение

Сливането на данни е когнитивен процес, аналогичен на процесите в човешкия разум, където постъпващите сигнали във вид на образ, звук, миризма и допир се преработва в обща картина на околната среда.

Исторически погледнато сливане на данни винаги се е практикувало в зависимост от моментното състояние на технологиите. В последните години с интензивното развитие на технологиите рязко се увеличават параметрите на наблюдаваните обекти в сигурността. Поради тази причина автоматизирането на процеса на сливане на данни става от съществено значение за постигане високо ниво на сигурност.

Сливането на данни е съществен елемент от информационния процес и е интегрирана част от всяка система в сферата на сигурността, от обикновения сензор до комплексните информационни системи. На практика не съществува единен, универсален модел на сливане на данни, за това специалистите в сигурността трябва да се концентрират върху изграждане и развиване на способности за сливане на данни в информационните системи, с цел справяне с новите предизвикателства в съвременната среда за сигурност и създаване на условия за използване на възникващите възможности. Процесът на сливане на данни дава възможност за достъп до информационни потоци и бази данни, което увеличава възможностите на всички сензори и информационни ресурси. Стойността на ресурсите се увеличава за сметка на съвместното им ползване и комбинирането на техните качества.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Теорията на сливането на данни е обособена специализирана област на научното знание. Таксономията и категоризирането на отделните теоретични елементи се извършва от създадена през 1986г. в САЩ работна група по сливане на данни. Тя синтезира общ модел и терминологичен речник. Резултатът е функционално ориентиран модел за обработка на информация, структурни варианти на възможните архитектури за сливане на данни и концепциите за конкретни приложения. Моделът е известен, като „Модел на съвета на директорите на научноизследователски лаборатории“ (Joint Directors of Laboratories, JDL) и е приет, като стандарт в САЩ. Неговата мисия е да подпомага унификацията и стандартизацията на изследванията в тази област и да улеснява комуникациите на концептуално равнище. Структурата му включва сензорна, преносна, обработваща и визуализираща части. Обработката на информацията се реализира в три базови равнища, предшествани от предварителен етап, при който получените сигнали и данни се подреждат, синхронизират, мащабират и селектират по предварително зададени признаци.

За да има успешен процес на сливане на данни в сигурността се изискват следните експертни познания:

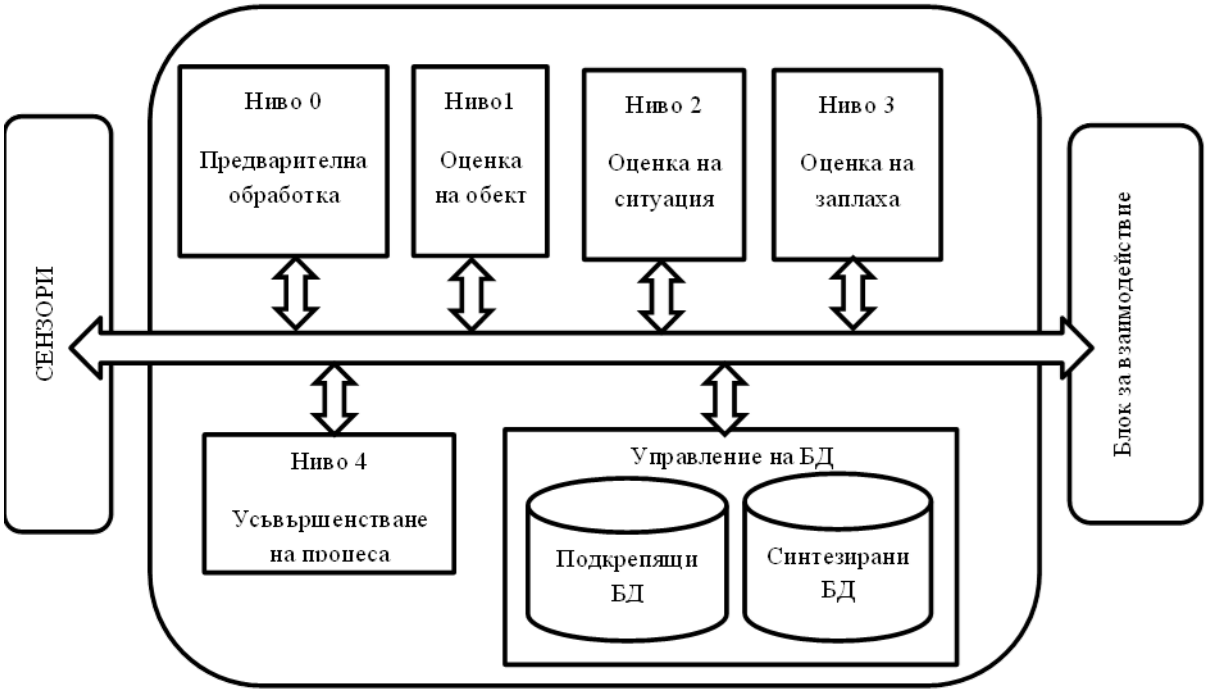
1. Познание и разбиране на физическото естество на сензорите в сигурността, както и процеса на събиране на данни в тези области;
2. Познаване и разбиране на цялостния процес на сливане на данни и подходите за развитие на този процес;
3. Познаване и разбиране на смисъла и целите на операциите в сигурността;
4. Познаване и разбиране на информационните нужди на потребителя на информация (този който взима управленски решения).

2. Изложение

Модел на сливане на данни (JDL)

Сливането на данни в сферата на сигурността е комплексен информационно-обработващ процес, чиято цел е да се оцени ситуацията и заплахите в средата за сигурност. В последните години са разработени множество методи и алгоритми за обработка на информация. В тези постижения сливането на данни се интерпретира, като целенасочен процес на извличане на необходимата информация от средата за сигурност, нейното транспортиране до центровете за обработка, синтезиране на обща картина на ситуациите и заплахите в представляващи интерес области на пространството и обратно доставяне на тази картина до всички нуждаещи се от нея потребители. Сливането на данни е процес на автоматизирана обработка на информация за нуждите на стратегическото ръководство и управление. Той осигурява качествено ново равнище на ефективност на извличане на знания, необходими за нуждите на планирането, организацията, координацията, ръководството и контролът на системата за защита на сигурността.

Както вече беше споменато най-популярният модел за синтез на данни до момента е известен, като „Модел на съвета на директорите на научноизследователски лаборатории“ (Joint Directors of Laboratories, JDL). (фиг. 1). Неговата мисия е да подпомага унификацията и стандартизацията на изследванията в тази област и да улеснява комуникациите на концептуално равнище.



Фиг. 1. Ревизиран модел JDL, от 1998г.

JDL моделът от 1998г. има следните четири функционални нива на сливане:

Ниво 1: Анализ на обект. Комбинира сензорни данни, за да се получи най-надеждната и точна оценка на позицията, скоростта и идентичността на обекта. Сензорната информация се превръща в измервания и се оценяват параметрите и състоянията на представляващите интерес обекти.

Ниво 2: Анализ на ситуация. Разработва описание на текущите взаимоотношения между обекти и събития в контекста на тяхната среда. Разкриват се взаимовръзките между отделните обекти и събития в общия контекст на динамичната обстановка. Разпределението на отделните обекти във времето и пространството се анализира с цел да се изяснят динамиката, тенденциите, намеренията и замисълът на техните действия, както и възможностите им. Допълнително ситуацията се корелира с получена странична информация, която доизяснява същността на цялостната картина. Този анализ се извършва с отчитане на особеностите на средата за сигурност.

Ниво 3: Анализ на заплахи. Проектира се настоящата ситуация в бъдещето, за да се направят изводи за заплахите, уязвимостта и възможностите за операции. Обработва се динамиката на регистрираната ситуация с цел да се оцени замисълът на конкурента (противника), неговата уязвимост и възможностите за противодействие. Оценяването на заплахите е процес при, който се използват знанията за възприетите доктрини, нивото на подготовка, политическата обстановка и текущата ситуационна информация. На това равнище се разкриват възможните замисли и стратегии, както и ефектът от липсата на достоверни данни относно обектите на интерес, тяхната тактика поведение и обкръжение.

Ниво 4: Усъвършенстване на процеса. Осъществява се мониторинг на общия процес на синтез на данни, за да се оцени и подобри ефективността на системата в реално време. Трите нива се обхващат от обслужващ процес, в който се реализират четири ключови функции:

- Контрол и диагностика на сливането на данни в реално време;

- Оценка на нуждите от подобряване на процеса;
- Генериране на общи заключения за работата на системата;
- Формулиране на специфичните изисквания към разположение на сензорите, с цел да се постигне максимален ефект.

Блокът за взаимодействие на човека с компютър (HCI) осигурява интерфейс, който позволява на човека да взаимодейства със системата за сливане. Блокът за управление на бази данни осигурява управление на данни за синтез (разузнавателна информация, данни от датчици, информация за околната среда, модели, оценки и т.н.).

Обработката на ниво 0 (асоцииране и оценка на субективните данни) има за цел да комбинира данни от различни нива, за да се получи първоначална информация за характеристиките на наблюдаваната цел. Предварителното обработване на източника включва обработка на отделни данни от сензорите за извличане на информация, подобряване на съотношението сигнал-шум и подготовка на данни като пространствено-времево подравняване за следваща обработка на сливане. В предварителната обработка се извършват следните процеси:

- Форматиране. Процес при който новите данни и информация се привеждат в съответствие с информационната система. Трябва да се гарантира правилното разчитане на данните и запазване на техния смисъл и входните им параметри, време, място и т.н.;
- Оценяване на информацията. Оценява се източникът на информация, съдържанието на самата информация и пътят по, който тя е получена (информационен канал). Източниците се оценяват по вид, надеждност, достъп до информация, чувствителност и др. Съдържанието на информацията се оценява по достоверност, релевантност, когнитивен клас и т.н. При оценка на информационния канал се отчита вероятността от загуба на информация, деформиране или промяна, получаване на фалшиво съобщение и др.;
- Систематизиране на информацията. Процес при, който новите данни и информация се подреждат в масивите, с цел оптимизиране на тяхното ползване;
- Класифициране на информацията. Процес на йерархично подреждане на информационните записи в зависимост от оценката им. В резултат на това подреждане те могат да се разпределят в три основни групи: червена зона – предназначена за унищожение и изследване на грешките; жълта зона – предназначена за проверка и допълнително изясняване (формулиране на вторични информационни цели); зелена зона – предназначена за използване и следващо обработване.

Обработката на ниво управление на бази данни (когнитивно повторение) има за цел да подобри взаимодействието между система за сливане и един или повече потребители / анализатори. Извършените функции включват помощни средства за визуализация, когнитивна помощ, отстраняване на пристрастия, сътрудничество, взимане на решения в екип и др.

Този набор от функции осигурява мениджмънта на сливането на данни, включително контрола върху тяхното съхранение, архивиране, компресиране и предпазване от несанкциониран достъп.

Краен продукт на сливането на данни е цялостното и обективно отражение на средата за сигурност, което способства за реална оценка на ситуациите и заплахите за сигурността.

Всички тези фактори осигуряват следните предимства за службите за сигурност пред носителите на заплаха за сигурността:

- Сензорите могат да работят синергично;
- Разполагането на повече сензори и тяхното правилно позициониране гарантират по-точна, навременна и достоверна информация за състоянието и движението на обектите в пространството и времето.

3. Заключение

В контекста на информационния домейн сливането на данни не е технология, а начин на мислене за света и за околната среда, който се фокусира върху съдържанието на данни и информация, които са от значение за човека, и решенията, които трябва да бъдат взети. Същността на командването и контрола (C2) е, че хората взимат своевременни решения в условията на несигурност и действат съобразно тези решения. В съвременната среда за сигурност нараства значимостта на технологиите, при проследяване на цели и процеси, които не са постижими само с една сензорна система. Повечето процеси на взимане на оперативни и стратегически решения на C2 изискват широк спектър от сензори и източници. Достигането на решение или изпълнение на целта е невъзможно без да се ползва организиран процес на сливане на данни в цикъла за обработка на информация.

ЛИТЕРАТУРА:

[1] Йовчев, Цв. Информационен мениджмънт. - Софтрейд, 2011;

[2] Семерджиев, Цв., Стратегически информационни системи, С., 2007;

[3] Das, S., High-Level Data Fusion, 2008;

[4] Liggins, M., Hall, D., Llinas, J. Handbook of multisensor data fusion: theory and practice, 2008;

[5] Maguire, E., Critical Intelligence Community Management Challenges, 2008;

[6] Mitchell, H., Data Fusion: Concepts and Ideas, 2012;

[7] http://www.nato.int/ 2017;

[8] https://fas.org/ 2017.

Име на автора: доц. д-р Константин Кирилов Казаков
Месторабота: УниБИТ, гр.София, България
E-mail: kkazak@mail.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 175 - 182 Problems of Security Systems

ROLE AND PLACE OF SPECIAL SERVICES IN NATIONAL CRITICAL INFRASTRUCTURE PROTECTION SYSTEM - REPUBLIC OF ROMANIA

KONSTANTIN I. STOYANOV

ABSTRACT: *A critical infrastructure is a complex system of socially significant elements, sub-sectors, sectors and their relationships, all of which are essential to ensuring national security, a thriving economy and the continued provision of basic societal needs. Critical infrastructure systems are constantly exposed to the negative effects of incidents and their failures can have significant impacts on society.*

KEYWORDS: *Defense, critical infrastructure, Romania.*

РОЛЯ И МЯСТО НА СПЕЦИАЛНИТЕ СЛУЖБИ В НАЦИОНАЛНАТА СИСТЕМА ЗА ЗАЩИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА – РЕПУБЛИКА РУМЪНИЯ*

КОНСТАНТИН И. СТОЯНОВ

АБСТРАКТ: *Критичната инфраструктура е сложна система от социално значими елементи, подсектори, сектори и техните взаимоотношения, всички от които са от съществено значение за гарантиране на националната сигурност и процъфтяващата икономика, както и за продължителното предоставяне на основни обществени потребности. Критичните инфраструктурни системи постоянно са изложени на негативните ефекти от инцидентите и тяхното увреждане може да има значително въздействие върху обществото.*

1. Въведение

Развитите общества изискват инфраструктури за нормалното си функциониране, както и за подобряване на общото благосъстояние и непрекъснатото развитие. Целта на критичните инфраструктури е ефективно и бързо да разпределят енергията, стоките и услугите на получателите (т.е. обществото) чрез своите сектори, елементи и връзки. Въпреки това, инфраструктурите по целия свят постоянно са застрашени от широк спектър от взаимодействащи антропогенни и естествени опасности. Активираната заплаха може да увреди даден компонент или функция на инфраструктурата. Разбира се, такова събитие не е много вероятно, но въздействието му може да бъде огромно. Нивото на неприемливо въздействие зависи от тежестта на пораженията, причината (т.е. характера на заплахата) и критичността на засегнатите елементи или сектори [5].

Сигурността и икономиката на Европейския съюз, както и благосъстоянието на неговите граждани, зависят от някои важни инфраструктури и от услугите, които те предоставят. Например телекомуникационните и енергийните мрежи, финансовите услуги и транспортните системи, здравеопазването, както и осигуряването на безопасна питейна вода и храни са от решаващо значение за ЕС и неговите държави-членки. Всяко унищожаване или прекъсване на инфраструктурата за предоставяне на услуги от ключово

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

значение, от една страна, и неадекватна реакция на събитие от такъв тип, от друга страна, биха могли да доведат до загубата на човешки животи, до загуба на имущество и до срив на обществеността доверие в ЕС. Сложната взаимозависимост означава, че дадено събитие може да окаже ефект на доминото върху други сектори и области, които на пръв поглед не са непосредствено и явно свързани. Този вид взаимна свързаност не е достатъчно изследван, като това може да доведе до недостатъчна защита и сигурност за гражданите на ЕС по отношение на критичната инфраструктура [1].

За ефикасното установяване на рисковете, заплахите и уязвимите места в съответните сектори се изисква комуникация както между собствениците/операторите на европейска критична инфраструктура[†] (ЕКИ) и държавите-членки, така и между държавите-членки и Европейската комисия. Всяка държава-членка следва да събира информация относно ЕКИ, които се намират на нейна територия. Комисията следва да получава от държавите- членки обща информация относно уязвимите места, заплахите и рисковете в секторите, в които са били установени ЕКИ, включително, когато е необходимо, информация за възможни подобрения в ЕКИ и междусекторни зависимости [2].

2. Роля и място на румънските специални служби в националната система за защитата на критичната инфраструктура

В Република Румъния, като страна-член на ЕС, дейностите по гарантиране сигурността на критичната инфраструктура се регламентират от Национална стратегия за защита на критичната инфраструктура на страната. Стратегията е разработена през 2006 год. в съответствие с разпоредбите на Стратегията за национална отбрана на Румъния, Бялата книга на националната сигурност и отбрана и институционалната концептуална делимитация в тази област – национално и международно ниво, като по този начин се установяват политиките и насоките за действие в тази област, необходими за разработването и завършването на националната регулаторна рамка.

Една от заложените цели на Стратегията е участието на всички национални органи с правомощия в тази област, както и на партньорите, при формулирането и прилагането на структурни и процедурни мерки - да се осигури координирано действие на национално равнище за идентифициране, обозначаване и защита на критичната инфраструктура. [4]

Съгласно Правителствена наредба № 98 от 3 ноември 2010 г. обществените органи, отговарящи за защитата на критичната инфраструктура[‡] в Румъния, са както следва:

- Министерство на вътрешните работи;
- Министерство на икономиката;
- Министерство на транспорта;
- Министерство на информационното общество;
- Министерство на националната отбрана;
- Министерство на околната среда и изменението на климата;
- Министерство на земеделието и селските райони;

[†] Европейска критична инфраструктура, е национална критична инфраструктура, чието разрушаване или унищожаване би имало значително въздействие поне върху две държави-членки на ЕС. Значимостта на въздействието се оценява в зависимост от междусекторните критерии. Това въздействие включва последващите ефекти, произтичащи от междусекторната зависимост от други видове инфраструктури.

[‡] Защита на критичните инфраструктури, представлява единна група процеси и дейности, организирани и проведени, за да се осигури правилната функция, непрекъснатост и целостта на НКИ / ЕКИ, за да се възпира, намали и неутрализира заплахата, или уязвимост чрез идентифициране, внедряване и поддържане на охранителни, организационни, технически, процедурни и други мерки, произтичащи от процесите на управление на риска.

- Министерство на националното образование;
- Министерство на здравеопазването;
- Министерство на регионалното развитие и благоустройството;
- Румънска служба за информация;
- Служба за външна информация;
- Специална телекомуникационна служба;
- Национален санитарен ветеринарен орган и орган по безопасност на храните;
- Румънската космическа агенция.

Отговорните публични органи изпълняват следните задачи:

а) установяване на секторните/междусекторни критерии и техните критични прагове[§];

б) предлагат определянето на национална критична инфраструктура[**] (НКИ) и ЕКИ в зависимост от съответните им области на отговорност;

в) координиране на процеса на идентифициране на конкретни НКИ/ЕКИ в съответната област на отговорност;

г) уведомяване на правителството за състоянието на прилагането на нормативните актове в съответната област;

д) проверява начина, по който собствениците/операторите/администраторите на НКИ/ЕКИ изпълняват задълженията, установени с Наредбата, и прилага, чрез упълномощени органи, санкции за неспазването им;

е) одобряване на специални оперативни процедури за сектори в областта на отговорност;

ж) да участва, по искане на МВР, чрез Център за координиране на защитата на критичната инфраструктура (*Centrul de Coordonare a Protectiei Infrastructurilor Critice – CCPIC*), при двустранни/многостранни разисквания за сключване на споразумения, необходими за създаване на Европейска гражданска инициатива;

з) установява/предоставя, по целесъобразност, мерки за подобряване на специфичната дейност на НКИ ЕКИ в областта на отговорност;

и) информиране на МВР на етапа на идентификация на НКИ/ЕКИ в областта на отговорност;

й) осигуряване на необходимите финансови ресурси за организиране и осъществяване на специфични дейности в областта на ЗКИ;

к) участва, по искане на Европейската комисия, в разработването на насоки за прилагане на секторни и междусекторни критерии и приближаване на критичните прагови стойности, използвани за идентифициране на ЕКИ [3].

Сложността и разнообразието на рискове и заплахи все повече взаимосвързани, и характеризирани с множество дефиниции, изисква интегративен подход, системни и всеобхватни цели за сигурност, с акцент върху защитата на тези жизненоважни компоненти за безопасност и сигурност, и доброто развитие на социално-икономическия живот.

[§] Критични нива (прагове) са гранични стойности, определени в зависимост от тежестта на въздействието, разрушаването или унищожаването на инфраструктура, която може да се идентифицира като критична инфраструктура

[**] Национална критична инфраструктура, наричана по-долу *NCI* , е елемент, система или един от нейните компоненти, разположени на националната територия, която е от съществено значение за поддържането на жизненоважни обществени функции, здраве, безопасност, сигурност, или социалното благополучие на хората и разрушаването или унищожаването на които биха имали значително въздействие на национално равнище в резултат на неизпълнението на тези функции.

Дейността за защита на критичната инфраструктура вече не съществува в национални граници и включва съвместни усилия за идентифициране и оценка на уязвимите места. Защитата на критичната инфраструктура, като определящ фактор за поддържане на стабилност и сигурност, изисква повишаване загрижеността на основните международни участници (държави и организации) за разработване и хармонизиране на стратегиите в тази област.

Те трябва да позволяват идентификация и ранно предупреждение за рискове и заплахи, като в същото време приемат и предприемат подходящи действия решения/подходи за превантивна намеса и противодействие.

Полето също е в сферата на компетентност специалните служби, които осъществяват дейности за целите на мониторинга, прогнозирането, предотвратяване и противодействие на заплахите срещу критична инфраструктура. Ефективната дейност на информационните служби зависи от способността на другите държавни институции да гарантират сигурността на нацията [7].

Румънска служба за информация (*Serviciul Roman de Informatii – SRI*) е тази която основно реализира приоритетите по защита на критичната инфраструктура в Република Румъния. Службата е създадена на 26.03.1990г. с Постановление №. 181 като държавна институция, специализирана в събирането на разузнавателни данни за националната сигурност. Тя функционира на основата на Закон № 14 за организацията и дейността на Румънската служба за информация, приет от Камарата на депутатите и Сената на обща сесия на *24 февруари 1992 г.* Дейността на службата се регламентира и със Закон № 51 от 1991 г. за националната сигурност, Закон № 415 за организацията и функционирането на CSAT и Закон № 182 от 2002 г. за защитата на класифицираната информация

От гледна точка на правомощията функциите на румънската разузнавателна служба при осигуряването на защита на националната критична инфраструктура, включва прилагане на следните мерки:

А. Информационни (разузнавателни) мерки

Те имат за цел да идентифицират заплахи от всякакъв тип за критичната инфраструктура, както и уязвимости, състояния на опасност и рискове, които оказват влияние върху тяхната сигурност, последвано от предаване на въпроси на юридически лица – бенефициенти на обекти от критичната инфраструктура.

SRI има за задача да информира постоянно и своевременно, чрез предоставяне на информационни материали, както и да координира на национално ниво с други държавни структури.

Информационната дейност относно критичната инфраструктура включва всички действия и операции, провеждани постоянно за планиране, търсене, получаване, проверка, аналитична обработка на данни и информация, имащи отношение към защитата на критичните инфраструктури и информиране на компетентните в тази област лица, отговорни за вземането на решения.

Информацията за защита на критичната инфраструктура е част от информацията за националната сигурност, дефинирана като продукт на разузнавателната дейност, включително нови познания за вече съществуващите ситуации / явления / факти / деяния, които представляват или могат да станат заплахи или източници на риск за националната сигурност.

Като такива сред специфичните дейности, извършвани от структурите на SRI, са:

- получаване на първични данни и информация за рисковите фактори, които влияят върху целостта и функционирането на критичната инфраструктура;

- разработване на оценка и цялостен анализ на състоянието на сигурността на критичната инфраструктура, което да даде възможност за идентификация и уведомяване на потенциалните заплахи;
- предоставяне на информация за потенциални рискови ситуации/заплахи за критична инфраструктура на институциите, отговорни за вземане на решения.

Предоставянето на класифицирана информация на бенефициентите се ръководи от принципа „необходимост да се знае“, така че лицата, отговорни за вземането на решения в различни области, получават информация в зависимост от компетенциите, които са им дадени от закона.

Б. Мерки за осигуряване на физическа защита на критични инфраструктури

Предотвратяване и борба с тероризма - една от най-големите заплахи за критичната инфраструктура – се извършва в съответствие с националното законодателство, международните конвенции, по които Румъния е страна и международни разпоредби.

Мерките са изведени от националния антитерористичен орган на SRI и технически координатор на Националната система за предотвратяване и борба с тероризма (*Sistemului Naţional de Prevenire şi Combatere a Terorismului – SNPCT*). Те се прилагат постепенно в зависимост от нивото на опасност, определено въз основа на специализирана информация за оценка на риска, а именно:

- даване на становище за антитерористична защита/интервенция в случай на осъществяване на заплаха от такова естество – задачи в компетенциите на специализираните членовете на SNPCT;
- борба с тероризма, в случай на терористична атака - в строга компетентност на SRI и с подкрепата на други членове на SNPCT;
- осигуряване на антитерористичен контрол и защита на тероризма в гражданските летища - в компетенциите на SRI.

В. Мерки, произтичащи от дейността на Националния център за кибер-разузнаване (CYBERINT)

Компютърните системи, които експлоатират най-критичните инфраструктури, са преобладаващата цел на кибератаките, които са все по-организирани и сложни. Атаките на компютърни системи, принадлежащи на държавни институции или частна собственост, стават все по-опасни и трудни за предотвратяване. Те могат да бъдат инициирани от организирани престъпни групи, насочени в повечето случаи към получаване на финансови ресурси, но също така и към враждебни държави, като оръжие за постигането на политически цели

Създаването през 2008 г. на Националния център CYBERINT е в резултат от процеса на трансформация и модернизация на SRI, който има за цел да обоснове институционална концепция и собствена архитектура на услугата, за да осигури адекватен отговор на такива заплахи (предотвратяване, защита, реагиране и управление на последствията в случай на кибератаки). CYBERINT включва:

- платформата за сътрудничество на институциите в рамките на системата за национална сигурност;
- интерфейс за сътрудничество с идентични структури на НАТО.

Г. Физически, правни и процедурни мерки за защита на класифицираната информация за критични инфраструктури

SRI като определен орган за сигурност, компетентен в областта на защита на класифицираната информация, извършва дейности, целящи да гарантират сигурността на класифицираната информация, управлявана от публични органи и институции или юридически или публичноправни субекти, попадащи под нейната юрисдикция, в съответствие с разпоредбите на Закон № 182/2002 г. за защита на класифицираната информация и последващите нормативни актове.

При упражняване на всички свои правомощия по тези регламенти, специализираната структура на SRI, осигурява:

- защитата на класифицираната информация на НАТО и ЕС, управлявана от SRI;
- Обща координация и контрол на мерките за защита на класифицираната информация в сферата на отговорност на SRI, за да се предотврати компрометирането на националната класифицирана информация, съответно такава на НАТО / ЕС;
- разработване на национални стандарти за защита на класифицираната информация;
- надзор на действията, предприети от държавни органи и институции, търговски дружества със 100% или частично държавно участие в капитала и други юридически лица, регулирани от публичното или частното право, за защита на държавната тайна;
- сътрудничество в областта на защитата на класифицираната информация с органи и структури на определени специализирани чуждестранни партньорски служби за сигурност;
- предоставяне на специализирана помощ в областта на защита на класифицирана информация и прилагане на закона чрез санкции, съгласно нормативната уредба [7].

Специална телекомуникационна служба (*Serviciul de Telecomunicatii Speciale - STS*) е създадена на базата на оперативно-техническото управление на Sekuritate „Тонола“. Извършва радиоелектронно наблюдение и осъществява държавните комуникации и свръзки, като осигурява тяхната защита чрез криптиране.

STS е публичен орган, отговарящ за управляваната критична инфраструктура, свързана със секторите на информационните и комуникационните технологии и националната сигурност съгласно действащото законодателство. Категорията критична инфраструктура, управлявана от STS, е:

- Инфраструктура на комуникациите и информационните технологии;
- Центрове за данни;
- Информационни системи и услуги;
- 112 услуга;
- Услуги, предоставяни в специални мрежи и сътрудничество.

STS организира и координира дейностите в областта на специалните телекомуникации за публичните власти в Румъния и други потребители, предвидени в закона. Съгласно разпоредбите на Закон №. 92/1996, STS има следните правомощия:

а) администрира, експлоатира и развива специални далекосъобщителни мрежи;

б) управлява радиочестотния спектър, предназначен за специални телекомуникации;

в) води документацията и мониторинга на територията на страната за целите на защитата на радиочестотния спектър и на органите, принадлежащи към националната отбранителна система;

г) извършва технически контрол на телекомуникационните мрежи от администрацията и осигурява поверителността на специалните телекомуникации;

д) организира и провежда обучение и мобилизация в съответствие със законовите разпоредби, военните заповеди, инструкции и наредби;

е) при обявяването извънредна ситуация, мобилизация или война определя като приоритет специалните връзки за Националния военен команден център и другите компоненти на националната отбранителна система на централно и териториално ниво;

ж) да си сътрудничат с Министерството на съобщенията и информационното общество и с институциите в областта на отбраната, националната сигурност и обществения ред въз основа на обща методология, за да се осигури съвместимостта на собствените им телекомуникационни системи с тези на националната отбранителна система, както и с обществеността телекомуникации;

з) осигурява националните мерки за безопасност в своята сфера на дейност съгласно действащото законодателство;

и) осигурява неприкосновеността на специалните телекомуникационни инсталации, оборудване и мрежи, съгласно законовите разпоредби [7].

Служба за външна информация (*Seviciul de Informaţii Externe – SIE*) е организирана като автономен административен орган с юридическа правосубектност, част от румънската система за национална сигурност.

С Декрет № 111 от *8 февруари 1990 г.* на Съвета на Фронта за национално спасение е образуван Център за външна информация, който прераства в SIE със Закон № 39 от 13 декември 1990 г. за създаване на Служба за външна информация. Нейната дейност се регламентира и със Закон № 51 от 1991 г. относно националната сигурност на Румъния, Закон № 415 от 2002 за организацията и функционирането на Висшия съвет за национална отбрана (*Consiliului Suprem de Apărare a Ţării – CSAT*) и Закон № 1 от 6 януари 1998 г. за организацията и функционирането на SIE.

Национална стратегия за защита на критичната инфраструктура на Румъния залага цели за постигане от всички структури отговарящи за защитата на критичната инфраструктура в страната:

- Извеждане на всички съществуващи или предвидими рискове, заедно с идентифицирането на елементите и критични процеси;
- премахване на дисфункциите, които могат да повлияят на стабилността и оптималното функциониране на критичната инфраструктура, като прилагат проактивни мерки в рамките на ефективна система за управление на риска;
- повишаване на нивото на експертиза и непрекъснато актуализиране анализа на риска, включително чрез сравнителни оценки със специфични ситуации на територията на други държави, с транспонирането превеждане на тези резултати в национални стандарти;
- спазването на правилата за поверителност и защита на данните, съгласно действащото национално законодателство, нерегламентиран достъп до които може да засегне защитата на системите за критична инфраструктура [4].

ЛИТЕРАТУРА:

[1] Директива 2008/114/ЕО - установяване и означаване на европейски критични инфраструктури и оценка на необходимостта от подобряване на тяхната защита. EUR-Lex - jl0013 - EN.

[2] Решение на Съвета относно Предупредителна информационна мрежа за критичната инфраструктура (CIWIN).

[3] Център за координиране на защитата на критичната инфраструктура (Centrul de Coordonare a Protectiei Infrastructurilor Critice). официална интернет-страница, Букрещ, Румъния (http://ccpic.mai.gov.ro).

[4] Национална стратегия за защита на критичната инфраструктура/NATIONAL STRATEGY on Critical Infrastructure Protection, STRATEGIA NAŢIONALĂ privind protecţia infrastructurilor critice. Обн. ДВ №555 от 4 август 2011.

[5] „International Journal of Critical Infrastructures”, vol. 14, (2016).

[6] Наредба №.98 от 3 ноември 2010 г. относно определянето, обозначаването и защитата на критичните инфраструктури.

[7] Centrul pentru Cultură de Securitate. Brosura Protectia Infrastructurilor Critice Букурещ, Румъния (http://www.sri.ro).

[8] Специална телекомуникационна служба (Serviciul de Telcomunicatii Speciale). официална интернет-страница, Букурещ, Румъния (http://www.stsnet.ro).

Име на автора: инж. докторант Константин Илиев Стоянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 183 - 187 Problems of Security Systems

THE AGGRESSION AS INTERNATIONAL CRIME

KREMENA B. RAYANOVA

ABSTRACT: *The question of crime aggression has always been important for international doctrine. The majority of scholars are unanimous about the fact that a major feature of contemporary international law is the responsibility for aggression. Aggression is the most serious international crime.*

KEYWORDS: *Crime aggression, Law, Responsibility.*

АГРЕСИЯТА КАТО МЕЖДУНАРОДНО ПРЕСТЪПЛЕНИЕ

КРЕМЕНА Б. РАЯНОВА

АБСТРАКТ: *Въпросът за престъплението агресия винаги е бил важен за международноправната доктрина. По-голямата част от учените са единодушни по отношение на това, че главна отличителна черта на съвременното международно право е отговорността за агресията. Агресията е най-сериозното международно престъпление.*

1. Въведение

Както е отбелязано от Ю А. Решев, терминът "международна престъпност", първоначално възниква, за да се характеризира агресивната война . Учените, справедливо отнасят нормите, които забраняват агресията към императивните норми на съвременното общо международно право, нарушаването на които е недопустимо [1], [2], [3], [4], [5].

Идеята за противоправността на агресивната война е присъща на международното право от самото му създаване. В трудовете на "бащите на международното право" от класическия период (F. de Vittoria, B. Ayala, G. Grotius) се казва, че справедлива и позволена може да бъде само война, започна в отговор на нарушени на права [1], [2], [3], [4], [5].

2. Изложение

Разработена е и друга концепция за войната, включително и агресивната, която признава допустимостта на всяка война по силата на това, че е борба между народите, следователно всички войни трябва да се считат за законни [1], [2], [3], [4], [5].

Забраната за "агресивната война" е изрично закрепена в Хагските конвенции от 1899 г. и 1907 г. относно мирното уреждане на международните спорове и Парижкия пакт за отказ от войната като инструмент на националната политика(Пакт Бриан-Келогг) от 1928. В Хагските конвенции от 1899 г. и 1907 г. е заявено, че договарящите се страни "ще търсят най-ефективните средства за осигуряване на траен мир за народите", както и желанието на държавите за мирно уреждане на международни спорове [1], [2], [3], [4], [5].

До края на Първата световна война, войната, независимо от целите й, се счита за неотменимо право на всяка държава (jus ad bellum), като проявление на суверенитета й в международните отношения. Това право е защитено от цялата система от принципи и норми националното право [1], [2], [3], [4], [5].

След края на Първата световна война са приети редица международноправни актове, с които се забранява агресивната война.

Хартата на Обществото на народите е първият акт, в който на междудържавното ниво се вменява задължението на държавите, да не се прибягва до война, като средство за разрешаване международни спорове (член 10). Чл. 11 от Хартата гласи, че "... всяка война или заплахата от война, независимо дали пряко засяга или не някоя от държавите-членки на Обществото на народите, засяга интересите на цялото ОН“ и то трябва да предприеме действия, способни да защитят всички народи [1], [2], [3], [4], [5]. Проблемът за агресивната война е обсъждан, както в Обществото на народите, така и много международни конференции [1], [2], [3], [4], [5].

За необходимостта от забрана на агресивната война се споменава и в проекта на Договора за взаимопомощ от 15 август 1923 г., в Женевския протокол за мирно разрешаване на спорове от 2 октомври 1924 г, но и двата акта, никога не получават задължителна сила [1], [2], [3], [4], [5].

На 24 септември 1927 г. Общото събранието на Обществото на народите приема специална декларация, с която обявява, че всяка агресивна война е и остава забранена и представлява международно престъпление. Практическото значение на тази декларация се намалява не само, защото тя не съдържа пряка забрана за агресия, но и допуска (чл. 12, 13 и 15) използването на войната за уреждане на международни спорове, при спазване на определени формални изисквания, т. е. по същество декларацията легализира войната. Агресията, от гледна точка на декларацията, е призната само под формата на нападение, извършено в нарушение на международноправните норми [1], [2], [3], [4], [5].

Първата реална стъпка към забраната на агресията е направена с Парижкия пакт от 27 август 1928 г., в който се осъжда използването на войната за уреждане на международно спорове, провъзгласява се отказа от войната в качеството й на инструмент на националната политика [1], [2], [3], [4], [5].

Трябва да се отбележи, че с този акт за първи път се установява задължението на държавите за отказ от употреба на сила. По този начин Парижкият пакт несъмнено отива по-далече от Хартата на Обществото на народите, въпреки, че съдържащите се в Пакта разпоредби не са подкрепени от ефективна система от санкции в случай на нарушение. Съществен недостатък на Пакта „Брианд-Келлог“ е съществуването на резерви, които дават възможност на държавите да се отклонят от задълженията си [1], [2], [3], [4], [5].

През февруари 1933 г. на конференция по разоръжаването в Женева, СССР представя проект на Декларация за определение на понятието „нападаща държава“. Проектът предвижда, че за нападаща страна в международен конфликт ще бъде призната държава, която първа извърши едно от следните действия - да обяви война на друга държава, чиито сили, дори без да обявят война, ще нахлуят в територията на другата държава; чиито въоръжени сили бомбардират територия или умишлено атакуват кораби и самолети на друга държави; установяват морска блокада по бреговете или пристанищата на друга държава [1], [2], [3], [4], [5].

Този проект за конвенция не е приет, въпреки че предложеното определение формира основата на Лондонската конвенция за агресията от 1933 г. и оказва влияние върху редица международни договори [1], [2], [3], [4], [5].

В международното право в следвоенния период продължава да се формира понятието „агресия“, като най-тежкото престъпление против мира, извършването на което вменява индивидуална отговорност по международното наказателно право [1], [2], [3], [4], [5].

След Втората Световна война в Проекта за Конвенцията за учредяване на Съд на ООН за военните престъпления, Комисията на ООН по военните престъпления предвижда, че този съд ще осъществява само преследване на лица, „действащи с разрешение или чрез разрешение, или чрез споразумение със заинтересованата държава или политическа организация във война, или военни действия срещу една от договарящите се държави“ [1], [2], [3], [4], [5].

С други думи, персоналът на съюзническите държави не би могъл да бъде преследван съдебно, колкото и жестоки да са били действията му. Съдиите от Нюрнбергския трибунал, които решават, че са извършени "престъпления против мира" или "военни престъпления", са ръководени главно от мирните договори по които Германия е страна [1], [2], [3], [4], [5].

Най-сериозно влияние върху развитието на концепцията за агресивната война, като международно престъпление оказва създаването и функционирането на Международния военен трибунал в Нюрнберг. В неговия Устав са формулирани норми за състава на най-сериозните международни престъпления - срещу мира и човечеството и военните престъпления. При този вид международни престъпления, като престъпно поведение са признати планирането, подготовката и воденето на агресивна война, а така също и „участието на държавите в общи действия или заговор насочени към осъществяването на някой от горепосочените действия“ . В този акт, за първи път е установен принципа за индивидуалната наказателна отговорност за извършването на всякакви действия на агресивна война [1], [2], [3], [4], [5].

При разработването на Устава на ООН, не е включена дефиницията за агресия, въпреки че са направени предложения от редица делегации на конференцията в Сан Франциско. Уставът на ООН задължава членовете на организацията да разрешават всички спорове само с мирни средства (чл. 2 (3), като не допускат изключения от този принцип и да се въздържат в своите международни отношения от заплаха или използване на сила срещу териториалната цялост или политическата независимост на която и да е държава или държави, по какъвто и да е начин несъвместими с целите на ООН [1], [2], [3], [4], [5].

Използването на сила от страна на държава се разрешава само в краен случаи - при упражняване на правото на индивидуална или колективна самоотбрана, при въоръжена атака срещу държава-членка на ООН и само докато Съветът за сигурност не предприеме необходимите мерки за поддържане на международния мир и сигурност (чл. 51) или при изпълнението с решение на Съвета за сигурност на принудителни мерки, насочени към предотвратяване и премахване на заплахите за мира и предотвратяване на актове на агресия(чл. 39, 41-43, 48) [1], [2], [3], [4], [5].

През 1974 г. Общото събрание на ООН приема Резолюция относно определението за агресия, в която се установява, че "агресивната война е престъпление срещу международния мир и всяка държава, нарушавайки този международноправен принцип, носи международна отговорност" (чл. 5, ал.2). Резолюцията подчертава, че агресията представлява използването на въоръжена сила от страна на държава срещу суверенитета, териториалната цялост или политическата независимост на друга държава [1], [2], [3], [4], [5].

Чл. 3 от този документ се отнася до следните актове на агресия - нахлуването или нападението на въоръжените сили на държавата на територията на друга държава; военна окупация, макар и временна, в резултат на въоръжено нахлуване; анексиране на територията на друга държава или част от нея; бомбардирането или използването на други оръжия срещу територията на друга държава; блокада на пристанищата или бреговете на една държава от въоръжените сили на друга държава и др. [1], [2], [3], [4], [5].

Списъкът на посочените актове на агресия не е изчерпателен. Съветът за сигурност може да реши, че и други актове представляват агресия в съответствие с разпоредбите на Устава [1], [2], [3], [4], [5].

Следва да се отбележи, че резолюцията не се отнася до индивидуалната наказателна отговорност за актове на агресия, поради което възниква въпросът дали определението за агресия, дадено в нея, се отнася до престъпни деяния, извършени от физически лица.

В края на XX век разбирането, че агресивната война е най-тежкото международно престъпление срещу мира, е твърдо вкоренено в международната правна доктрина и в актовете на международното право [1], [2], [3], [4], [5].

През 1998 г. е приет Римският статут на Международния наказателен съд (МНС), призован да администрира правосъдието по отношение на лица, извършили престъпления срещу човечеството, агресия, геноцид, военни престъпления [1], [2], [3], [4], [5].

Изглежда, че повече от петдесет години доктрината за международното наказателно право е установила недвусмислено разбиране за агресията или за агресивната война. Това обаче не е съвсем така - по-нататъшното развитие на международното наказателно право отново доведе до проблема за разбирането на самото определение за агресия, характеристиките на това престъпление и субектите на наказателна отговорност за неговото извършване [1], [2], [3], [4], [5].

От всички престъпления, свързани с компетентността на Международния наказателен съд (чл. 5 от Римския статут), престъплението агресията е изключително за много моменти. В него (Статута) няма определение, няма фиксиран списък от актове, които са прояви на агресия, няма списък с конститутивните елементи на състава. Римският статут установява, че окончателният текст, който определя признаците на престъплението агресия трябва да бъде в съответствие с разпоредби на Устава на ООН. Неразрешеният въпрос за наказателно преследване за извършване на актове на агресия е един от основните недостатъци на Римския статут [1], [2], [3], [4], [5].

Освен това следва да се отбележи, че във връзка с престъплението агресия се обръща специално внимание на член 16 от Статута на Международния наказателен съд, съгласно който Съветът за сигурност на ООН има право да отлага разследването или наказателното преследване в продължение на една година, с възможност за удължаване на този период всяка година, чрез приемане на резолюция по глава VII от Устава на ООН. По този начин е избегната възможността да се блокира работата на Съда. Такова разглеждане може да продължи безкрайно и да не бъде придружено от приемането на каквото и да е решение. Съгласно Статута, трябва да се вземе специално решение, което прави процедурата за забавяне много по-сложна, отколкото просто да се обмисли ситуацията или дори да се определи като заплаха за света. Освен това, Статутът се занимава конкретно с отлагането на разследването или наказателното преследване, което означава, че в крайна сметка, то ще се осъществи [1], [2], [3], [4], [5].

Въпреки тези прогресивни разпоредби на Статута, за отношенията между МНС и Съвета за сигурност на ООН, проблемът за наказателното преследване за извършване на агресия остава неразрешен, което правилно може да се счита за един от основните неуспехи на конференцията по приемането на статута. Престъплението агресия е включено в юрисдикцията на МНС в съответствие с ал. 1 на чл. 5 на Статута [1], [2], [3], [4], [5].

3. Заключение

Позовавайки се на Статута на Международния наказателен съд, можем да отбележим, че в съответствие с неговите норми, агресията е престъпление по отношение

на което договорно е определено неприлагането на давностни срокове (чл. 29 ал. 2) . До сега, този въпрос се регулира от Конвенцията за неприлагане на давност по отношение на военните престъпления и престъпленията против човечеството от 26 ноември 1968 г [1], [2], [3], [4], [5].

Международната правна доктрина позволява да заключим, че акт на агресия може да се разглежда като престъпление, извършено от индивидуално определени лица и като престъпление, извършено от държави и/или от юридическо лице. Тази ситуация все още повдига неразрешения въпрос кой трябва да бъде отговорен за извършването на агресия и как [1], [2], [3], [4], [5].

ЛИТЕРАТУРА:

[1] Решетов Ю.А. Борьба с международными преступлениями против мира и безопасности / Ю.А. Решетов. – М., 1980.

[2] Устав на Международния военен трибунал

[3] Устав на ООН

[4] Определение агрессии от 14 декабря 1974 г. // Резолюции, принятые Генеральной Ассамблеей на 29-й сессии 17 сентября – 18 декабря 1974 г. Т. 1. – Нью-Йорк, 1975.

[5] Статут на Международния наказателен съд.

Име на автора: доц. д-р Кремена Божидарова Раянова
Месторабота: Юридически факултет на Русенски университет „Ангел Кънчев“
E-mail: krayanova@uni-ruse.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 188 - 195 Problems of Security Systems

GOVERNANCE, COMMAND AND MANAGEMENT OF THE ARMED FORCES IN PARTICIPING IN COUNTER-TERRORISM IN OPERATIONS IN THE COUNTRY

LYUBOMIR K. DUCHEV

ABSTRACT: *Optimization of the organization and the system for governance, command and management of the Armed Forces of the Republic of Bulgaria when participating in counter-terrorism operations in the country, based on the existing legal framework.*

KEYWORDS: *Governance, command, management, Armed Forces, Counter Terrorism.*

РЪКОВОДСТВО, КОМАНДВАНЕ И УПРАВЛЕНИЕ НА ВЪОРЪЖЕНИТЕ СИЛИ ПРИ УЧАСТИЕ В ОПЕРАЦИИ ЗА ПРОТИВОДЕЙСТВИЕ НА ТЕРОРИЗМА В СТРАНАТА*

ЛЮБОМИР К. ДУЧЕВ

АБСТРАКТ: *По своята същност тероризмът е акт на насилие, който създава страх и несигурност в обществото и дестабилизира институциите, с оглед постигане на конкретни политически и идеологически цели, като основни характеристики са изненадата, липсата на предварително предупреждение и причиняването на възможно най-големи щети върху човешки живот и съоръжения.*

1. Въведение

По своята същност тероризмът е акт на насилие, който създава страх и несигурност в обществото и дестабилизира институциите, с оглед постигане на конкретни политически и идеологически цели, като основни характеристики са изненадата, липсата на предварително предупреждение и причиняването на възможно най-големи щети върху човешки живот и съоръжения.

Като предмостие на евроатлантическата ценностна система към Близкия Изток и Азия, България е поставена пред огромното предизвикателство да спира проникването на тероризма и международната организирана престъпност от изток, да се противопостави на радикалния ислямски фундаментализъм и да прекъсне пътищата за финансиране, незаконния трафик на хора, наркотици, оръжия и ембаргови стоки. В тази връзка могат да бъдат посочени следните рискови фактори за националната сигурност:

- събитията в Сирия, Ирак и Северна Африка и влиянието на терористичната организация „Ислямска държава в Ирак и Леванта” (ИДИЛ) в тези райони;

- многобройните имигрантски потоци от Сирия, Афганистан, Ирак, Северна Африка и други кризисни региони към Европа, които преминават през територията на България, както и преминаването на чуждестранни граждани, отправящи се към конфликтни зони с цел присъединяване към действащи терористични групи.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

- достъп до радикална пропаганда в Интернет за радикализиране на българското население;

- трайно установили се в страната чужди граждани от рискови държави;

- активизиране на дейността на религиозни организации и емисари сред определени български общности;

- международното участие в антитерористични и военно-хуманитарни операции на Република България.

От описаното до тук може да се обобщи, че съществува реална опасност за осъществяване на терористична дейност на територията на Република България, като най-сериозна заплаха са терористичните атаки срещу стратегически обекти, обектите и свързаните системи на критичната инфраструктура, мрежово-компютърни атаки срещу възлите на информационната инфраструктура.

Противодействието на тероризма в Република България се осъществява съгласно изискванията на Закон за противодействие на тероризма и редица специални закони - за министерството на вътрешните работи, за държавната агенция "Национална сигурност", за разузнаването, за отбраната и въоръжените сили на Република България, за военната полиция, за държавната агенция „Технически операции", за специалните разузнавателни средства, за мерките срещу прането на пари, за управление и функциониране на системата за защита на националната сигурност и др.

На основание на Конституцията и законите в Република България въоръжените сили участват в операции за противодействие на тероризма в страната съвместно с други държавни и местни органи и структури.

2. Изложение

Въоръжените сили на Република България включват: - Българската армия; - служба "Военна полиция"; - служба "Военна информация"; - военните академии и висшите военни училища; - Военномедицинската академия; - Националната гвардейска част; - Военно-географската служба; - Стационарната комуникационна и информационна система; - Централното военно окръжие; - Централния артилерийски технически изпитателен полигон; - Комендантство – МО.

Ръководството на въоръжените сили е дейност и отговорност на политическото и военно-политическото ръководство, а командването и управлението се осъществява от военните командири от всички нива по степени на правомощия. Системата за ръководство, командване и управление на въоръжените сили е изградена на три нива:

- стратегическо ниво (Президент, Министерски съвет, министър на отбраната, началник на отбраната, както и подчинените им щабове и служби);

- оперативно ниво (Съвместно командване на силите, Сухопътни войски, Военновъздушни сили и Военноморски сили);

- тактическо ниво – включва командирите и щабовете на формированията от въоръжените сили.

Държавното ръководство реализира ръководните си функции спрямо въоръжените сили: - *косвено* - закони и други нормативни актове, които въздействат с включените в тях правила, норми, ценности, мотиви и принципи; - *пряко* - заповеди, разпореждания, директиви, указания и др.

Ръководството е механизъм, който реализира идеите на управляващия субект по цялата йерархична верига в низходящ ред. По тази причина може да се приеме, че ръководство има и на военностратегическо, оперативно и тактическо ниво. Разглеждано в посочения смисъл, ръководството изразява обективно съществуващото единство между

две страни - управляващия субект (ръководител, командир или началник) и подпомагащите го управленски звена (щаб, отдел, екип от експерти и др.).

Първата страна е свързана с факта, че ръководството е акт на налагане на волята на управляващия субект спрямо управляваната система, което в научната литература се дефинира като *командване*. Втората страна на понятието е свързана с дейността на посочените подпомагащи звена по създаване на предпоставки за реализация и по прилагането на този акт, което се нарича *управление*. Единството на двете страни на ръководство се дефинира като *командване и управление*.

Командването и управлението са специализирани, експертни дейности, които обединяват всички управленчески функции във въоръжените сили и се осъществява по степени на правомощия. Командването и управлението се отнасят до всички нива на армейската структура в целия спектър от мисии и задачи. Чрез тях командирът упражнява предоставената му власт и носи пълна отговорност за изпълнението на задачите и постигането на поставените цели.

В мирно време въоръжените сили поддържат способности за участие в операции в отговор на кризи, кризисни ситуации и инциденти на територията на страната за осъществяване на: - дейности по контрола на въздушното пространство и морските пространства; - защита на стратегически обекти, включително на системите за производство, доставка и разпределение на енергийни ресурси; участие в операции по сдържане и неутрализиране на терористични, екстремистки и престъпни групи; - защита и подпомагане на населението при природни бедствия, аварии и екологични катастрофи; - неутрализиране на невзривени боеприпаси; - оказване на хуманитарна помощ; - съдействие за контрола на миграцията; - спасителни и евакуационни дейности; - помощ, при необходимост, на други държавни органи, организации.

Въоръжените сили на Република България участват в операции за противодействие на тероризма и в преодоляване на последиците от тероризъм в съответствие със закона и плановете за противодействие на тероризма, като имат право да извършват проверки за установяване на самоличността на лица, да задържат лица, да извършват обиск, да проверяват лични вещи и превозни средства, да извършват проверки в помещения без съгласието на собственика или обитателя или в тяхно отсъствие, да използват физическа сила и помощни средства, да използват оръжие.

При извършване на терористичен акт на територията на страната и обявяване на извънредно положение с решение на Министерския съвет държавните органи и въоръжените сили:

- охраняват обекти, застрашени от тероризъм;
- ограничават или забраняват полети на граждански въздухоплавателни средства и да въвеждат особен режим на корабоплаване в териториалното море и вътрешните морски води на страната;
- забраняват преминаването през държавната граница на Република България;
- ограничават движението по основни пътни артерии;
- ограничават движението на железопътния транспорт и да установяват контрол върху пътниците и товарите;
- ограничават свободното придвижване и да установяват контрол върху гражданите и превозните средства;
- контролират обектите от критичната инфраструктура на страната;
- ограничават или забраняват достъпа до държавни учреждения;
- забраняват провеждането на събрания, митинги и манифестации.

Въоръжените сили участват в съвместни операции за противодействие на тероризма, които могат да бъдат три основни форми:

- антитерористични – отбранителни мерки използвани да редуцират уязвимостта на индивидите и достъпа за терористични актове;

- контратерористични – нападателни действия за предотвратяване, възпиране и отговор спрямо тероризма;

- войскови – мащабна антитерористична операция с привличане на значителен контингент на сили и средства от въоръжените сили, чиито задачи не биха могли да бъдат изпълнени от една отделна силова държавна институция.

За провеждане на операции по противодействие на тероризма се извършва единно планиране на дейността в национален мащаб, подготовка на формированията, организиране на взаимодействието, управлението и осигуряването на операциите. За осигуряване на постоянна и адекватна защита на гражданите, територията и националните интереси от терористични заплахи се ангажират всички структури на държавното и местно управление, имащи отношение към въпросите на сигурността в държавата, областите и общините в Република България, съгласно Национален план за противодействие на тероризма, изготвен от Министерския съвет на Република България. За координиране на действията се въвеждат единни нива на заплаха и степени на готовност за обединяване усилията на Министерство на вътрешните работи (МВР), Министерство на отбраната (МО), Министерство на външните работи, Национална служба за охрана, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Министерство на енергетиката, Министерство на икономиката, Министерство на транспорта, информационните технологии и съобщенията, Министерство на здравеопазването, Министерство на земеделието и храните, Министерство на туризма, областни управители и кметове на общини.

Общото ръководство по противодействие на тероризма в Република България се осъществява от Министерския съвет, подпомаган от Съвет по сигурността. При възникване на необходимост към Съвета по сигурността се създават Консултативна група по противодействие на тероризма, Национален оперативен щаб, а за непосредствено управление на силите за реагиране в зоната на терористичния акт със заповед на ръководителя на националния оперативен щаб (НОЩ) се създава Временен оперативен щаб (ВОЩ).

Началникът на отбраната е в състава на консултативна група по противодействие на тероризма, която се ръководи от министъра на вътрешните работи.

Заместник-министър на отбраната, заместник-началник на отбраната и офицери от Щаба на отбраната са в състава на НОЩ за управление на силите и средствата при терористични заплахи или при овладяване на ситуацията вследствие на осъществени терористични актове с ръководител Министъра на вътрешните работи. В състава на ВОЩ се включват ръководителите на екипите, изпълняващи задачи по овладяване на ситуацията и представители на областния управител и кмета на общината. Ръководството на ВОЩ се осъществява от директора на областната дирекция на МВР, на чиято територия е извършен терористичен акт.

При провеждане на операции по противодействие на тероризма въоръжените сили изпълняват следните задачи:

- следят обстановката в кризисните региони за своевременно идентифициране и оценка за потенциални заплахи от терористични действия и разпространяване на оръжия за масово унищожение;

- поддържат в готовност сили и средства за: развръщане в съответствие с рисковете и заплахите; отбраната на територията, териториалното море и въздушното пространство на страната; поддържане на готовност и оказване на съдействие на компетентните държавни органи при хуманитарна помощ и спасителни действия на територията и в морските пространства на страната;

- оказват съдействие на органите на държавната власт по сигурността и охрана на реда в борбата им срещу разпространяване на оръжия за масово унищожение, незаконен трафик на оръжие и международен тероризъм;

- участват в охраната на стратегически обекти, на обекти и системи от критичната инфраструктура, за което може да се сключи договор със заинтересуваните лица, както и в операции за пресичане на терористични действия;

- във взаимодействие с органите на държавната власт по сигурността и охрана на реда разкриват, предотвратяват и пресичат терористични актове, освобождаване на заложници, разпространение на оръжия за масово унищожение и незаконен трафик на оръжие.

Съгласно изискванията на Закона за военната полиция, служба "Военна полиция" осъществява антитерористична дейност в Министерството на отбраната, в структурите на пряко подчинение на министъра на отбраната и в Българската армия с цел разкриване, предотвратяване, пресичане и противодействие на замислени, подготвени или започнали терористични актове и намаляване на рисковете за извършването им. За осъществяване на тези дейности, както и за задържане на извършители на особено опасни престъпления от общ характер, които оказват или са склонни да окажат въоръжена съпротива, или при освобождаване на заложници на органите на служба "Военна полиция" може да бъде възложено изпълнението на задачи в условията на висок риск и непосредствена опасност за живота и здравето.

Основни фази на операциите за противодействие на тероризма с участието на въоръжените сили:

1. Формиране, подготовка и поддържане в готовност - събиране и обмен на информация, кризисно планиране, определяне на необходимите сили и средства, провеждане на подготовка и докомплектуване с материални ресурси.

2. Овладяване на кризата - въвеждане на сили и средства от въоръжените сили в зоната на операцията с цел нарастване на способностите на министерството на вътрешните работи.

3. Ликвидиране на последствията - оказване на помощ на централната и местната власт за ликвидиране последствията от извършен терористичен акт със силите и средствата на наличните формированията за овладяване и/или преодоляване на последиците от бедствия.

4. Изтегляне - организирано изтегляне на формированията и завръщане в пунктовете за постоянна дислокация.

Решение за привеждане в действие на формированията за противодействие на тероризма от състава на въоръжените сили се взема от министъра на отбраната на Република България. Оповестяването и привеждането в готовност на органите за управление и определените формирования се извършва изборно, в съответствие с решението на министъра на отбраната, съобразно искането за оказване на помощ, възможностите на въоръжените сили и конкретната обстановка. Непосредственото привеждане в действие на формированията от въоръжените сили се извършва от командирите, началниците, от чийто състав са определените сили и средства.

Координацията при провеждане на операции за противодействие на тероризма се извършва от ВОЩ, а оперативното командване в района на операцията от оперативна група от Щаба на отбраната с представители на видовете въоръжени сили и структурите на пряко подчинение на министъра на отбраната, участващи в операцията. Тактическото командване и управление се осъществява от командирите на военните формирования, определени за изпълнение на задачите в съответните зони. За изпълнението на задачите от приведените в действие формирования за участие в операцията и въпросите свързани с управлението, осигуряването и взаимодействието с органите на държавната власт се докладва по команден ред.

За успешното участие на въоръжените сили при провеждане на операции за противодействие на тероризма е необходимо:

- своевременен обмен, обработване и анализиране на информация;
- осигуряване на необходимите материални и финансови ресурси;
- съгласуване на действията с органите на изпълнителната власт;
- своевременно развръщане на формированията от ВС;
- ефективно неутрализиране на терористичните и сепаратистки елементи;
- контрол на придвижването в районите на операцията;
- използването им в съответствие с делегираните права и отговорности.

При участието на въоръжените сили в операции за противодействие на тероризма е целесъобразно да бъдат отчетени следните специфични особености:

- при извънредна обстановка могат да бъдат наложени известни ограничения на основни права и свободи на гражданите;
- важно условие за успешен край на операцията е взаимодействието между всички държавни органи, компетентни да противодействат на тероризма, и средствата за масово осведомяване;
- предварително разработване на принципи за водене на преговори с терористи;
- прецизиране на съотношението между прилагането на сила при обезвреждане на терористи и психологическото въздействие върху тях;
- определяне на допустимите предели за прилагане на сила при неутрализиране на терористи.

В резултат на спецификата на терористичните актове и използването на факторите изненада, асиметричност и значителен брой жертви са необходими способности за незабавна реакция и съсредоточаване на значителен ресурс от сили и средства, за което се разработват планове на оперативно и тактическо ниво във въоръжените сили и съгласувани процедури за действие с органите на държавната власт и местната власт, за изграждане на къса, ясна и недвусмислена командна верига с конкретно делегирани правомощия по командване и управление.

Спецификата на операциите за противодействие на тероризма и включването на няколко ведомства в разрешаването на кризата изисква детайлно взаимодействие между институциите и единно управление. Според основни водещи документи „Подготовката на страната за отбрана обхваща изграждане на единна система за информация, сигурност, ранно предупреждение и управление на страната и въоръжените сили”.

Във връзка с участието на въоръжените сили в операции за противодействие на тероризма е необходимо да бъдат набелязани следните приоритетни задачи:

- постоянно усъвършенстване на нормативната уредба за противодействие на тероризма;
- изграждане на ефективно интегрирано разузнаване за осигуряване на навременна, точна информация за заплахите;

- усъвършенстване на методите за събиране на информация и изграждане на нова рамка за предупреждение по линия на разузнаването;

- подобряване на системата за управление, контрол, информационни системи и комуникации в структурата на въоръжените сили;

- усъвършенстване подготовката и оборудването на антитерористичните модули за увеличаване на тяхната мобилност и възможности;

- доразвиване на системата за медицинска помощ за придобиване на възможности за противодействие на биотероризма, борбата със заразни болести предизвикващи епидемии, както и с опасности водещи до жертви и пострадали.

Участието на въоръжените сили в борбата срещу тероризма се определя в зависимост от мащабите на неговото проявление. Формированията от въоръжените сили могат да участват в операции срещу разпространението на оръжия и терористични действия, когато усилията на органите за сигурност са недостатъчни за овладяване на обстановката и се застрашава сигурността и суверенитета на страната.

Управлението на въоръжените сили и структурите за национална сигурност и охрана на обществения ред при провеждане на операции за противодействие на тероризма трябва да бъде извършвано чрез изграждане на интегрирана система за ръководство, командване, управление и комуникационно-информационно осигуряване на съответните равнища.

Управлението на тактическите модули във въоръжените сили се осъществява по линия на дежурните служби, управленските звена на видовете въоръжени сили, подчинените щабове, ръководителите на зони и райони, оперативните дежурни и дежурните по военни формирования, чрез интегрираната комуникационно-информационна система на Българската армия.

За поддържане необходимия потенциал на силите, за повишаване и поддържане на способности следва да се провежда подготовка на формированията от въоръжените сили, която да осигурява:

- функционалност на формированията, обученост на личния състав, сглобеност и поддържане на висока готовност;

- придобиване и усъвършенстване на необходимите знания, умения и навици за успешно изпълнение на задачите;

- придобиване и усъвършенстване на способности за командване и управляване, организиране и ръководене на подготовката, и осигуряване на формированията за водене на операции за противодействие на тероризма;

- непрекъснато повишаване и усъвършенстване на квалификацията;

- готовност на формированията да водят решителни и ефективни операции чрез непрекъсната, целенасочена и постоянна подготовка, максимално близка до реалната обстановка.

Динамичният характер на операциите за противодействие на тероризма определя необходимостта от ефективна намеса, сигурност и гъвкаво ръководство, надеждна система за ранно предупреждение, тясно координиране и непрекъснато командване и управление на формированията (тактическите модули) от въоръжените сили.

3. Заключение

Като една от силовите институции в държавата въоръжените сили имат своето място в противопоставянето на заплахи, минимизирането на рискове, предотвратяването и ликвидирането на последствия от терористични актове т. е. във всички етапи на борбата с тероризма. Важно е да се подчертае факта, че въоръжените сили не са водеща институция в борбата срещу тероризма поради спецификата на тяхното основно предназначение. Те

могат да подпомагат общите усилия на държавата или определен международен кръг от държави за по-успешно справяне с този проблем.

Участието на въоръжените сили в операции за противодействие на тероризма означава провеждане на необходимата подготовка за справяне с тези задачи, както и усъвършенстване на взаимодействието им с държавните органи за сигурност и охрана на обществения ред и с тези на държавната и местната власт за постигане на висока ефективност в действията при противодействие на тероризма.

Усилията следва да са съсредоточени върху развитието на сили със способност за бързо развръщане. Те трябва да притежават висока бойна ефективност, да бъдат използваеми в целия спектър от мисии и способни за развръщане за операции в страната. За тази цел е необходимо да бъдат определени ясни приоритети и да бъдат осигурени съответните ресурси за реализирането им, което да гарантира ефективно изпълнение на възложените задачи на въоръжените сили при участие в операции за противодействие на тероризма в страната.

За постигане на основната цел по противодействие на тероризма в страната е необходимо да бъдат развивани професионално подготвени сили, които да бъдат достатъчно гъвкави и способни за изпълнение на задачи в широк спектър.

ЛИТЕРАТУРА:

[1] Закон за отбраната и въоръжените сили, обн. в ДВ на 12.05.2009 г., посл. изм. и доп., бр. 17 от 1.03.2016 г.

[2] Закон за управление и функциониране на системата за защита на националната сигурност, обн., ДВ, бр. 61 от 11.08.2015 г., в сила от 1.11.2015 г.

[3] Закон за противодействие на тероризма, обн., ДВ, бр. 103 от 27.12.2016 г.

[4] Стратегия за национална сигурност, приета с Решение на НС от 25.02.2011 г., обн., ДВ, бр. 19 от 8.03.2011 г.

[5] Национална отбранителна стратегия, МО, С., 2016.

[6] Доктрина на въоръжените сили на Р България, МО, С., 2017 г.

[7] Стратегия за противодействие на радикализацията и тероризма (2015-2020г.), приета с РМС № 1039 от 30.12.2015 г.

[8] Райков П., Тероризъм и военен антитероризъм, Издателство “Ваньо Недков”, С., 2009.

[9] Слатински Н., Националната сигурност: аспекти, анализи, алтернативи, С., 2004.

[10] Krastev, K., Hristov, H., Development of warfare and counter-terrorism, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 6, 2014, pp. 179-186.

[11] Христов, Х., Подходи за оцеляване при терористичен акт, Proceedings of the international conference "MATTEX 2014" - 20 - 22 November 2014 г., ISSN: 1314-3921, vol. 2, 2014, pp. 125-131.

Име на автора: докторант Любомир К. Дучев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: l_duchev_2012@abv.bg

NAZISM AND ISLAM

MILEN M. IVANOV

ABSTRACT: *German diplomat Eberhard von Storrer, a man with serious experience in diplomacy in the Arab world, received as a German ambassador to Cairo, concludes that by fighting against the United Kingdom and France, Germany has a very profitable role in the eyes of the Muslims. According to him, it is time to strengthen the relationship between Islam and national-socialism.*

KEYWORDS: *Nazism, Islam.*

НАЦИЗЪМ И ИСЛЯМ

МИЛЕН М. ИВАНОВ

АБСТРАКТ: *Немският дипломат Еберхард фон Щорер, човек със сериозен опит в дипломацията в арабския свят, получен като германски посланик в Кайро, стига до извода, че воювайки против Великобритания и Франция, Германия получава изключително изгодна роля в очите на мюсюлманите. Според него е настъпило време да се укрепят отношенията между исляма и национал-социализма.*

1. Въведение

Американският историк Дейвид Моутъдел (David Motadel) в своето обширно изследване „Ислямът и войните на нацистка Германия“ (Islam and Nazi Germany’s War)[1] разказва за следния епизод от есента на 1941 година: Немският дипломат Еберхард фон Щорер, човек със сериозен опит в дипломацията в арабския свят, получен като германски посланик в Кайро, стига до извода, че воювайки против Великобритания и Франция, Германия получава изключително изгодна роля в очите на мюсюлманите. Според него е настъпило време да се укрепят отношенията между исляма и национал-социализма. На 18 ноември 1941 г. той изпраща на висшето германско ръководство меморандум, в който предлага да се развърне широка програма за взаимодействие между двете идеологии, която да е базирана на предпоставките за близко родство между тях. Двете идеологии, според Щорер, намират общи черти в безпрекословното подчинение на лидера, приоритет на семейните ценности и привързаността към войната. Мюсюлманите, посочва тай, са „де факто фанатици“, и лесно могат да се уговорят за обединение с нацистите, още повече че „фюрерът и без това се ползва с уважение и авторитет среди мюсюлманите заради борбата му с юдаизма“.

2. Изложение

Този пронацистки курс е поддържан силно и от великия йерусалимски мюфтия Мухàмед Хадж Амин ал-Хуссейни, бившия премиер-министър на Ирак - Рашид ал-Гайлани, шейх Арслан в Сирия и много други арабски политици2. Особено активен в тази

[1] *Motadel, D.* „Islam and Nazi Germany's War“; Belknap Press, November 2014; ISBN 9780674724600.
[2] *Breitman, R, Goda, N.J.W,* „Hitler’s Shadow – Nazis and the Middle East“, http://www.crethiplethi.com/hitler-s-shadow-nazis-and-the-middle-east/the-holocaust/2012/ , Посетен на 27.08.2018 г.

насока е Хадж Амин ал-Хуссейни. Още през 1933 г. той установява контакти с нацистите, които по-късно, по време на големите погроми над еврейското население през 1936 г. в Палестина, започват да му оказват военна и финансова помощ. През 1939 г. мюфтията отива в Багдад, където активно съдейства за идването на власт на протежето на нацистите Рашид ал-Гайлани през 1940 г. След като английските власти подавят прогерманското въстание, организирано от ал-Гайлани, мюфтията бяга в Техеран, а след това, вече по време на Втората световна война, през октомври 1941 г. пристига в Италия, откъдето Мусолини го изпраща в Берлин. Там той установява тесни връзки с Адолф Айхман. Заедно с гауптщурмфюрера от СС Брунер[3], посещава концлагерите Заксенхаузен, Освенцим и Майданек. След края на войната мюфтията съдейства на Брунер да избяга и да се укрие в Близкия Изток.

Мюфтията получава в Берлин ежемесечно 75 хиляди марки, част от които се използват за внедряване на нацистката агентура в арабските страни. Също така подпомага Хитлер при създаването на мюсюлманските формирования в състава на войските на СС. След него в Берлин пристига и Алимджан Идрис, който превежда „Майн Кампф“ на персийски език, и е изпратен в окупираните територии на СССР, за да вербува студенти-мюсюлмани, които да учат в Германия. И Амин ал-Хусейни, и Алимджан Идрис са отявлени антисемити и използват религиозната риторика, за оправдание на своите позиции и привързаност към нацистката идеология.

През 1941 година мюфтията подготвя проект на договор между арабските държави и страните от Оста (Германия, Италия и т.н.), като една от точките гласи следното: „Германия и Италия признават незаконността на еврейското национално огнище в Палестина. Те признават правото на Палестина и другите арабски страни да решат еврейския въпрос в Палестина и в другите арабски страни, както това изискват техните национални интереси и по такъв начин, както еврейския въпрос се решава в страните от Оста.“

В навечерието на Втората световна война германското разузнаване създава в арабските страни широко разклонена шпионска мрежа, в която са завербувани представители от всички слоеве на населението. Пропагандата се опитва да внуши на арабската общественост, че Германия е „най-добрия приятел на арабските народи“ и че избавлението от англо-френското колониално управление те могат да постигнат само с помощта на германското ръководство, което, както и арабските политици, е решително против всякакви планове за създаване на еврейска държава в Палестина.

През 1937 г. видният нацист и ръководител на „Хитлеюгент“ Балдур фон Ширах посещава няколко арабски страни. През 1939 г. в Каиро пристига Йозеф Гьобелс, а малко преди войната Адолф Айхман се среща в Палестина със свои съмишленици. Всички тези политически ходове показват трайното обвързване на нацистка Германия с арабските политици и сериозните намерения и на двете страни за съвместни действия и тясно сътрудничество. Химлер скромно счита своята идея да постави мюсюлманите под есесовските знамена за гениална. В беседа с Гьобелс, рейхсфюрерът заявява: „Аз нямам нищо против исляма, защото той обещава на мюсюлманите рай, ако те загинат в бой, а това е религия, която е много прагматична и привлекателна за войниците!“.

[3] Ало́из Бру́ннер (нем. Alois Brunner, 1912—2010) — гауптштурмфюрер от СС, един из главните съратници на Адолф Айхман при осъществяване на т.нар. „Окончателното решение на еврейския въпрос“. Като ръководител на специалните отряди на СС Бруннер от 1939 до 1945 година е отговорен за депортацията на повече от 100 хиляди евреи от Виена, Берлин, Гърция, Франция и Словакия в лагерите на смъртта на Третия райх.

На 11 март 1941 г. барон фон Вайцзекер, щатс-секретар на нацисткото министерство на външните работи, предава на личния секретар на великия йерусалимски мюфтия в Берлин съобщение: „Немците и арабите имат в лицето на англичаните и евреите общи врагове и станаха съюзници в борбата против тях“. А на 23 май 1941 г. Хитлер подписва заповед № 30, в която пише, че „арабското освободително движение в Средния Изток се явява наш (на Германия) естествен съюзник против Англия“.4

Както пише Шимон Бриман в своята статия „Мюсюлманите в СС“5, „именно тесните отношения на хитлеристите с ислямистите и арабските националисти стават трамплин за бягството на стотици нацисти към Близкия Изток след разгрома на Третия райх. Предварително създаденият „Арабо-германски център за емиграция“ веднага след края на войната успява да прехвърли в арабските страни от региона почти 1500 хитлерови офицери (към края на 50-тегодини броят им нараства до 8000). С цел маскировка хиляди нацисти приемат исляма и взимат арабски имена. Центърът се ръководи от бившия офицер от щаба на фелдмаршал Ромел, подполковник Ханс Мюлер. Той, както и много други нацистки офицери, приема исляма и се легендира като сирийския гражданин Хасан Бей.

Според различни израелски източници и според мнението на знаменития „ловец на нацисти“ Симон Визентал, избегналите възмездието военнопрестъпници се опитват да се самоорганизират и създават международна нацистка мрежа, известна като „Организация на бивши членове на СС“ (Organisation der ehemaligen SS-Angehцrigen – ODESSA)6. Тази организация успява да осигури прехвърлянето на нацистите по т. нар. „пътеки на плъховете“. Участие в дългогодишното функциониране на тези пътища взима и Ватикана.7 Още в края на 1942 година, кардинал Луиджи Мальоне, поради съмнения относно победния край на войната за нацистка Германия, започва да сондира властовите и клерикалните кръгове в Аржентина за възможността там да емигрират определен брой нацисти. Голяма част от тези нацисти наистина бягат в Аржентина, Бразилия, Парагвай и Чили, друга голяма група се прехвърля в Съединените Щати, Канада, Испания, а третия вектор на бягствата са в страните от Арабския Изток. Маршрутите за прехвърляне в арабските страни са организирани от родения във Франция кардинал Ежен Тиссеран, признат специалист по източни езици, включително арабски и иврит8.

Поражението на Германия през 1945 г. не води до крах на германо-арабските отношения, насочени към западните демокрации и „световното еврейство“. Пронацистките настроения в арабския свят продължават да съществуват и след войната. И не е случайно, че именно Арабския изток, наред с Латинска Америка, става убежище за нацистките престъпници, където те не без основания разчитат на топъл прием. Бягащите нацисти установяват тесни връзки с щаб-квартирата на Хадж Амин ал-Хуссейни в Каийро. Важен за отбелязване факт е, че дългогодишния председател на Организацията за освобождение на Палестина (ООП) - Ясер Арафат9, е племенник на мюфтията, който

---

[4] *Борисов А.,* Нюрнбергский процесс, сборник документов (Приложения) «Hitlers Weisungen fur die Kriegfuhrung 1939—1945», стр. 120—122.

[5] http://rjews.net/gazeta/Lib/briman/5-briman.shtml Посетен на 02.08.2018 г.

[6] *Guy Walters* (2010). Hunting Evil: The Nazi War Criminals Who Escaped and the Quest to Bring Them to Justice. Crown/Archetype. ISBN 0307592480 – via Google Books, preview.

[7] *Шахрад С.*, „Тайны Ватикана. История, святыни, жизнь и смерть в святой обители“; Рипол Классик, 2008, ISBN: 978-5-386-01006-5

[8] *Гельман, З.* Нацистское обетование Арабского Востока; 26.06.2015, http://nvo.ng.ru/spforces/2015-06-26/14_nazi.html. Посетен на 20.04.2018 г.

[9] роден като Мухаммад ’Абд ар-Рахман ’Абд ар-Ра‘ӯф ‘Арāфат ал-Кхидуа ал-Хуccайнӣ

умира през 1974 г. в Бейрут, и по време на следването10 си преминава обучение при Ото Скорцени.1112

Емигриралите в Близкия Изток нацистки офицери започват да работят по специалността си във всички държави, в които се установяват. Поради ограничено място на публикацията даваме само няколко примера:

Бившият офицер СС войските Тифенбахер участва в изграждането и обучението на съвременната египетска полиция.

Оскар Дирлевангер (специалист по противопартизански операции, воюва в Легиона "Кондор" в Испания, командир на SS батальон „Дирлевангер“ (SS-Sonder Bataillon Dirlewanger,) подготвя диверсанти за египетската армия за действия против Израел.

Отделът за пропаганда на египетската служба за сигурност ръководи Хусса Налисман, или бившия обергруппенфюрер от СС Мозер.

Тайната държавна полиция на Египет оглавява Хамид Сулейман – или бившия ръководител на Гестапо в Улм, группенфюрера от СС Хенрих Зелман.

Политическият отдел на полицията се оглавява от полковник Халил Ибн-Салям - в миналото оберштурмбанфюрер от СС Бернхард Бендер.13

Генерал-лейтенант Артур Шмитт, командир на една от дивизиите на Африканския корпус (дивизията „Bardia“ в сектора на Sollum-Bardia). Попада в британски плен през 1942 г. и освободен през 1947. Веднага след това е нает от Лигата на арабските държави за „формиране на ефективни египетски и сирийски бойни части“. Живее в Кйро под псевдонима „Г-н Голдщайн“ .

Според историка от сръбски произход Джени Лебел14:

Штурмбанфюрер от СС Хенрих Вилерман от Дахау (Наим Фахим) става ръководител на концлагера „Самара“ (200 км. на югозапад от Александрия, Египет).

Началникът на Гестапо във Варшава и бивш командир на личната охрана на Хитлер, Леополд Хлейм (Наем ан-Нашар), се занимава със създаването на съвременната египетска тайна полиция15.

Началникът на Гестапо в Рур - Йохан Демлинг извършва реорганизацията на службата за сигурност на Египет през 1953 г. и е съветник на министъра на вътрешните работи на Египет.

Генералът от вермахта Оскар Минцел, благодарение на Отто Скорцени, ръководи реорганизацията и подготовката на танковите войски.

Координатор на цялата египетска пропаганда против Израел става бившия съратник на Гьобелс Йохан фон Леерс – антисемит, редактор на нацистко списание и автор на книгата „Евреите сред нас“ (1935)16. Заради възможността да продължи да воюва с евреите Леерс приема през 1956 г. исляма. В Кайро Леерс ръководи „устройването“ на избягалите в арабските страни немски военни престъпници. В качеството си на съветник на министерствата на държавното ръководство на Египет, и с активното участие на

---

[10] Ясер Арафат завършва инженерния факултет на Каирския университет. Служи като лейтенант от инженерните войски в египетската армия.

[11] *Otto Skorzeny*, My Commando Operations: The Memoirs of Hitler's Most Daring Commando Commando (Schiffer Military History) Hardcover – January 1, 1995

[12] В Египет е заминава по молба на Рейнхард Гелен.

[13] *Яков Этингер*, «Сакраментальный Альянс. Германские нацисты на арабском Востоке после Второй мировой войны.», Лехаим 6 (110), июнь 2001

[14] *Lebl, Ženi*, Haj Amin and Berlin, Belgrade 2003

[15] *Сергей Кулида*. Израильский Зорге: жизнь и судьба. Mishmar.Info (5 июня 2009). Посетен на 26.08.2018 г.

[16] https://newsland.com/user/2152808416/content/velikie-liudi-raznykh-epokh-govoriat-o-evreiakh-evrei-govoriat-o-sebe/1384345. Посетен на 20.09.2018 г.

специалиста по арабските дела във ведомството на Рибентроп барон фон Милденщайн, Леерс последователно насажда в Арабския изток идеите на нацизма. Във връзка с това на 30 март 1956 г. германския социал-демократически вестник „Форвертс“, съобщава, че Леерс се стреми да създаде в Египет „постоянна арабска нацистка организация“. И тук не става въпрос само за пропаганда чрез разпространението на „Майн кампф“, книга, която и до днес е бестселър в арабските държави, но и до създаването на мощна пропагандна машина насочена към адаптацията на нацистките идеи към мюсюлманската идеология.

Близък колега на Леерс е секретарят на ръководеният от мюфтията ал-Хуссейни Ислямския конгрес17 Салаб Гафа или бившия член на НСДАП Ханс Апплер. По този повод „Ню-Йорк таймс мегазин“ съобщава на 27 юли 1958 г.: „Египетските пропагандисти с помощта на германски специалисти, оцелели след краха на нацизма, превръщат каирското радио в необичайно мощно оръдие на нацистката пропаганда, насочено срещу Израел“.18

Подобна е ситуацията и в другите арабски държави в региона. Например в Сирия, бившият служител на Гестапо Рапп оглавява сирийската служба за сигурност и по-специално контраразузнаването. За истински родоначалник на съвременните сирийски специални служби се счита споменатият вече Алоис Брунер. Гауптштурмфюрерът от СС, доверено лице на Айхман, се появява в Дамаск през 1954 г. под името „Георг Фишер“, бягайки от ФРГ, където живее под чужди имена, и поставя основите на Главното управление за безопасност (Idarat al-Amn al-Amm)19.

Начело на германската военна мисия, която ръководи обучението и подготовката на местната армия се намира бившия полковник от хитлеровия Генерален щаб – Крибл20.

Хитлеристите взимат и активно участие в многобройните държавни преврати в Сирия. Например, Рапп е един от организаторите на военния пуч в Дамаск през март 1949 г. По време на управлението на генерал Адиба аш-Шишакли в страната действат поне 11 германски военни съветници - бивши висши и старши офицери от Вермахта, които помагат на сирийския диктатор в организирането на обединението на арабските държави в Обединената Арабска Република.

Нацистката пропаганда в Ирак започва още през 1933 г., когато нацистите идват на власт в Германия и Берлин започва да излъчва радиопредавания на арабски език. В Ирак се разпространява нацистка литература, а през 1933 г. е и първият опит да се преведе „Майн кампф“ на арабски език – преводач е Юнис ал-Сабави.

Нацистка Германия е основния организатор и поддръжник на държавният преврат в Ирак, предвождан на Рашид Али ал-Гайлани през април 1941 г. Възползвайки се от пораженията на Англия в Европа и в Близкия Изток, Рашид Али ал-Гайлани и прогерманската националистическа групировка „Златния квадрат“, ръководена от полковниците Салах ад-Дин ас-Сабах, Махмуд Салман, Фахми Саид и Кямил Шабиб, заедно с началника на иракския генерален щаб Амин Заки Сулейман, осъществяват

[17] Световния ислямски конгрес (The World Islamic Congress) е организация създадена от Саудитска арабия в Ерусалим през 1931 г. и включва 22 ислямски държави. Щаб-квартира в Карачи (Пакистан). Реално организацията започва своята дейност през 1949 г.. http://www.motamaralalamalislami.org/

[18] *Шимон Бриман*, „Мусулмане в СС“, Вести, Иерусалим, 25 апреля 2002

[19] http://agentura.ru/dossier/syria/ , Посетен на 26.08.2018 г.

[20] Rainer Kriebel. Преди да замине като съветник в Сирия е използван като анализатор от американското разузнаване. https://de.wikipedia.org/wiki/Rainer_Kriebel , Посетено на 28.08.2018 г.

военния преврат21.След преврата министър на просвещението става Джабр Омар – бивш офицер абверовия спецназ „Бранденбург“.22

Съвременният екстремизъм на саудитските уахабити също е изкован от бивши есесовци. За това съобщава още преди 50 години авторитетния каирски вестник „Аль-Ахрам“: „Бившите немски офицери проявяват голям интерес към Саудитска Арабия. Те разглеждат уахабитите като едно от най-перспективните направления в исляма. Офицерите от СС са създали в този страна военно-тренировъчни лагери, в които преминават подготовка млади уахабити“. Вероятността и Бин-Ладен, и редица чеченски полеви командири да са придобили опит и да са тренирали по методиките на СС е доста голяма.

Всичко казано до тук ни води към логичното заключение, че използвания от много автори термин „ислямски фашизъм“ може да се счита за напълно легитимно твърдение. Още през 2002 г. Фукуяма твърди, че днешния „конфликт на цивилизациите“, е не просто борба с тероризма и не борба с исляма като религия или цивилизация, а по-скоро „борба с ислямофашизма“, тоест с радикално нетолерантна и антисъвременна доктрина, отричаща ценностите на западната цивилизация, която е получила разпространение в много части ислямския свят23.

Популяризаторите на термина „исламофашизъм“ аргументират неговото използване по следните причини24: През времето, след Втората световна война, терминът „фашизъм“ е изгубил своя етно-расов оттенък и започва да означава всяка тоталитарна система и идеология, пропагандираща превъзходството на дадена група хора над всички останали, отричаща демокрацията, плурализма, свободата на словото и т. н. Типични проявления на такова тоталитарно мислене някои изследователи считат омразата към Запада, към евреите, към хората с нетрадиционна сексуална ориентация, склонност към теориите на конспирациите, и готовност да се оправдават насилието и жестокостта в името на политически цели, които оправдават средствата.

Според някои сведения, един из теоретиците на съвременния радикален ислям, египтянина Сейид Кутб25 признава влиянието, което му е оказал френския фашистки философ Алексис Каррел26.

После атентатите на 11 септември в Ню-Йорк, терминът „исламофашизъм“ е популяризиран в САЩ от журналиста Кристофър Хитченсън27, а след това е използван от президента на САЩ Джордж Буш в официално заявление28.

Терминът „ислямофашизъм“ по отношение на ислямските радикали използват и бившия премиер-министър на Великобритания Тони Блеър29, министърът на

---

[21] Садам.меч востока. Глава 4. Независимый Ирак. XX век, http://saddam-mech-vostoka.narod.ru/ir7.html, Посетен на 26.08.2018 г.

[22] *Сатановский, Е.*, „Жил-был народ… Пособие по выживанию в геноциде“, ЛитРес;2015, ISBN: 978-5-699-82416-8

[23] *Дугин А. Г.* Глава 4. Малый шайтан исламо-фашизма (рецензия на статью Ф. Фукуямы «Исламо-фашизм») // Геополитика постмодерна. — М.: Амфора, 2007. — 177 с.

[24] Феофанофф Г. Исламофашизм: оскорбление или комплимент?. «Время новостей» (28 августа 2006). Проверено 19 сентября 2015. Архивировано из первоисточника 30 августа 2006.

[25] Сейид Ибрахим Кутб - египетски писател и философ, идеолог на „Мюсюлмански братя“.

[26] *Феофанофф Г.* Исламофашизм: оскорбление или комплимент?. «Время новостей» (28.08.2006). http://www.blagovest-info.ru/index.php?ss=2&s=7&id=8533 , Посетен на 26.08.2018 г.

[27] *Николя Лебур.* «Исламофашизм»: новое заблуждение французских левых. Slate.fr (18.02.2015). https://inosmi.ru/world/20150218/226350235.html , Посетен на 25.08.2018 г.

[28] Президент Буш о Ливане. Редакционный комментарий, отражающий точку зрения правительства США. Голос Америки (08.12.2006). https://web.archive.org/web/20150919110624/http://www.golos-ameriki.ru/content/a-33-2006-08-12-voa3/655559.html , Посетен на 26.08.2018 г.

националната сигурност на САЩ Майкъл Чертофф30, бившият съветник на Ричард Никсън Чак Колсън31, политически наблюдатели от редица американски медии32.

Ако в Германия, след края на Втората световна война е проведена денацификация, то нищо подобно не се случва в Близкия Изток. Напротив, в много арабски страни на власт идват хора, тясно свързани в близкото си минало с нацистите и считащи Хитлер за герой и учител. В арабските страни бягат и намират убежище тези нацистки последователи, които не се примиряват с поражението, и планират и реализират главната нацистка геополитическа програма. Голяма част от избягалите офицери през 60-те и 80-те години се завръщат в Западна Германия и даже се включват в политическия живот на страната.

Например канцлерът Аденауер (федерален канцлер на ФРГ от 1949 до 1963 г.) назначава за министър по въпросите на бежанците Теодор Оберлендер, ветеран от СС батальона „Нахтигал“. Друг член на кабинета – министърът на вътрешните работи Герхард Шрьодер – започва политическата си кариера като хитлеров щурмовак. Министърът на правосъдието Фриц Шеффер в миналото нарича Хитлер „спасителят на райха“. Още по-противоречива е кандидатурата за поста на държавен секретар. Ханс Глобке е човек с добре известно нацистко минало, който отговаря за ключовите назначения в апарата на правителството и е близък приятел на Аденауер и втория по влияние човек в Германия. Като комисар на Третия райх по въпросите на защитата на немската кръв и немската чест, адвокатът Глобке играе ключова роля в изготвянето на расистките Нюрнбергски закони през 1935 г. и разработва принципите за „германизация“ на завоюваните народи в окупираните страни.

Вероятно, именно Глобке в най-голяма степен способства за завръщането и влизането във властта на голям брой бивши нацисти. Макар нацисткият елит да е ликвидиран в резултат от самоубийства и бягства зад граница или приключва земния си път на бесилото в резултат от Нюрнбергския трибунал, много високопоставени чиновници успяват да запазят и получат високи постове в държавното управление. През октомври 1951 година самият Аденауер признава, че неговото Министерство на външните работи е пълно с бивши нацисти и протежета на Йоахим фон Рибентроп. Скритата реставрацията на нацизма по времето Аденауер въвежда в оборот двойните морални стандарти, станали след това неотменна част от обществения живот на Германия и до днес.

Във връзка с горното трябва да отбележим и голямата роля, която играят нацистите за формирането на арабския тероризъм. Характерно е, че традициите, заложени още в първите следвоенни години, се оказват твърде витални. Достатъчно е се припомним за тесните връзки на германската терористична група „Баадер-Майнхоф“ с палестинските терористи.

Франсис Фукуяма и Надав Самин в своята статия за ислямизма отбелязват: “Ислямизмът,... всъщност не си поставя за цел възстановяването на някакви архаични, изконни форми на исляма. Това не е традиционалистско, а съвсем съвременно движение... Влиянието на тези идеологии е особено забележимо при египтянина Сейид Кутба, станал,

---

[29] *Феофанофф Г.* Исламофашизм: оскорбление или комплимент?. «Время новостей» (28.08.2006). http://www.blagovest-info.ru/index.php?ss=2&s=7&id=8533 , Посетен на 26.08.2018 г.

[30] *Pipes, D.*, „At War with Islamic Fascists“, FrontPageMagazine.com, August 14, 2006. Посетен на 25.08.2018 г.

[31] *Колсон, Ч.*“Сто миллионов мусульман во всем мире находятся под влиянием исламо-фашизма“, regions.ru, 13.06.2007. https://web.archive.org/web/20100630101935/http://i-r-p.ru/page/stream-event/index-13699.html, Посетен на 26.08.2018 г.

[32] National Review Online: Для такой характеристики радикального ислама, как «исламский фашизм», есть все основания, Голос России: Эфир дайджест, 02.10.2006, https://web.archive.org/web/20071108042155/http://i-r-p.ru/page/stream-event/index-8089.html, Посетен на 25.08.2018 г.

след Втората световна война лидер и главен идеолог на Асоциацията на мюсюлманските братя. В своята основна работа „Жалони по пътя“ Кутб призовава към създаването на монолитна държава, ръководена от ислямска партия, като в името на тази цел е оправдано използването на нсякакви, дори и най-жестоки средства. Обществото, което изгражда в своето въображение Кутб, трябва да е безкласово: „егоистичните индивиди“ на либералното общество ще бъдат ликвидирани заедно с „експлоатацията на човек от човека“. Такъв „ленинизъм в ислямска обвивка“ се използва днес в идеологията на голяма част от ислямистите. Същите цели проповядват и национал-социалистите. Бенито Муссолини в своята статия „Основни идеи на фашизма” пише: „Извън държавата няма индивид, няма и групи (политически партии, общества, профсъюзи, класи). Затова фашизмът е против социализма, който свежда историческото развитие до класовата борба и не признава държавното единство, сливащо класите в единна икономическа и морална реалност; фашизмът е против класовия синдикализъм”. Не е трудно да се разбере, че концепцията Кутба е точно повторение именно на фашистката идея за монолитна държава, а не на комунистическата идея с нейните сложности. Не бива да пренебрегваме и самоопределението на арабите, като „висша мюсюлманска раса“, което произтича, разбира се, от арабския произход на Пророка.

О всичко казано до тук може а обобщим, че на доктиранално ниво имаме почти пълно съвпадение на идеите на част от мюсюлманското общество и по специално това от Арабския Изток с тези на нацистите и фашистите. Имаме множество примери за дифузия на идеите, заложени доктрините им. Това позволява след Втората световна война, нацистките престъпници да се укрият и да се имплантират успешно в арабското общество, като стават гръбнака на висшите класи и оказват сериозно въздействие върху политическото и икономическото развитие на тези държави. Приемайки бита и традициите на арабското общество и държави днес, вероятно наследниците на тези, укрили се нацисти, заемат многобройни високи постове в същото това общество и продължават да оказват влияние на геополитиката. В същото време още от времето на Аденауер в самата Германия във висшите етажи на немското общество действат оцелели нацисти, а днес вероятно и многобройни техни наследници и сподвижници, за които идеите на дедите им едва ли са чужди [34], [35], [36].

Тук вече може да поставим въпрос и за мигранските процеси, толкова парадоксални и необясними в голямата си част, под светлините на новото знание, което имаме на базата на написаното до сега и да оценим смисъла, мащабите и значимостта на феномен. Какъв е истинския смисъл от такова методично преместване на огромни маси хора? Защо сега и защо именно към сърцето на Европа – Германия? Дали това е търсене от страна бедните ислямски мигранти на „достойно място за работа“ или е опит да се възродят плановете за световно господства на нацистката идеологии на базата на нова, този път – мюсюлманска, - идеология?

3. Заключение

Имаме пълното основание да считаме, че наследниците на Хитлер са определили ислямския свят за плацдарм за нов опит да се наложи световно господство. Основа за такова странно, на пръв поглед преобразование на нацизма е ясното заявление та Хитлер за сходството на мюсюлманските и нацистките идеи, което той прави по време на една от срещите си с мюфтията ал-Хуссейни.

Това още веднъж показва, че терористите в Близкия Изток не са стадо безмозъчни фанатици, а специален държавен проект. Пък и те самите се наричат така – Ислямска държава. Именно държавни структури осигуряват прикритията им в медиите, помагат да

се маскират под определена идеология, пускат контролирано конфиденциална информация, формират контрамерки и организират прикрития. Генералната цел на всичко това не е нова, и не се крие. Тя е такава каквато е била през 1933 г. –световно господство на единната държава – нацистката.

ЛИТЕРАТУРА:

[1] Motadel, D. „Islam and Nazi Germany's War“; Belknap Press, November 2014; ISBN 9780674724600.

[2] E. von Stohrer: Vorschläge für ein «Islam-Programm» v. 18. November 1941. in Bernd Philipp Schröder: Deutschland und der Mittlere Osten im Zweiten Weltkrieg. Reihe: Studien und Dokumente zur Geschichte des 2. WK., Hg. Arbeitskreis für Wehrforschung, 16. Musterschmidt, Göttingen 1975 ISBN 3788114169.

[3] Breitman, R, Goda, N.J.W, „Hitler’s Shadow – Nazis and the Middle East“, http://www.crethiplethi.com/hitler-s-shadow-nazis-and-the-middle-east/the-holocaust/2012/ , Посетен на 27.08.2018 г.

[4] Ало́из Бру́ннер (нем. Alois Brunner, 1912—2010) — гауптштурмфюрер от СС, един из главните съратници на Адолф Айхман при осъществяване на т.нар. „Окончателното решение на еврейския въпрос“. Като ръководител на специалните отряди на СС Бруннер от 1939 до 1945 година е отговорен за депортацията на повече от 100 хиляди евреи от Виена, Берлин, Гърция, Франция и Словакия в лагерите на смъртта на Третия райх.

[5] Борисов А., Нюрнбергский процесс, сборник документов (Приложения) «Hitlers Weisungen fur die Kriegfuhrung 1939—1945», стр. 120—122.

[6] http://rjews.net/gazeta/Lib/briman/5-briman.shtml Посетен на 02.08.2018 г.

[7] Guy Walters (2010). Hunting Evil: The Nazi War Criminals Who Escaped and the Quest to Bring Them to Justice. Crown/Archetype. ISBN 0307592480 – via Google Books, preview.

[8] Шахрад С., „Тайны Ватикана. История, святыни, жизнь и смерть в святой обители“; Рипол Классик, 2008, ISBN: 978-5-386-01006-5

[9] Гельман, З. Нацистское обетование Арабского Востока; 26.06.2015, http://nvo.ng.ru/spforces/2015-06-26/14_nazi.html. Посетен на 20.04.2018 г.

[10] роден като Мухаммад ’Абд ар-Рахман ’Абд ар-Ра‘ӯф ‘Арāфат ал-Кхидуа ал-Хусс̣айнӣ

[11] Ясер Арафат завършва инженерния факултет на Каирския университет. Служи като лейтенант от инженерните войски в египетската армия.

[12] Otto Skorzeny, My Commando Operations: The Memoirs of Hitler's Most Daring Commando Commando (Schiffer Military History) Hardcover – January 1, 1995

[13] В Египет е заминава по молба на Рейнхард Гелен.

[14] Яков Этингер, «Сакраментальный Альянс. Германские нацисты на арабском Востоке после Второй мировой войны.», Лехаим 6 (110), июнь 2001.

[15] Lebl, Ženi, Haj Amin and Berlin, Belgrade 2003.

[16] Сергей Кулида. Израильский Зорге: жизнь и судьба. Mishmar.Info (5 июня 2009). Посетен на 26.08.2018 г.

[17] https://newsland.com/user/2152808416/content/velikie-liudi-raznykh-epokh-govoriat-o-evreiakh-evrei-govoriat-o-sebe/1384345. Посетен на 20.09.2018 г.

[18] Световния ислямски конгрес (The World Islamic Congress) е организация създадена от Саудитска арабия в Ерусалим през 1931 г. и включва 22 ислямски държави. Щаб-квартира в Карачи (Пакистан). Реално организацията започва своята дейност през 1949 г.. http://www.motamaralalamalislami.org/

[19] Шимон Бриман, „Мусульмане в СС“, Вести, Иерусалим, 25 апреля 2002

[20] http://agentura.ru/dossier/syria/ , Посетен на 26.08.2018 г.

[21] Rainer Kriebel. Преди да замине като съветник в Сирия е използван като анализатор от американското разузнаване. https://de.wikipedia.org/wiki/Rainer_Kriebel , Посетено на 28.08.2018 г.

[22] Садам.меч востока. Глава 4. Независимый Ирак. XX век, http://saddam-mech-vostoka.narod.ru/ir7.html, Посетен на 26.08.2018 г.

[23] Сатановский, Е., „Жил-был народ… Пособие по выживанию в геноциде“, ЛитРес;2015, ISBN: 978-5-699-82416-8.

[24] Дугин А. Г. Глава 4. Малый шайтан исламо-фашизма (рецензия на статью Ф. Фукуямы «Исламо-фашизм») // Геополитика постмодерна. — М.: Амфора, 2007. — 177 с.

[25] Феофанофф Г. Исламофашизм: оскорбление или комплимент?. «Время новостей» (28 августа 2006). Проверено 19 сентября 2015. Архивировано из первоисточника 30 августа 2006.

[26] Сейид Ибрахим Кутб - египетски писател и философ, идеолог на „Мюсюлмански братя“.

[27] Феофанофф Г. Исламофашизм: оскорбление или комплимент?. «Время новостей» (28.08.2006). http://www.blagovest-info.ru/index.php?ss=2&s=7&id=8533 , Посетен на 26.08.2018 г.

[28] Николя Лебур. «Исламофашизм»: новое заблуждение французских левых. Slate.fr (18.02.2015). https://inosmi.ru/world/20150218/226350235.html , Посетен на 25.08.2018 г.

[29] Президент Буш о Ливане. Редакционный комментарий, отражающий точку зрения правительства США. Голос Америки (08.12.2006). https://web.archive.org/web/20150919110624/http://www.golos-ameriki.ru/content/a-33-2006-08-12-voa3/655559.html , Посетен на 26.08.2018 г.

[30] Феофанофф Г. Исламофашизм: оскорбление или комплимент?. «Время новостей» (28.08.2006). http://www.blagovest-info.ru/index.php?ss=2&s=7&id=8533 , Посетен на 26.08.2018 г.

[31] Pipes, D., „At War with Islamic Fascists“, FrontPageMagazine.com, August 14, 2006. Посетен на 25.08.2018 г.

[32] Колсон, Ч.“Сто миллионов мусульман во всем мире находятся под влиянием исламо-фашизма“, regions.ru, 13.06.2007. https://web.archive.org/web/20100630101935/http://i-r-p.ru/page/stream-event/index-13699.html, Посетен на 26.08.2018 г.

[33] National Review Online: Для такой характеристики радикального ислама, как «исламский фашизм», есть все основания, Голос России: Эфир дайджест, 02.10.2006, https://web.archive.org/web/20071108042155/http://i-r-p.ru/page/stream-event/index-8089.html, Посетен на 25.08.2018 г.

[34] Христов, Х., Солаков, Т., Процеси на реислямизация сред мюсюлманската общност и провеждана малцинствена политика в Република България, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 105 -114.

[35] Христов, Х., Солаков, Т., Различия между ислямски радикализъм и турски рационализъм. Причини, довели до разделението на мюфтийството, Юридически сборник на Бургаски свободен университет, Център по юридически науки, том XXV -2018, ISSN 1311-377, гр. Бургас, България, 2018 год., с. 114 - 123.

[36] Солаков, Т., Христов, Х., Мюсюлманската общност в Република България, Сборник доклади от Годишна Университетска Научна Конференция, Национален военен университет „Васил Левски”, гр. В. Търново, България, ISBN 978-619-7246-20-9 (online e-book), 14-15 Юни 2018, с. 621-630.

Име на автора: доц. д-р Милен Мирчев Иванов
Месторабота: преподавател в Академия на МВР, гр. София и Русенски университет "Ангел Кънчев"

ORGANIZATIONAL THEORY AND SECURITY IN CRISIS MANAGEMENT

NEDELCHO R. NEDELCHEV

ABSTRACT: *The term "security" in recent years has entered not only in the normative documents regulating the activities of structures such as SCIS, SANS, MoD, MI, but also in the media and public space. Considering "security" as a word explained in the interpretive dictionary and the synonymous dictionary of the Republic of Bulgaria, we get an idea of what is expected of us as specialists and of the structures we manage or construct for the protection of the population in the case of non-military crises. A number of authors define "security" as a degree of resistance or harm. Others extend the notion to the state of the system, which ensures the neutralization and counteraction of external factors that have a destructive impact on the system or organization.*

KEYWORDS: *Security, system, organization, disaster protection, organizational behavior.*

ОРГАНИЗАЦИОННА ТЕОРИЯ И СИГУРНОСТТА В УПРАВЛЕНИЕТО ПРИ КРИЗИ*

НЕДЕЛЧО Р. НЕДЕЛЧЕВ

АБСТРАКТ: *Терминът "сигурност" през последните години се вписва не само в нормативните документи, регулиращи дейността на структури като ДКСИ, ДАНС, МО, МВР, но и в медиите и общественото пространство. Като се има предвид „сигурността" като дума, обяснена в тълкувателния речник и синонимния речник на Република България, ние получаваме представа какво се очаква от нас като специалисти и структури, които управляваме или изграждаме за защита на населението в случай на невоенни кризи. Редица автори определят „сигурността" като степен на съпротива или вреда. Други разширяват понятието към състоянието на системата, което осигурява неутрализирането и противодействието на външни фактори, които имат разрушително въздействие върху системата или организацията.*

1. Въведение

Понятието „сигурност” през последните години навлезе силно не само в нормативните документи регламентиращи дейността на структури като ДКСИ, ДАНС, МО, МВР, но и в медийното и публичното пространство. Разглеждайки „сигурността”, като дума обяснена в тълковния речник и синонимния речник на Република България, добиваме представа какво се очаква от нас като специалисти и от структурите, които управляваме или изграждаме за защита на населението при кризи от невоенен характер. Редица автори определят „сигурността” като степен на съпротива или предпазване от вреда. Други разширяват понятието до състояние на дадената система, което да осигури неутрализирането и противодействието на външни фактори, които оказват деструктивно влияние на системата или организацията [8], [9], [10], [11].

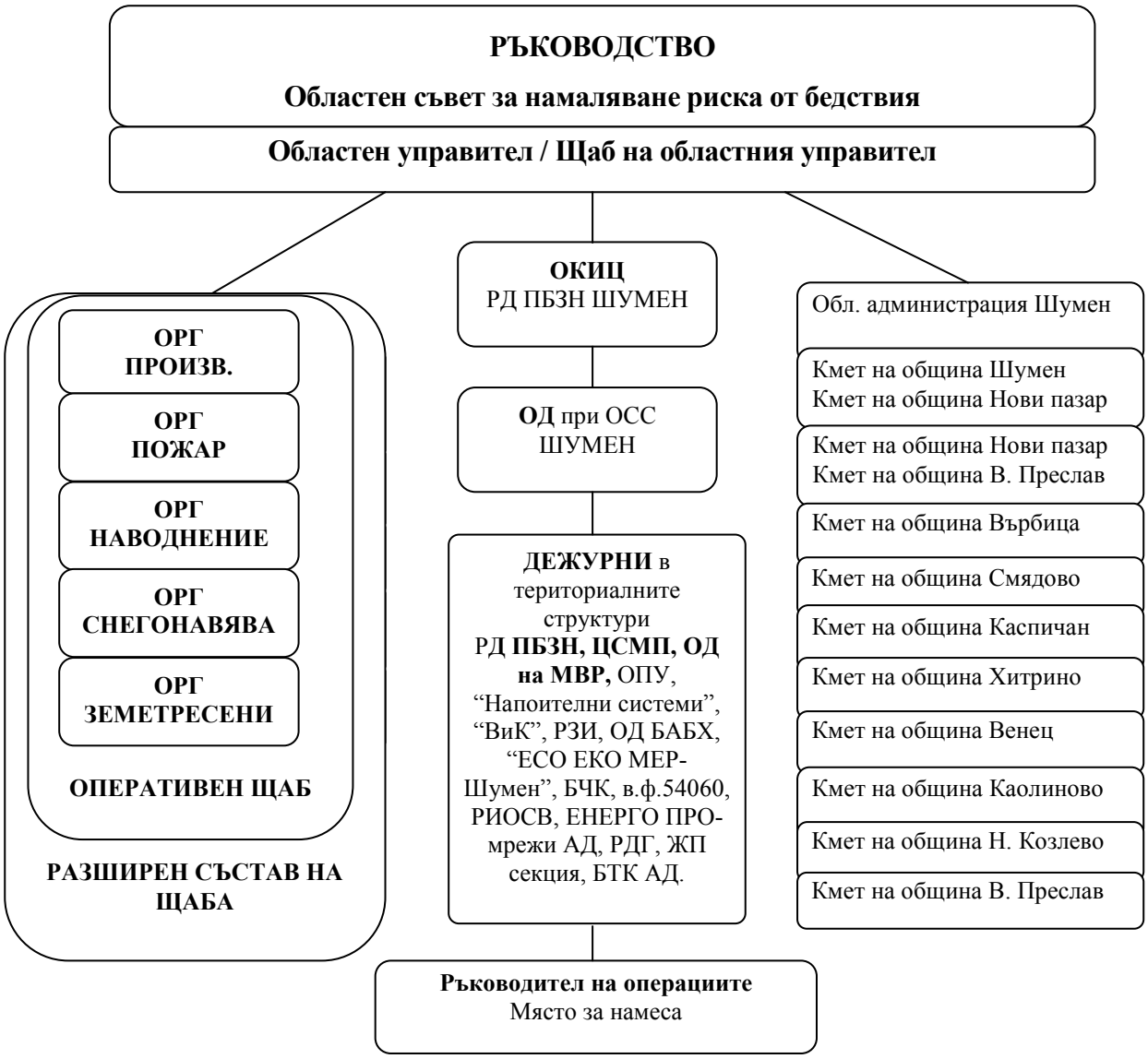
В повечето случаи споменавайки термините „национална”, „социална”, „икономическа”, „физическа сигурност“, „сигурност на отбраната“, „информационна

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

сигурност“, не си даваме сметка какво стои зад всеки един термин. Очакваме единствено звената за сигурност да си свършат професионално работата и да осигурят държавната и нашата персонална защита. Но зад думата сигурност не стои един специалист, а организирана система от специалисти, държавни и частни структури, обединени в една обща цел. Управлението при кризи от невоенен характер или както е залегнало в сега действащата нормативна уредба – защита на населението при бедствия и аварии също е сложна организационна структура [2]. Защитата при кризи от невоенен характер има два основни етапа – превантивна дейност и аварийно-спасителна дейност. И двата етапа се осигуряват от структури влизащи в Националната, Областната, Ведомствената или др. видове изградени предварително системи за защита на населението. На областно ниво това са Съветите за намаляване риска от бедствия, създадени на основание чл. 64а от Закона за защита при бедствия (ЗЗБ).

2. Модел на системата за управление при кризи от невоенен характер на областно ниво

Модел на системата за управление при кризи от невоенен характер на областно ниво е даден на фиг. 1.



Фиг. 1. Модел на системата за управление при кризи от невоенен характер в шуменска област

Измененията в ЗЗБ през 2016 г. при организацията на дейността на тази система наложиха някои съществени промени в терминологията и структурите изграждащи тази система. Въвеждането на термина „Областен съвет за намаляване риска от бедствия" реши проблема с двузначността при използването на наименованието ЩАБ. Сега ЩАБ е наименованието на ръководената от областните управители група от ръководители и/или специалисти пряко ангажирани с втория етап – аварийно-спасителната дейност.

Областните съвет за намаляване риска от бедствия е органа по превантивната дейност. За съжаление създаването на съветите по намаляване риска от бедствия ни задължиха да включим и неправителствени организации, имащи възможност да подпомогнат аварийно-спасителните дейности и представители на общинските съвети, като в по-голяма степен тези хора са неосведомени и неподготвени по темата за защитата на населението при кризи и утежняват с присъствието си и с изказванията си и без това тежката работа на тези съвети. На областно ниво членовете на тези съвети е от 38 до 45 представители на държавни институции, юридически лица и неправителствени организации. В системата за управление при кризи са включени и общините, оперативните центрове на областните администрации, регионалните дирекции на ПБЗН и щабовете на ръководителите на операции, намиращи се най-често в района на бедствието. Цялата тази система трябва да бъде много добре организирана [1], [8], [9], [10], [11].

На фигура 2 е показано взаимодействието между отделните елементи на системата за управление при кризи от невоенен характер в йерархичен ред. Поради огромния брой участници се наложи да бъде извършен анализ на работата на тази система и отделните и елементи с цел съкращаване времето за работа.

Фиг.2. Взаимодействие на елементите от системата за управление при кризи от невоенен характер

Забележка: ОЩ – оперативен състав на щаба
РЩ – разширен състав на щаба

Едно от решенията е разделянето на областния Щаб за защита на населението на отделни оперативни работни групи. Състава на тези групи е прецизиран от специалистите в тази област и приет на заседание на областния съвет за намаляване риска от бедствия. Списъчния състав на тези групи е предаден на оперативните дежурни в областната администрация. Оперативните дежурни, след като оповестят служителя по защита на населението при бедствия, оповестяват членовете на оперативните групи, без да чакат разпореждане от областния управител или служителя по защита на населението, бучена, ръководена и координирана.

Разглеждайки елементите от системата за защита на населението при кризи от невоенен характер доказахме, че тя се състои от: отделни личности със своите манталитет, теоретични познания и професионални качества; екипи на държавни институции, юридически и физически лица; различни по вид и интензитет междуличностни и междуфирмени взаимоотношения; както и възникналите в тези отношения проблеми. Тази организация наречена система за защита на населението при кризи трябва да работи като един организъм в интерес на населението. Именно поради отговорната роля, която имаме, като организатори и координатори в действията на отделните елементи на системата като цяло се налага научен подход при разглеждане създаването и функционирането на системата за защита на населението при кризи. Сигурността в управлението на системата и действията на ръководителите на отделните елементи зависи от правилния подход при изграждане на системата и регламентиране на взаимоотношенията вътре в нея. В този процес възниква необходимостта от разглеждане на Теорията на организациите, избор на концепция и внедряването и в практиката.

Преди да разгледаме основните теории за организациите трябва да изясним съдържанието на понятието “организация”. Първата преносна употреба на понятието се свързва с Аристотел, който употребява термина „организация“ при разглеждане науката логика като όργανον за правилно мислене. На старогръцки όργανον означава инструмент. В наши дни терминът “организация” има няколко значения и може да означава ред, степен на подреденост; дейност за създаване на предното; институция. Съвременният термин “организация” означава “доброволно обединение на лица, обществени групи или държави, свързани в обща програма, задачи и цели” [5].

„За да функционира организацията по определените правила и процедури в нея, е необходимо да се управляват хората и групи от други хора и групи, а не материалите, вещите и процедурите“ [4]. В своя труд „Организационно поведение” М. Паунов приема, че “организацията е подредеността на частите на система, в която поне един от елементите е новакът или съвкупността от хора (респективно дейността за създаването на въпросната подреденост)“.

От посочените определения могат да се направят следните изводи:

- Организацията е сложна система от поне два задължителни елемента: хора и правила.
- Хората са разделени поне на управляващи и ръководени, което поражда сложни взаимовръзки на интересите за постигане организационните, груповите и личните цели на членовете на организацията.
- В процеса на функционирането на организацията освен индивидуалното се проявява и организационното поведение, което е отражение на организационната култура.

Всеки прекарва живота си в някаква организация, зависи от нея и осъществява целите и интересите си в нея. Организацията има ясно обособени граници, йерархичен

статут на длъжностните позиции, социални разслоения, централна власт, многообразни отношения между хората в нея. Организацията е сложна социална система. Поради този характер и процесите, които протичат в нея, тя е обект на изследване от много науки, които могат да се разделят в три групи: инженерно-технически, занимаващи се с технологичните процеси от гледна точка на инженеринга; мениджмънт, занимаващ се с управленските процеси за организиране и управление на производствените технологии; социално-организационни науки, като организационна психология, социални организации и други, занимаващи се с изучаване на съответните проблеми в организацията [3,6].

Изследванията на редица водещи учени в областта на организационната психология, като М. Вебер, Т. Парсън, Р. Мертън, П. Блау, Д. Скот, Р. Ликерт, Г. Осипов, Н. Лапин и други, показват, че в организациите доминират преди всичко социалните отношения между членовете на социалните групи.

В живата природа има изключително разнообразие на форми на организираност. Много често този тип организации се отличават с висока степен на организираност, но за разлика от хората организационното общество на животните има характер на генетично заложени данни в индивидите, които му позволяват да изпълнява функциите си инстинктивно. Например най-силният лъв става водач на прайда и останалите му се подчиняват.

При хората е съвсем различно. Те организират живота си рационално – в съответствие с поставените цели. Тези цели отговарят на виртуалния модел за ситуацията и предстоящите за решаване задачи за постигане на целта. Обединяването на хората в групи е продиктувано от удовлетворяването на техни важни жизнени потребности. Още първобитното общество установява от практиката, че постиженията са по-добри и резултатите по значими, ако усилията са обединени и действат в групи – малки или големи. Те интуитивно усещат синергичния ефект от обединяването за изпълнение на дадена задача, при което резултатът от общите действия е по-висок от сумата от индивидуалните резултати от самостоятелните действия на всеки член.

По тази причина в практиката хората в групите започват да осъзнават необходимостта от обединяване на усилията за по-добро задоволяване на потребностите и за оцеляване на племето. За реализацията на тези потребности започват да формират социални обединения. Целият социален живот се проявява в асоциация между хора, които обединяват усилията си за постигане на различни цели. По същество социалните организации представляват връзки между хората, които отразяват техните интереси и служат за мотивиране на определени решения. Тоест социалните връзки се появяват при обединяване на хората за постигане на определени цели чрез съвместна дейност.

Постепенно социалните асоциации в най-важните дейности стават вътрешно организирани, което свидетелства за:

- Поява и развитие на общественото разделение на труда, насочено към първичното разпределение на труда, а и към разпределяне на задълженията за по-добро изпълнение на индивидуалните задължения в интерес на постигане целите на организацията по най-добрия начин.
- Поява и функциониране на вътрешен координационен орган, който осъществява съгласуваност, целенасоченост и функционално единство на действията чрез използване лостовете на властовото въздействие.
- Създаване на общо поле за работа на членовете на обединението, което цели оптимално постигане на резултата в конкретните условия.

Френският учен Файол, работещ в сферата на класическата теория на организациите, въвежда понятието „организационна структура на управлението”, като определя йерархията като процес на институционализиране на отношенията и осигуряване на прозрачност в дейността на организацията.

На база теорията на организациите можем да изберем, като основополагащи при структуриране системата за защита на населението при кризи, следните принципи на управлението:

- Единоначалие или единство на разпорежданията;
- Рационализация на схемата на контрола – определен брой подчинени на един ръководител;
- Организационна специализация – ясно и точно разделяне функциите на управление в организацията;
- Изключение – само важните и неповторимите решения в организацията трябва да се оставят в компетенциите на ръководителя.

Като доказателство, избягвайки от авторитарния начин на управление и от големи организационни единици, където принципите на управление са основополагащи в управлението на ежедневните процеси, можем да разгледаме семейството, като вид организация, една ловна дружинка или отделен производствен цех в дадена фабрика. Във всички един от тях се вижда ролята на единоначалника или човека поемащ огромна отговорност в управлението на процеси, производство, финансите и др., разграничаваме определения брой подчинени на ръководителите на отделни звена, ясните и точни разделения на функциите на отделните звена и личности.

В добрите организации единствено най-важните, неповторими и недвусмислени решения по най-критичните проблеми се взимат от ръководителя. Права по управлението и взимането на решения са дадени и на ръководителите от по-долно ниво.

Тези анализи и разсъждения следва да докажат, че организацията, разглеждана като явление, процес и дейност е състояние и същност на всяка една система в обществото. Тъй като за системата за защита на населението говорим като за една добре организирана, ръководена и действаща организация, изградена върху координираните и обединени действия и цели на отделни нейни елементи, би следвало да анализираме теорията на организациите от гледна точка на системния подход. Не е приоритет на доклада задълбочаване в представянето на теорията на организациите и системния подход в детайли. За нас е важен избора на научен подход при организирането и координирането на целия цикъл на защитата на населението при кризи от невоенен характер – превантивна дейност и аварийно-спасителни дейности.

Николай Слатински определя системното мислене и действие като единствен възможен и ефективен метод при изучаване на сигурността. Сигурността в процеса по защита на населението при кризи е гарантирана единствено при разглеждане на организацията като система на интегрирана общност от взаимосвързани елементи, ефектът от взаимодействието между които се измерва със свойства, които са синергичен резултат от свойствата на отделните елементи. Като резултат постигането на целите на отделните елементи и структури в системата неминуемо води до постигане на общата цел – ефективна защита и осигуряване на населението [7].

По-висок синергичен ефект може да се постигне чрез:

- По-съвършена организация;
- По-качествено колективно усили на членовете на организацията – като равнище на научен, интелектуален и морален потенциал;

- По-добра координация и синхронизация на усилията в организацията.

3. Заключение

След направеният съществен анализ на системата за защита на населението при кризи, пречупен през призмата на теорията на организациите в контекста на системния подход, можем да направим следните изводи:

- Научния подход при създаване и функциониране на всяка организация води до трайно добри резултати.
- Защитата на населението при кризи от невоенен характер е организирана но сложна система изградена от вътрешни подсистеми, подложени на разнопосочни и непредвидими външни въздействия.
- Постигането на главната цел на организацията е синергичен резултат от постигането на целите на отделните елементи в организацията.

ЛИТЕРАТУРА:

[1] Диманова, Д., Защита при бедствия, аварии и катастрофи. УИ Епископ Константин Преславски, Шумен (2016).

[2] Досев, Н., Национална сигурност и устойчиво развитие - Научна конференция „40 години Шуменски университет 1971-2011”, Сборник Научни трудове, Шумен (2011).

[3] Манев, Е., Организационна култура - същност, промяна, измерване, София (2007).

[4] Паунов, М., Организационно поведение. София (1998).

[5] Речник на чуждите думи в българския език, София (2003).

[6] Семерджиев, Ц., Стратегическо ръководство. Лидерство, София (2000).

[7] Слатински, Н., Национална сигурност – аспекти, анализи, алтернативи, София (2004).

[8] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[9] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[10] Христов, А., Андреев, А., Оптимизиране дейността на структурите за бърза реакция при кризи, чрез използване на екипи по TASK-FORCE принцип. Научна конференция с международно участие „MATTEX“, ШУ „Еп. К. Преславски“ 11-13ноември 2016 г., ISSN: 1314-3921, т. 2, 2016, стр. 72-76.

[11] Христов, А., Андреев, А., Компютърно симулирани учения КСУ с използване на геоинформационен модел за симулиране на наводнения. Научна конференция с международно участие „MATTEX“, ШУ „Еп. К. Преславски“ 11-13ноември 2016 г., ISSN: 1314-3921, т. 2, 2016, стр. 65-71.

Име на автора: д-р Неделчо Русанов Неделчев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, Катедра „Управление на системите за сигурност“
E-mail: jo_nn@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 213 - 221 Problems of Security Systems

CONFLICTS IN THE ORGANIZATION AND THEIR MANAGEMENT

NELI G. BORISOVA

ABSTRACT: *The modern approach regards conflict as an inevitable consequence of the daily life of the organization, caused above all by the internal complexity of the system. Through various mechanisms (eg, problem-solving approaches), resolving a conflict can lead to positive changes in the organization, i.e. not the conflict leads to the destruction of the relationship in the organization, and the failure to constructively deal with it.*

KEYWORDS: *Conflict, organization, management.*

КОНФЛИКТИ В ОРГАНИЗАЦИЯТА И ТЯХНОТО УПРАВЛЕНИЕ[1]

НЕЛИ Г. БОРИСОВА

АБСТРАКТ: *Конфликтът присъства постоянно в груповия живот. Разбирането, че конфликтът е вреден за организацията, че е синоним на насилие, ирационалност, че е нещо което трябва да се избягва, вече е преодоляно. Днес все повече се приема интеракционисткия възглед (Стивън Робинс), че конфликтът може да бъде както вреден, така и понякога може да бъде полезен и трябва да се стимулира.*

1. Въведение

Конфликтът присъства постоянно в груповия живот. Разбирането, че конфликтът е вреден за организацията, че е синоним на насилие, ирационалност, че е нещо което трябва да се избягва, вече е преодоляно. Днес все повече се приема интеракционисткия възглед (Стивън Робинс), че конфликтът може да бъде както вреден, така и понякога може да бъде полезен и трябва да се стимулира.

Съвременният подход разглежда конфликта като неизбежно следствие от ежедневието на организацията, причинен преди всичко от вътрешната сложност на системата. Посредством различни механизми (напр. подходите за разрешаване на проблеми), разрешаването на един конфликт може да доведе до положителни промени в организацията, т. е. не конфликтът води до разрушаване на взаимоотношенията в организацията, а неуспехът в конструктивното справяне с него.

2. Изложение

Конфликтът е напрегната емоционална ситуация или „война“ (студена или топла), обявена между лица или група от лица, които си оспорват влияние, власт или интереси върху нещо, което до известна степен изглежда неделимо и чието притежание субективно им се струва много важно. Във всеки конфликт има: няколко страни, които се стремят да придобият нещо, което изглежда неделимо, а желанието да го получат води страните до обтягане на отношенията, скъсване или до агресии.

Предпоставки за конфликта

[1] Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Има различни ситуации, които обикновено са предпоставки за възникване на конфликт. Най-често срещаните между тях са:

• Несъвместими личности или ценностни системи;
• Препокриващи се или неясни принципи на работа;
• Конкуренция за ограничени ресурси;
• Неадекватна комуникация;
• Взаимозависими задачи;
• Организационна сложност;
• Неразумни или неясни политики, стандарти или правила;
• Неразумни крайни срокове или изключителен времеви натиск;
• Колективно вземане на решения (колкото повече хора участват, толкова по-голям е потенциалът за конфликт);
• Взимане на решения с консенсус;
• Нереализирани очаквания;
• Нерешени или потиснати конфликти.

Добрият ръководител разчита навреме тези ситуации, като предупреждение за възможен конфликт и взема необходимите мерки. За да се вземат такива мерки обаче, е необходимо да се познава начинът, по който протичат конфликтите. От значение е как се поражда конфликта. Обикновено той се може да се основава на:

- Действителни факти: по-тясно разпределение на задачата, липса на участие, подценяване и др.;
- На погрешни впечатления или на преиначена информация.

Фази на конфликта:

Един от популярните модели на конфликта като процес включва пет основни етапа, които илюстрират разгръщането му във времето.

1) Латентен конфликт - конфликтът започва още когато условията за него се появяват (изразени различия между индивидите или групите), още преди да има явен, открит сблъсък.

2) Възприеманият конфликт е етапът, на който индивидите и групите вече знаят, че има конфликт.

3) Почувстваният конфликт е етап, който следва с известно забавяне във времето между интелектуалното му възприемане и емоционалното му преживяване.

4) Явният конфликт е наблюдаемото поведение, предназначено да попречи на опитите на другите да преследват своите цели и е най-откритата форма на конфликт, която може да се прояви като открита агресия или като оттегляне на подкрепата за някого.

5) Последиците от конфликта след неговия край водят до възникването на нова реалност.

Според други автори конфликтът като процес има четири етапа:

1) Потенциална опозиция - налице са условията, които създават възможността да възникне конфликт. Те не водят директно към конфликт, но едно от тях е достатъчно, за да възникването му. Тези условия, които могат да се разглеждат като причини или източници на конфликта, могат да бъдат обединени в три категории: комуникация, структура и личностни характеристики.

Комуникацията води до конфликт, когато съществуват семантични трудности (трудности на разбирането), недоразумения и „шум“ в комуникационните канали. Във връзка с комуникацията изследователите са стигнали до един изненадващ извод – потенциалът за конфликт расте, когато има твърде малко или твърде много комуникация.

Прекалено многото информация, както и недостатъчната информация могат да залегнат в основата на даден конфликт.

Структурата включва такива променливи като размера на групата, степента на специализацията в задачите, възложени на членовете на групата, юридическата яснота, съвместимостта на целите на отделните членове, стилът на лидерството, системата на възнагражденията и степента на зависимост между групите. Голямото разнообразие в тези елементи може да доведе до конфликт както поради тях, така и вътре в тях и между тях.

Личностните характеристики - равнището на самоуважение, степента на авторитарност, ценностната система и др. са фактори, които ако действат в различни или в противоположни посоки, създават условия за конфликт.

2) Познание и персонализация. Когато условията на първия етап предизвикват недоволство, потенциалът за противопоставяне се актуализира на втория етап. Тези условия могат да доведат до конфликт само ако една или повече от страните в евентуалния конфликт, първо, са наясно със съществуването му (възприемат го, знаят за него) и второ, чувстват се лично засегнати от него (чувстват го).

3) Поведение. На този етап даден член или членове на групата се ангажират с поведение, което има за цел да попречи на друг член или членове да постигнат целите си и да задоволят своите интереси. Това вече е открит конфликт и на този етап страните в него започват да прилагат различни средства за разрешаването му.

В това отношение действията им следват шест основни ориентации:

• Съперничество - усилия да се постигне дадена цел без оглед на въздействието върху другите;

• Сътрудничество - ситуация, при която страните в конфликта се стремят към взаимно приемлив изход, задоволяващ всички;

• Избягване - отдръпване от конфликта или потискане на конфликта поради нежелание да се участва в него или поради взаимната зависимост на членовете на групата при изпълнението на нейните задачи;

• Приспособяване - едната страна демонстрира желание да сътрудничи за задоволяване на интересите на другата, поставя ги пред своите. Това поведение цели едновременно да успокои нещата и да задължи по определен начин другата страна;

• Компромис - всяка от страните се отказва от нещо, така че в тази ситуация да няма печелещи и губещи. Подход, при който и вземаш, и даваш;

• Принуждаване (доминация) - едната страна се опитва да задоволи само собствените си интереси, без да е склонна да се съобразява с интересите на другата дори в минимална степен.

4) Изход - последици от конфликта

Симптомите на конфликта

Конфликтите са свързани обикновено със силни чувства и емоции (яд, гняв, уплаха, облекчение, удовлетворение). Преобладаването на емоциите в конфликтна ситуация затруднява адекватното разрешаване на проблема, предизвикал сблъсъка. Конфликтът води, както до външни (във взаимоотношенията), така и до вътрешни промени (вегетативни, психични, соматични, които са взаимосвързани така, че външните са израз на вътрешните, а вътрешните предизвикват външните.

А) Външни промени:

• в обичайната честота на взаимните контакти, на размяната на реплики;

• грубо аргументиране „на висок тон“;

• в тематиката на разговорите;

• пряка или непряка атака на идеите или фактите на другите;
• неотстъпчивост и твърдост в отстояване на позицията;
• в обичайния емоционален тон на взаимоотношенията, поява на емоционално напрежение у участниците;
• нетърпеливост и слабо взаимно съгласие;
• взаимни обвинения;
• ниска продуктивност
• в начините на извънслужебно общуване;
• в приятелския кръг;
• прекомерна раздразнителност или прекомерна мнителност.

Б) Вътрешни промени:

• вегетативни: промяна на пулс, кръвно налягане, дишане, сърдечна дейност, изпотяване, изчервяване, пребледняване, треперене;

• експресивни: промяна в интонацията на говора, промяна на силата на говора, повишаване на глас, по-бързо говорене, треперене на гласа, промяна на дистанцията между участниците, избягване на физически допир, промяна на позата на участниците, промяна в интензивността на жестикулацията, барабанене с пръсти, свиване на юмруци, намръщване, гримасничене, подкосяване на краката и др.;

• промени в психичните процеси и състояния: промяна на настроението, силни и бурно протичащи емоционални преживявания (страх, злоба, ужас, гняв, ярост, агресивност, отчаяние и др.), намален самоконтрол, намалени нормални прагове на усещания, нарушения в обема на вниманието, нарушения във възприятните възможности на човека, в мисловната дейност и способностите за волеви усилия, промяна в мотивацията за труд, разклащане или срив на ценностната система и др.

• соматични проблеми: болки в стомаха, сърдечната област, главоболие и др.

Последствия от конфликтите

Последиците от конфликта, както вече казахме, могат да бъдат положителни (функционални) или отрицателни (дисфункционални).

Функционалните конфликти са конструктивни, те подобряват качеството на решенията, стимулират креативността и иновацията, разкриват източниците за решаване на проблемите в групата. Те са своеобразен „антидот“ на закостенялото групово мислене и на конформизма. Конфликтът е предизвикателство към статуквото и тласка към нови идеи и решения, свързани с груповите цели и дейности. Изследванията показват също, че конфликтът може да има положително влияние върху производителността на групата.

Дисфункционалните конфликти са деструктивни. Те предизвикват неконтролирано противопоставяне в групата, пораждат общо недоволство, разкъсват връзката между нейните членове, като може да доведат и до разпадането и. Във всички случаи, когато конфликтът не се управлява, той води до намаляване на груповата ефективност, на сцеплението и сътрудничеството в групата и заплашва нейното оцеляване.

Ефектът от конфликта трудно може да се предскаже. Тук е необходимо да се имат предвид две хипотези. Според първата екстремните равнища на конфликт, съпроводени с открита борба или насилие, рядко са функционални. Функционалният конфликт в повечето случаи се характеризира с умерени равнища на не толкова открито и контролирано противопоставяне. Втората хипотеза е свързана с характера на работата, която извършва групата. Според нея колкото по-творчески или непрограмирани са процесите на вземане на решения и задачите на групата, толкова е по-голяма вероятността вътрешният конфликт да е конструктивен. Групите, които решават проблеми, изискващи

нови и новаторски подходи, са по-облагодетелствани от конфликта, отколкото групите, изпълняващи твърдо програмирани, рутинни действия.

Видове конфликти

Основание за типология на конфликтите са: целите на участниците в конфликта; съответствието на техните действия на установените норми; крайният резултат на конфликтното взаимодействие и влиянието на конфликта на развитието на организацията.

В зависимост от характера на конфликта се обуславят следните типове конфликти в организацията:

1) Конструктивни (функционални) - конфликти спомагат за повишаването на стабилността на функциониране на организацията в новите условия на променящата се външна среда за сметка на преустройство на нейните функции и структури и установяване на нови връзки.

2) Стабилизиращи - конфликти са насочени към отстраняване отклонението от нормите и затвърждаване на установените норми.

3) Деструктивни (дисфункционални) - конфликти спомагат за разрушаване на установените норми и възвръщане на стари норми или задълбочаване на проблемната ситуация. Участниците в деструктивните конфликти хабят своята енергия за да се контролират един друг или да оказват един на друг противодействие.

Съществуват също така деструктивно-ситуативни конфликти (техните участници се стремят към лична изгода) и деструктивно-тотални конфликти (участниците им се стремят към престиж или власт). И в двата случая стремежите на участниците противоречат на общите интереси на групата или организацията, доколкото те достигат своите цели със средства не одобрявани от другите, от обществото.

Друг подход това е разделянето на конфликтите на делови и емоционални. Всеки конфликт е съпроводен с емоции, а също така в организациите хората много рядко влизат в конфликт само затова, че не се харесват един друг. Най-често те се намират в ситуация, която предизвиква сблъсък.

Друга много популярна класификация дели конфликтите на вътрешно личностни (противоречие между „искам - не искам“, „мога - не мога“ и „трябва“ в различни съчетания) и социални.

По своята сила (интензивност, тежест) и влияние (значение) конфликтите могат да бъдат леки и тежки (силни), незначителни и значителни. По своята посока (съобразно структурата на организацията) могат да се окажат вертикални (между представители на различни йерархични нива - напр. конфликт между ръководителя и някой от неговата група или между групата и началника) и хоризонтални (на едно и също ниво - напр. конфликт между двама служители, или между две подгрупи, или работни екипи (обща цел); конфликт между две групи или работни екипи, които имат различни основни цели, но и двата екипа трябва да работят за една и съща обща цел (на организацията).

Могат да се опишат още редица конфликти: ситуативни и структурни; психични; невротични; политически; военни (въоръжени); международни; етнически; междуфирмени; междуведомствени; между отделни групировки; трудово-правни; семейни и др.

В нито един от тези случаи не се препоръчва забраната. Страните трябва да се „нападнат и да излеят яда си“. „Скритите“ конфликти са като не доизлекуваните рани, Впоследствие се появяват отново и с по-пълна сила. „Времето не лекува всичко“, а влошава още повече нещата.

Конфликт в организационната среда

Както посочихме по-горе конфликтът възниква, развива се и се решава на три равнища: индивидуално, вътрешногрупово и междугрупово. Всяка работна група или екип, рано или късно се озовава в конфликтна ситуация. Начинът, по който протича конфликта е най-добрият тест да се докаже дали едно работно звено наистина е сплотен екип, или не. Истинският екип се характеризира с решително и открито желание от страна на всичките му членове да разрешат конфликтното взаимоотношение.

Методи за управление на междугруповите отношения.

1. Координационни - всички те по същество са методи на координация, основната им цел е да предотвратяват търканията и конфликтите. Най-често използваните между тях са:

Правила и процедури - най-лесният и най-малко коствщия метод е предварителното установяване на система от формализирани правила и процедури, които определят точно как членовете на групите трябва да си взаимодействат.

Йерархия - ако правилата и процедурите са неадекватни, използването на организационната йерархия става водещият метод за управление на междугруповите процеси.

Планиране - то улеснява координацията. Определят се специфичните цели, за които е отговорна всяка група, така че всеки да знае какво трябва да прави. Междугруповите задачи, които създават проблеми, се решават на основата на целите и приносите на всяка група.

Определяне на специална роля за връзка на дадени индивиди, които да улесняват комуникациите между взаимозависимите единици.

Целеви групи - създаване на временни групи за решаване на даден проблем, след което участниците в тях се връщат към обичайните си задължения.

Екипи - когато задачите стават по-сложни и започват да възникват допълнително нови задачи в процеса на тяхното изпълнение, се създават постоянни екипи за решаване на възникващите проблеми.

Обединяване на подразделенията в организацията - когато междугруповите отношения станат твърде сложни, и горните методи стават недостатъчни.

Определеността на задачите. Този фактор отразява различията между силно рутинизираните и високо разнообразните дейности на различните групи. Колкото по-голяма е неопределеността на дадена задача, толкова по-нестандартно е изпълнението и обратно.

Ориентацията към времето и целите. Възприятието на дадени групи за това, кое е важно, може да се разглежда на основата на времевата рамка на тяхната работа и тяхната целева ориентация. Това пък може да затрудни съвместната работа на различните групи. Например групите, заети в непосредственото производство, имат краткосрочен поглед върху работата, докато заетите с изследователска и развойна дейност гледат подалеч във времето.

Тези методи се прилагат и развиват с оглед повишаването на ефикасността на междугруповите взаимодействия, оценявани от гледна точка на организационната ефективност (трансформирането на междугруповите конфликти в съгласувани действия) и качеството (степента, в която получените резултати се проявяват в добре дефинирано и трайно съгласие благодарение на което методите за координиране улесняват взаимодействието и редуцират дисфункционалния конфликт).

Регулирането на междугруповите взаимодействия и контролът върху междугруповите конфликти оказват същото положително влияние по отношение на

изпълнението на задачите и удовлетвореността от работата, както и на индивидуално равнище.

2.Управление на междугруповите конфликти

При конфликти достигнали стадии на дисфункционалност по отношение на дейността на организацията, успешно се използват следните методи на управление:

Конфронтационен - организиране на директни срещи на представители на конфликтуващите групи;

Поставяне на суперординарни цели - общи цели и перспективи за конфликтуващите групи;

Повишаване обема на достъпните ресурси - опит да се увеличат недостатъчните ресурси (пари, производствена територия, оборудване и др);

Бягство от конфликта (излизане) като временна мярка за изход;

Изглаждане - търсене на общи интереси на всички конфликтуващи групи, изглаждане на противоречията и различията помежду им;

Компромис - постигане на решения не идеални за страните, но позволяващи да се избегне появата на победители и победени;

Авторитарно ръководство - ръководството решава конфликтната ситуация по свое усмотрение и свежда своето решение до групите, които са в конфликт;

Замяна на човешкия фактор - изменение на поведението на членовете на групите;

Замяна на структурните фактори - изменение на формалната структура на организацията (прехвърляне, замяна, преместване на членовете на конфликтуващите групи);

Идентификация на „общия враг“ - временно разрешение на противоречията и обединение срещу „общия враг“ (например конкурента);

Преговори - конфликтуващите групи сядат на масите за преговори с цел търсене и постигане на взаимоприемливо споразумение; в резултат на успешните преговори всички участници изпитват чувството, че победители са те.

Пет стъпки за успешно преодоляване на конфликтите

Като„ръководител“ (шеф), който трябва да вземе мерки срещу всякакви конфликти в неговия отдел, долуописаните начини могат да ви помогнат да приемете конфликтите по положителен начин. Сега ще ги изброим стъпка по стъпка:

Първа стъпка: Поемете отговорността за решаването на конфликта.

Поемането на инициативата за намеса в ситуация, в която има конфликт има големи шансове да подобри положението и да промени онова, което преди е било считано за невъзможно.

Невъзможно е да го направите, ако не вземете решение да поемете отговорност за решаването.

Втора стъпка: Открийте, дефинирайте и обсъдете реалния проблем.

Функцията ви в тази връзка не се състои в прилагането на решение, а в откриването и точното определяне на проблема. След като сте го дефинирали, установете правилата на играта и обсъдете проблема със заинтересованите лица. Не потискайте изблика на емоции. Оставете всичко да се излее навън.

Да изразиш емоциите си не означава, че съвещанието трябва да заприлича на женски пазар. Има начини да се води открит разговор, който да е продуктивен и да излиза извън контрол. Трябва само да определите правилата на играта.

Всички ще са откровени и честни.

Всички ще чакат реда си и ще бъдат изслушани.

Всички ще изслушат другите,без да спорят или да проявят някоя отрицателна реакция.

Мненията и чувствата трябва да се основават на факти или примери за специфично поведение.

Трета стъпка: Питай и изслушвай!

Основни правила, които трябва да познавате са, свързани с това как да задавате въпроси и да изслушвате отговорите като истински професионалист.

Как да се задават подходящи въпроси?

Задавайте открити въпроси, които да подтикват към размисъл и подробно изложение в отговорите.

Подбирайте внимателно думите си, така че да представляват отражение на отговора, който очаквате.

Продължавайте да задавате сондиращи въпроси, ако някой от първоначалните въпроси не ви дава желаната информация.

Правила за изслушване с успех:

Изслушвайте обективно и внимателно.

Успокойте събеседника, че ви интересува каква е неговата представа за ситуацията.

Покажете положително участие в разговора, като повтаряте отговорите, които сте получили и задавате въпроси, основаващи се на новата информация.

Когато се показва на хората, че ги слушат активно и обективно, може да станат прекрасни неща. Положителното ви отношение ще им покаже, че разбирате проблемите им и сте солидарен с тях. А когато това стане, ще видите, че както те, така и вие започвате да поемате отговорност за решението на съответния проблем.

Четвърта стъпка: Поставяне на цели и създаване на план за действие.

Когато се поставят цели и се създава план за действие е важно те да се направят съвместно с останалите заинтересовани лица с цел постигането на всеобщо съгласие и да се гарантира пълното им разбиране.

Накрая, не позволявайте съвещанието да приключи, преди да сте се убедили, че онова, което сте искали да кажете е дало положителен резултат. Попитайте дали всички са съгласни с очертания проблем. Поискайте искреното съгласие на всички. А ако чувствате, че не всички са съгласни, продължете дискусията.

Пета стъпка: Продължение.

Настъпил е моментът да се създаде план за действие, за да се гарантира, че първоначалният конфликт няма отново да се появи. За тази цел трябва да определите дата и час на следващо съвещание с цел да сте сигурен, че всички имат предвид какъв ангажимент са поели.

Отговорността, решителността и искреността, които проявявате по време на процеса на решаване на конфликта ще ви възнаградят с по-добро общуване, по-висок морал и по-голяма производителност.

3. Заключение

Настоящото проучване е продиктувано от необходимостта за създаване на правила за управление на възникналите конфликти предвид сложната житейска ситуация пред която е изправен всеки един член на организацията.

ЛИТЕРАТУРА:

[1] Паунов М., Организационно поведение. С, 1997.

[2] Вълчев Р., Практически системи за решаване на конфликти, С, 1994.

[3] Христов Х., Подходи свързани с изследване сигурността на организацията - фирмата. Annual of Konstantin Preslavsky University of Shumen, Faculty of technical sciences, Univeristetско издателство - "Епископ Константин Преславски", ISSN 1311-834X, vol. V E, 2015, стр. 126-136.

[4] Христов Х., Система за вътрешен контрол в организациите от публичния сектор. Научна конференция с международно участие „Право и интернет" на Бургаски Свободен Университет -2016г., Юридически сборник том XXIII 2016, ISSN 1311-3771.

Име на автора: докторант Нели Г. Борисова
Месторабота: Шуменски университет „Епископ Константин Преславски", Факултет по технически науки, катедра „Управление на системите за сигурност"
E-mail: neli_borisova@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 222 - 230 Problems of Security Systems

GOOD PRACTICES IN THE EDUCATION OF FEMALE MILITARY PERSONNEL IN THE EUROPEAN MILITARY ACADEMIES

NEVENA TSV. ATANASOVA – KRASTEVA

ABSTRACT: *The presence of male and female cadets in the military academies and universities is considered as a necessary condition and guarantee for the national security of any European country. In this respect, over the last 15 years, effective mechanisms have been constantly sought to increase the motivation of young women to be involved in different professional spheres. The report presents and analyzes different practices in the recruitment, training and professional development processes of female cadets in the Armed Forces of some countries of the European Union.*

KEYWORDS: *Female cadets, military education, motivation.*

ДОБРИ ПРАКТИКИ ПРИ ОБУЧЕНИЕТО НА ЖЕНИ - ВОЕННОСЛУЖЕЩИ В ЕВРОПЕЙСКИТЕ ВОЕННИ АКАДЕМИИ

НЕВЕНА ЦВ. АТАНАСОВА – КРЪСТЕВА

АБСТРАКТ: *Човешкият фактор, въпреки съвременния технологичен напредък и научен прогрес, продължава да бъде гарант за успеха и престижа на всяка организация. Мотивирани, добре обучени и подготвени специалисти, компетентни служители биха допринесли за ефективността на дейността във всяка институция.*

1. Въведение

Човешкият фактор, въпреки съвременния технологичен напредък и научен прогрес, продължава да бъде гарант за успеха и престижа на всяка организация. Мотивирани, добре обучени и подготвени специалисти, компетентни служители биха допринесли за ефективността на дейността във всяка институция. Имплементирането на подобни очаквания в областта на сигурността и отбраната предполага постоянен анализ на състоянието на подготовката и служителите в конкретната социална среда, както и актуализиране на всички образователни ресурси, с цел поддържане на високо квалифицирани експерти – военни и цивилни лица.

Не случайно в „Програма за развитие на отбранителните способности на Въоръжените сили на Република България 2020“ се посочва, че „ Хората са основният потенциал и гаранция за успеха на всяка дейност в отбраната. Въоръжените сили се комплектуват с подготвен и мотивиран личен състав, чрез съвременни подходи, ясни правила и механизми за управление на човешкия ресурс.“ [1]

В съвременната среда на сигурност се наблюдават неблагоприятни тенденции както за задълбочаване на съществуващи конфликти, така и за появата на нови кризи, които имат влияние не само върху националната сигурност, но и върху международната стабилност. Тези процеси провокират на свой ред постоянно развитие на отбранителните способности на всяка страна и усъвършенстване на военно-образователната система.

На редица форуми – обществени и научни се дискутират съвременните показатели на образователните продукти, предлагани в европейските военни академии и университети. Идеята за интернационалността на военното обучение, за мобилността на курсанти и офицери, създаването на общи модули на обучение, признати във всички висши военни

учебни заведения, са доказателство за гъвкавото отношение на военните министерства и институти към съвременните предизвикателства пред армиите на страните -членки на ЕС и НАТО. Едновременно с това участието на жени -военнослужещи във Въоръжените сили на различни позиции е засилваща се тенденция, показателна за демократичните процеси във всяко общество.

2. Изложение

На годишната конференция на Комитета на НАТО по равнопоставеността на половете през 2018 г. заместник-председателят на Военния комитет на НАТО, генерал-лейтенант Стивън Шепро посочи, че "Срещи като тази, с представители на националните представители, НАТО и други международни организации, които се занимават с въпроси, експерти, академични среди и гражданското общество, осигуряват необходимия форум за измерване на постигнатия напредък в интегрирането на перспективите за равенство между половете в ежедневната работа. Защитата и овластяването на жените трябва да бъде общо усилие и не трябва да се пренебрегва, защото разнообразието от квалификации и ресурси е първостепенно, за да се гарантира постигането и запазването на мира и сигурността". [2]

Като едни от най-важните фактори, свързани с участието и обучението на жени във военните академии, са не само образователните планове и програми за различните специалности, но и по какъв начин се рекламира професията на офицер и се привличат жени и мъже – кандидати за професионална реализация и кариера. Целта на настоящия доклад е да анализира практиките, прилагани от различни европейски военни академии при набиране на желаещи жени и мъже, кандидати за курсанти и какви национални особености имат отношение към този процес.

В България висшите военни училища и академии организират рекламната си кампания и прием на курсанти и слушатели съгласно ежегодната наредба на Министъра на отбраната за условията и реда за приемане във висшите военни училища, която дава възможност за предварително планиране и провеждане на редица мероприятия. Постоянно се търсят нови начини за рекламиране на военната професия сред младото поколение и мотивиране му да кандидатства за обучение във военните училища. Този процес през последните 10 години се превърна в постоянна дейност, тъй като конкуренцията с останалите цивилни висши учебни заведения е много голяма. В редица университети се приемат студенти само с оценки от дипломата за средно образование или от зрелостните изпити като балообразуващи оценки. На този фон да се привлекат млади хора да участват в няколко кандидат-курсантски изпити, за да се достигне до приемането им за курсанти, се явява сериозно предизвикателство пред всички, ангажирани с този процес.

Когато се анализират кандидат - курсантски кампании във всички европейски академии винаги се подхожда към разглеждането на няколко елемента, които имат отношение впоследствие към решенията за похватите за привличане на жените и мъжете за военна служба. Как се набират кандидати, как получават военното си образование и как се справят с разнообразните изисквания във войсковия живот, как се реализират след завършването си като офицери в армейските редици са все въпроси, чиито отговори имат общи корени във всички страни и едновременно с това и национална специфика.

В българските висши военни училища се прилагат разнообразни прийоми за предлагане на висшето военно образование като атрактивен и перспективен избор. Разработват се съвременни рекламни материали, провеждат се разяснителни кампании по военните окръжия, активно се присъства и участва на всички кандидат-студентски борси. В последните 5 години след решение на Министерството на отбраната се завърна една

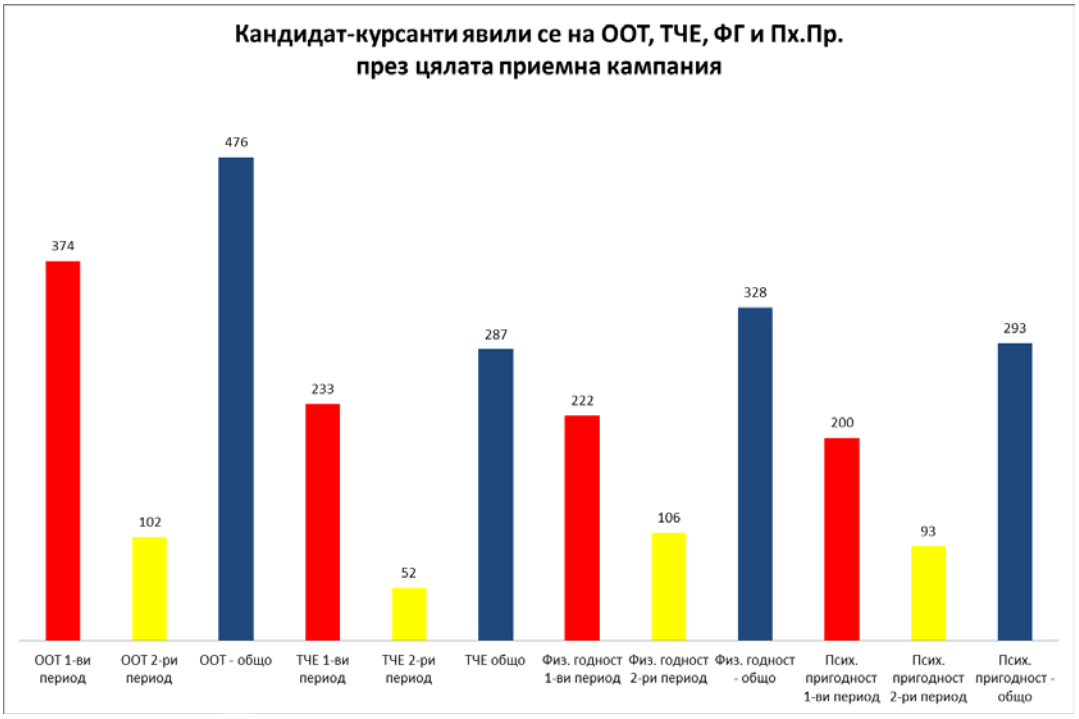
позабравена идея от близкото минало – включване на началното военно обучение в средните училища. Бе създадена специална програма за представяне в различни занятия на военната тематика пред учениците от горните класове във всички средни училища. Провокиране на интереса и осигуряване на разнообразна информация, свързани с военната история, традиции и постижения бяха едни от целите на занятията с 16-17 годишните младежи и девойки. Именно тази целева група – на съвременното интернет поколение, ползващо основно мобилни технологии, непознаващо същността на наборната военна служба, бе осигурена с подготвени офицери – преподаватели, които в определени часове предлагаха непозната информация и даваха добър пример. Въпреки че, се наблюдаваше и неприемане на тези часове в някои специализирани училища или липса на особен интерес или ентусиазъм по време на тези занятия, това е добра практика, насочени към родолюбивото възпитание на младите хора и формиране на техните ценности.

Друга практика, която е различна с другите европейски академии, както ще бъде посочено по-долу, е организирането и провеждането на т.нар. „ранни и изнесени“ изпити. Организирането на изпити още по време на учебната година, преди завършването на средното образование в средните училища, дава възможност на кандидатите да проверят своите знания и да се явят на някои изпити, които са коренно различни от всички останали университети. Така например – изпит по физическа подготовка, проверка на психичната пригодност за военна служба и медицинските прегледи са специфични за приемане във военните училища и не винаги кандидатите имат готовност и ясна представа за тяхната същност. Едновременно с това при положителни резултати, това осигурява една гаранция за бъдещото им приемане за курсант. В същото време провеждането на такива изпити и в други големи градове на България, извън града, в който е локацията на Военния университет, създава удобство за потенциалните кандидати и минимизиране на финансовите разходи за участие в кандидат-курсантската кампания. При анализа на резултатите от подобни решения в кампанията по прием на курсанти през 2018 г., представен на фигура 1, се наблюдава значително по-високия брой кандидати, участвали в предварителния прием през месеците февруари – април в сравнение с кандидатите, явили се след завършване на средното образование по време на редовната изпитна кампания през месец юли 2018 г.

Цифрите са достатъчно показателни за удачността на такова решение и за предпочитанията на младия българин да участва в предварителни изпити, с цел проверка на готовността за кандидатстване във ВУЗ, което се приема и като вариант при неблагоприятни резултати, да се насочи подготовката към повишаване на успеваемостта при редовното явяване на кандидат-курсантските изпити.

Интересно е да се отбележи, във връзка с предмета на настоящия доклад, че в нашата страна не се наблюдават затруднения при набирането на кандидати – жени за обучение във военните училища. Тъй като курсантите - жени в българското военно образование имат повече от 25-годишна история, а след 2002 г. много длъжности в Българската армия са заети и успешно се изпълняват от жени.

В таблица 1 са представени данните относно кандидатите – мъже и жени за Военния университет през последните две години. Наблюдава се стабилна тенденция на желанието на млади жени да получат висше военно образование, които представляват около 1/5 от всички кандидати или приблизително 20 %.



Фиг. 1. Кандидат-курсанти през 2018 г., явили се на Общообразователен тест (ООТ), тест по чужд език (ТЧЕ), физическа годност (ФГ) и психична пригодност (Пх.Пр.) през първи период (ранни и изнесени изпити) и втори период (редовна кампания)

Таблица 1. Брой на кандидатите за курсанти през 2017 и 2018 година по пол

НВУ „Васил Левски“ - Специалност	ОБЩО	Мъже	Жени
Кандидати за военна специалност през 2017 г.	509	409	100
Кандидати за военна специалност през 2018 г.	438	378	60

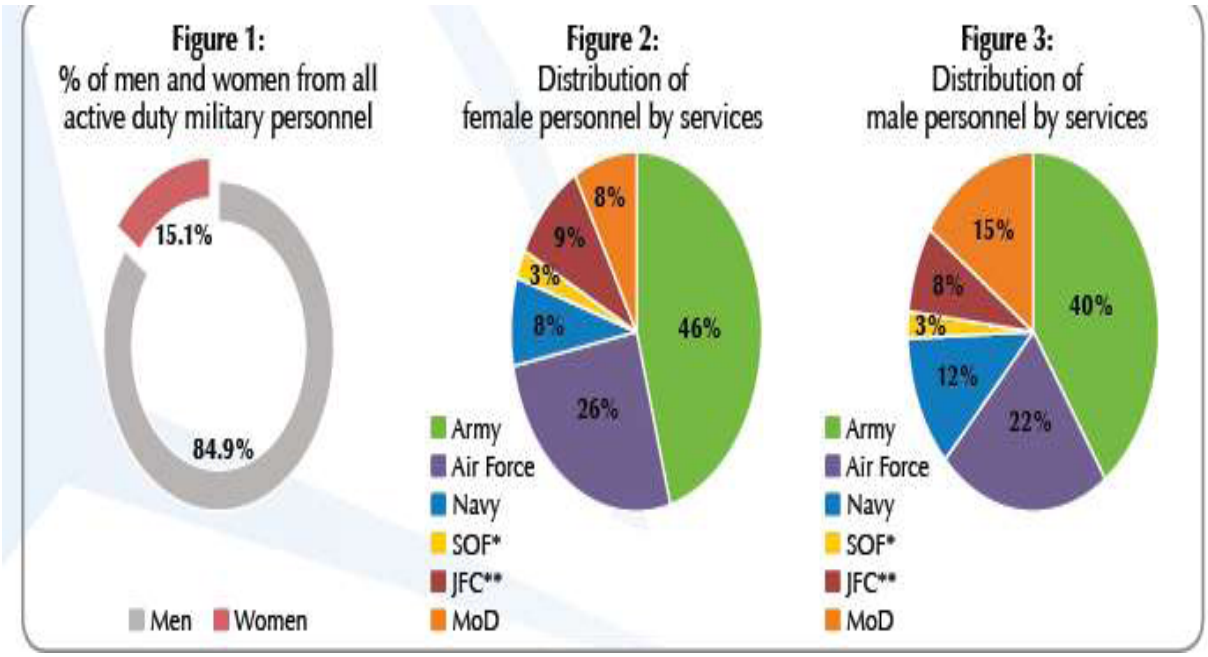
Аналогични са и данните на приетите за обучение във военният университет, показани по –долу. Приемът на жени – курсанти е 15 % от общия брой на приети курсанти, което съответства на делът на жените –военнослужещи като цяло в Българската армия. (табл. 2 и фиг. 2)

Таблица 2. Брой на приетите курсанти през 2018 година по пол

РАЗЧЕТ	Кандидати		Приети		Съотношение	
	М	Ж	М	Ж	М	Ж
НВУ „Васил Левски“	378	60	146	25	85%	15%

В Българската армия се наблюдава постоянен интерес на жените както към обучение във военните училища, така и към кандидатстването за заемането на различни позиции във всички родове и видове войски. Голям принос за тази тенденция е решението за премахване на квотния принцип при кандидатстване след 2010 г., което допринесе за навлизането на жени във всички военни специалности, а условието за това е тяхната мотивация и постигнати резултати при кандидатстването и по време на последващото

обучение. Това е и гарант за правилната позиция на България относно осигуряване на равни права на жените и мъжете за професионална реализация в среда, която до началото на настоящия век се приемаше предимно за „мъжка територия“, а жените в униформа се приемаха като „екзотика“ или „изключение“. (фиг. 2)



Фиг. 2. Процентно съотношение на мъжете и жените във Въоръжените сили на Р България, 2016 г. [3]

По-долу ще бъдат посочени подобни данни относно кандидатите – жени за военните академии в някои европейски страни, с цел сравнителен анализ и извеждане на общи проблеми пред европейското военно образование и набелязване на мерки, които биха повишили мотивацията на жените за кариера във военната среда.

В Чешката република през 2018 г. от 24 251 професионални войници, 3088 от тях са жени, което представлява 12,73 %. Основната образователна военна институция, която подготвя офицерски кадри за Чешката армия е Университета по отбраната в гр. Бърно. В трите му факултета се обучават жени и мъже, както следва:

- във Факултет по Военно лидерство – жените са 15 %;
- във Факултет по Военни технологии – жените са между 5 и 10% за различните години на обучение;
- във Факултета по Военни здравни науки – жените представляват между 15 и 20 % от общия брой курсанти.

Като обща тенденция се наблюдава стабилно присъствие на жените – курсанти в Университета между 10 и 15 %, където също няма квоти за мъже и жени при кандидатстване за военно обучение. Според експерти – изследователи на тези процеси, тези съотношения се приемат за адекватни във военното висше образование в Чехия. [4]

Въпреки добрите тенденции, продължават да се търсят различни и нови начини за популяризиране на офицерската професия сред младите хора в Чехия като задължителен фактор е създаването на равни условия и за двата пола. Допълнително се обръща внимание на реалистичната кампания, която информира бъдещите курсанти за същността на обучението и военните тренировки, наред със стремежа да се осигурява предварителна информация за вариантите за бъдещото работно място като специализация и дестинация.

Обект на постоянен интерес е изследване на мотивацията на младите хора под 18 години, като се търсят и начини за организиране на информационни кампании и чрез социалните мрежи.

В обобщение, в Чешките Въоръжени сили се търси баланс в представителството на мъжете и жените, като въпреки съществуващите усилия за увеличаване на кандидатите за жени – курсанти, постоянно се разширява обхвата на използване на възможностите на маркетинга, връзките с обществеността и др.

За Въоръжените сили на северната ни съседка – Р Румъния присъствието на жените на бойното поле не е ново нещо, тъй като в историята са налице много доказателства относно участието им в различни военни действия. През последните десетилетия обаче жените започват да получават очевидна роля в военната среда, като днес статутът на жените в Румънската армия е напълно различен, присъствието им се приема и тяхната работа се признава. Преходът е в ход, резултатът от който все още не е завършен, тъй като различията между половете продължават да бъдат „пречка“.

В Румънските Въоръжени сили няма ограничения за включването на жените в армията, нито съществуват ограничения, които се прилагат само за участие в операциите. Има военни структури, които са ангажирани с интегрирането на перспективите на пола в армията. Като статистика може да се посочат приетите през 2016 г. 220 жени на различни длъжности в Румънската армия от 2249 кандидати, а при мъжете – от 9556 кандидати са приети 1272. Тези данни са показателни са сериозните тестове и изпити, които се прилагат и в Румънската армия, както и в армиите на страните, посочени по-горе в настоящия доклад, което е очаквано и нормално с оглед на високите изисквания, предявявани към военнослужещите от двата пола във всички съвременни армии.

В едно от основните образователни институции в Румъния – Академията на Сухопътните войски, гр. Сибиу за последните три години са приети съответно 232 – 273 – 233 курсанти – мъже и 37-48-43 курсанти жени.

Както се вижда в таблица 3 процентът на жените – военнослужещи не е особено висок, в сравнение с други армии – членки на НАТО и ЕС – жените в униформа в армията на Румъния представляват 5,9 % от общия брой военнослужещи.

Таблица 3. Съотношение между жените и мъжете военнослужещи във Въоръжените сили на Румъния – 2016 г. [3]

Table 1: All Active Duty Military Personnel		
Service	**Men**	**Women**
Army	50,9%	2,1%
Air Force	13,4%	1,1%
Navy	8,0%	0,4%
Other	21,8%	2,3%
Total	94,1%	5,9%
Ranks	**Men**	**Women**
OF 6 and above	0,10%	0,03%
OF 3-5	11,00%	7,03%
OF 1-2	6,00%	27,68%
OR 5-9	35,60%	45,07%
OR 1-4	47,30%	20,19%

Но наред с това, могат да бъдат посочени добри примери за успешната реализация на жените в Румънските Въоръжени сили, които да послужат като мотивация при кандидатстването на жените в армията. В Румъния служи първата жена военен лекар с ранг генерал; жена командва Националния военен колеж, младши офицери служат като пилоти, инструктори, водолази и военни полицаи, участват в операции в Афганистан, някои жени – парашутисти имат над 1000 парашутни скока.

В заключение, румънските колеги работят усилено по посока на по-доброто промотиране на военната система сред учениците в гимназиите, което включва както предимствата, така и недостатъците на военния живот, трудностите и ползите от военното образование. Изключително се залага на популяризирането на успешните примери за военна кариера както на мъже, така и на жени с цел промяна на нагласите и предубежденията в обществото. Всички тези мерки разчитат на диалога, толерантността като ценности и приемане на разнообразието, което наред с активното участие на жените във всички сфери, може да се приема като доказателство за демократичните процеси в обществения живот.

Интересен и различен опит се наблюдава във Въоръжените сили на Кралство Белгия. През последните две години са предприети различни стъпки за привличане на кандидати за Кралската военна академия в гр. Брюксел. Направени са редица анализи откъде младите хора получават информация за армията като организация и функции, доколко процедурите по подбор са успешни и ефективни и др. Получените отговори ориентират белгийските колеги в промени относно рекламната и приемна кампания за жени и мъже. Отчитайки факта, че младите хора добиват непълна и често изкривена представа за армията от филмите и интернет – пространството, те залагат изключително на директната комуникация с кандидатите, организация на работен ден от жени – военнослужещи за жени – кандидати, фокусират се върху социалните медии с ясни послания.

Друга сериозна промяна е свързана с премахването на изпита по физическа подготовка за кандидатите за военната академия. Отчитането на факта, че изпита за физическа годност се приема от младите хора като един от най-силните страхове от евентуален неуспех, а при жените – кандидати като сериозен провал, е залегнало в идеята за прием на курсанти без изпит по проверка на физическите качества. За да се достигне обаче необходимото ниво на физическа натренираност, през първата година на обучението се залага много на физическата подготовка и изпълнението на нормативи, които трябва да достигнат определено ниво в края на първата година. При непокриване на изискванията на физическите стандарти, курсантите са освобождават от Академията и така обучението си продължават най-мотивираните, устойчивите и издръжливите курсанти от двата пола.

Добра практика в Белгия е назначаването на жени на отговорни длъжности, както и в момента, жена – генерал ръководи Кралската военна академия, която е военна институция на университетското образование, отговорни за академично, военно и физическо обучение на бъдещите офицери, както и за непрекъснатото усъвършенстване на обучението им по време на тяхната активна кариера в отбраната.

Посочените различни практики и подходи относно увеличаване на кандидатите за висшите военни академии и университети, и по-конкретно на броя на жените – кандидати за обучение за офицери, бяха обсъдени и анализирани на семинар на представителите на европейските военни институции в рамките на Европейската инициатива за обмен на млади офицери, вдъхновена от програмата „Еразъм“. Дискусиите между академичните преподаватели, ПР-специалисти, експерти по човешки ресурси доведоха до формулиране на общи изводи и заключения, които биха подпомогнали управленските решения относно

търсенето на нови похвати и средства за оптимизиране на рекламните кампании на военните ВУЗ, както и за привличане на мотивирани млади хора с позитивен атитюд към армейската среда, в т.ч. и увеличаване на дела на жените в европейските армии.

Някои то тези изводи са свързани с:

- разбирането, че жените – курсанти трябва да се третират наравно с всички останали техни колеги и само професионалните им изпълнения да са от значение, а не техния пол;
- популяризирането чрез съвременните медии на ролевите модели на успешните жени и служители във военната среда;
- участието на повече жени - курсанти в процеса по реклама и набиране на кандидати, с основни усилия към целевата група на младежите и девойките между 16 и 18 години;
- използването на социалните медии и институционални уебсайтове, особено по време на маркетинговия процес по набиране на кандидати;
- постоянен контрол, анализ и мониторинг на целия процес по набиране, обучение и реализация на жените – курсанти и офицери;
- организирането редовно на Дни на отворените врати както и във военните академии, така в средните училища;
- подготовката на реклами, които да са насочени повече към въздействие върху емоционалната сфера на потенциалните кандидати, в които да се показват и жени в техния ежедневен живот - личен и професионален опит; особено когато жените са на мисии и операции;
- осигуряването на възможност да предварително явяване на изпит по физическа подготовка и при нужда подготвяне не препоръки относно подходящ спорт за подготовка за успешно справяне с поставените нормативи;
- формирането на смесени екипи от мъже и жени – курсанти в с цел укрепване на интеграцията;
- създаването на асоциации или социални мрежи от курсанти и офицери;
- включването на темите за равнопоставеността на половете в лекционния материал в подходящи учебни дисциплини според националните изисквания, за да се формира чувствителност към тази тематика и да се формира уважение като ценност за работа в полово – смесена среда;
- създаването на програми за превенция на тормоза на работното място, включително и сексуален тормоз;
- залагане на мерки за подобряване на равновесието между професионалния и личния живот - наличие на т. нар. "социален пакет";
- предлагане на възможности за професионално развитие и кариерно израстване на жените.

3. Заключение

Тези и други добри практики биха допринесли за привличането на гъвкави и знаещи млади хора, с ясна визия за тяхната бъдеща професионална реализация в армейската среда, за укрепването на връзките между европейските военни институции, за хармонизирането на военното образование, чрез увеличаване на дела на включените жени на лидерски позиции. На свой ред, посочените мерки са от изключително значение за функционирането на съвременните модерни армии, за укрепване на техните отбранителни способности, за запазване на потенциала на човешкия фактор и за генериране на състоянието на мир и стабилност в европейските граждани.

ЛИТЕРАТУРА:

[1] Министерски съвет, Програма за развитие на отбранителните способности на Въоръжените сили на Република България 2020, София, 2015, www.md.government.bg/bg/doc/cooperation/20181009_Programa_razvitie_otbranit%20sposobnosti.pdf

[2] NATO and partners focus on strengthening gender perspectives, 2018, www.nato.int/cps/su/natohq/news_155527.htm

[3] Summary of the National Reports of NATO Member and Partner Nations to the NATO Committee on Gender Perspectives, 2016, www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_01/1801-2016-Summary-NR-to-NCGP.pdf

[4] Výroční zpráva o činnosti Univerzity obrany v Brněza rok 2017, Brno 2018, www.unob.cz/uredni_deska/Documents/VZ_UO_2017.pdf

Име на автора: полковник доцент д-р Невена Цветкова Атанасова – Кръстева
Месторабота: НВУ „Васил Левски“, катедра „Национална и регионална сигурност“, гр. Велико Търново, бул. „България“ № 76
E-mail: nzatanasova@nvu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 231 - 237 Problems of Security Systems

MANAGEMENT POLICIES IN KOZLODUY NPP

PETAR D. DJOROV

ABSTRACT: *"Kozloduy NPP" management policies reflect the commitment of senior management to achieve an efficient management system that guarantees safe and environmentally friendly energy production with guaranteed quality and security of supply in accordance with national and international standards. Management policies are disseminated, clarified and brought to the attention of all staff.*

KEYWORDS:.*Policies, management system, senior management.*

ПОЛИТИКИ ПО УПРАВЛЕНИЕ В АЕЦ КОЗЛОДУЙ*

ПЕТЪР ДР. ДЖОРОВ

АБСТРАКТ: *Политиките по управление в „АЕЦ Козлодуй" отразяват ангажимента на висшето ръководство за постигане на ефективна система за управление, гарантираща безопасно и екологично чисто производство на енергия при гарантирано качество и сигурност на доставките, в съответствие с националните и международни норми. Политиките по управление са разпространени, разяснени и доведени до знанието на целия персонал.*

1. Въведение

На територия на Република България, АЕЦ Козлодуй е единствената организация, която експлоатира ядрено съоръжение, чрез поддържане на високо ниво на ядрена безопасност и радиационна защита. Изхождайки от този факт и за да отговори на поставените цели, Висшето ръководство на атомната електроцентрала декларира политики за управление в различни области, чрез които изразява своята готовност и намерения да подържа структура, организация и система за управление, с които да осигури необходимите финансови и материални ресурси, необходими за безопасността на ядрените съоръжения през техния срок на експлоатация.

Целта на политиките е приемането на решения за това как и с какви подходи, средства и методи, организацията възнамерява да се защитава. Те определят посоката на управление и поддържане на функциите за безопасност и сигурност в конкретни области, в съответствие с изискванията на организацията и съответните законови регулации.

В тази връзка целта на доклада е да се направи анализ на декларираните политики за управление в АЕЦ Козлодуй, от страна на висшето ръководство, за постигане конкретните цели в тези области, съгласно изискванията на Закона за безопасно използване на ядрената енергия (ЗБИЯЕ) и други нормативни актове.

2. Политики в организацията, същност и основни понятия

Въз основа на своите собствени политики висшето ръководство в организацията изготвя планове за управление, определя конкретните цели и приоритети по отношение на

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

безопасността, здравето, околната среда, сигурността, качеството и други аспекти касаещи дейността в организацията.

Целта на политиките е приемането на решения за това как и с какви подходи, средства и методи, управляващият орган в Дружеството възнамерява да защитава поставените си висши цели. По този начин политиките определят посоката на управление и поддържане на функциите за безопасност и сигурност в конкретни области, в съответствие с изискванията на самата организацията и съответните законови регулации (фиг.1). Управлението на система е част от цялото управление в организацията, което се основава на оценка на риска и установява, допълва, извършва, планира, координира, контролира, преглежда и ръководи системата за управление. Необходимостта от разработване на Политики зависи преди всичко от:

- Изискванията за безопасност, сигурност и защита на системата;
- Възприетите ръководни принципи от организацията в съответствие с поставените цели;
- Наличните ресурси.

Фиг. 1. Алгоритъм на политики за управление

В най-общ вид политиките включват:

- Сфера на дейност;

- Цел на политиката в предметната област;
- Ангажимент на ръководството за поддържане на система за управление;
- Принципи, позволяващи реализиране на целите на политиката;
- Стандартите определят изискванията и критериите при изграждане, функциониране, управление на политиката;
- Законовите и вътрешни организационни и нормативно-технически документи и инструкции определят последователността на изпълнение изискванията на стандартите;
- Запознаване и разясняване на правила за дейността в предметната област на политиката.

Политиките отразяват преди всичко ангажимента на висшето ръководство за постигане на общи и конкретни цели, посочвайки подхода и прилаганите принципи за постигане на тези цели. По този начин те определят:

- Правилата в организацията (какво може и какво не може), като по тази начин поставят основата за реализиране защитата при управление на системата;
- Помагат за определяне на средствата и процедурите за осигуряване сигурност и безопасност на системата;
- Поставят основата за реализиране защитата при управление на системата;
- Дава възможност за постигане на договореност между ръководителите, приемащи ключови решения в организацията, както и за описване зоните на отговорност в организационната структура на системата за управление;
- Определя регламент са носене на отговорност при нарушаване на зададените правила или допускане на грешки;
- Създава основа за предприемане на юридически действия.

Политиките сами по себе си трябва да включват:

- Общи принципи, които определят подхода на системата за управление;
- Конкретни правила за работа, които определят което е разрешено и което е забранено. Възприетите правила могат да се допълнят или прецизират с конкретни процедури и различни ръководства;
- Технически подход (анализ), който подпомага изпълнението на принципите и правилата, залегнали в политиката.

Процес на реализиране политиките се изразява в:

- Разработване на Документ за политика;
- Внедряване на документа за политиката в конкретната система (подсистема);
- Мониторинг на системата;
- Тестиране;
- Актуализиране и внасяне на промени в политиката.

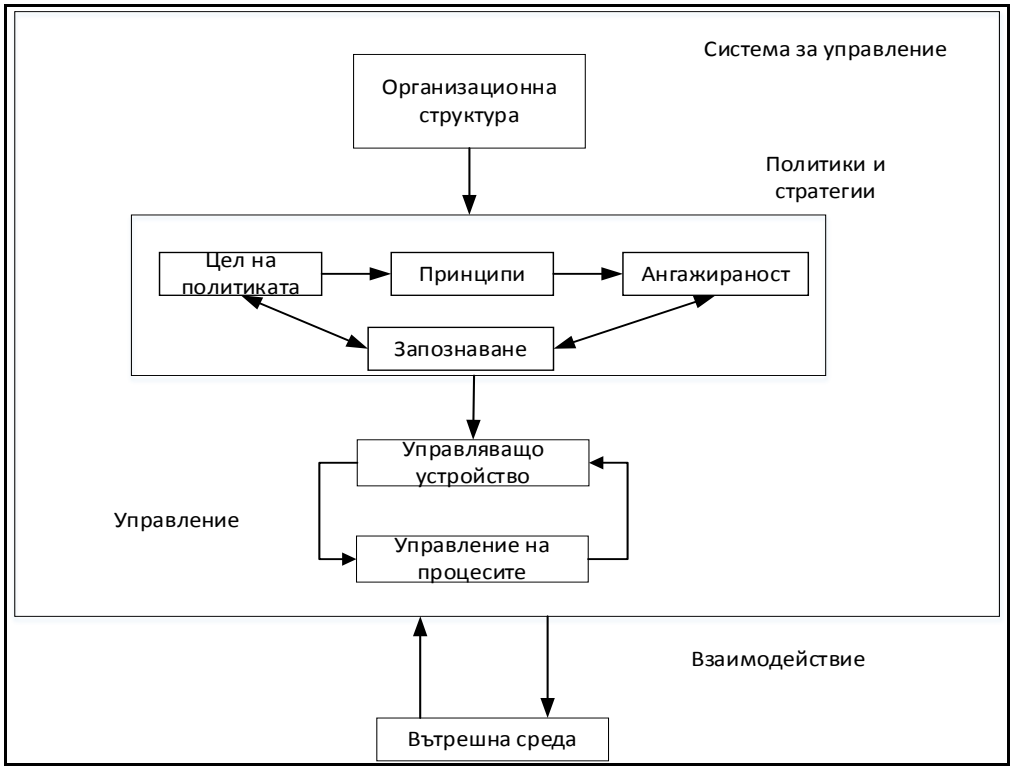
Политики по управление. Изхождайки от действащата нормативна уредба, приложена в Закона за безопасно използване на ядрената енергия, експлоатиращата организация трябва да притежава финансови, технически, материални ресурси и организационна структура за поддържане на високо ниво на безопасност за целия срок на експлоатация на ядреното съоръжение [2].

В тази връзка за да отговори на законовите изисквания, висшето ръководство на „АЕЦ Козлодуй“ разработва и разпространява съвкупност от декларирани политики, които установяват философията, принципите и основните фактори, които ръководят действията в организацията и системата за управление в Дружеството.

Изградената система за управление, създава условия за формиране и развитие на култура на безопасност, при която безопасността е с най-висок приоритет и има най-голямо значение за дългосрочния успех на Дружеството (фиг.2).

Изискванията на системата за управление описани в Наредбата за осигуряване на безопасността на ядрените централи обхваща [3]:

- Политики, декларации и стратегии на експлоатиращата организация;
- Описание на системата за управление;
- Внедряване на организационна структура на Дружеството, която осигурява реализацията на политиките и целите;
- Ясно определяне на отговорностите за вземане на решенията в рамките на система за управление;
- Описание на организационната структура, управленските нива, функциите на структурните нива;
- Развитие и поддържане на организационна култура сред персонала на Дружеството чрез спазване на вътрешните правила на поведение;
- Извършване на планирани прегледи за оценяване ефективността на система за управление.
- Описание на процесите и взаимодействието между тях.
- Осигуряване на необходимите ресурси за реализиране на определените политики и цели.



Фиг. 2. Модел на политики за управление в „АЕЦ Козлодуй“

Като процес системата за управление ясно определя кога, как и от кого се вземат решенията, свързани с осигуряване на ядрената безопасност при експлоатация. Изхождайки от законодателната рамка, задължение на експлоатиращата организация е да разработва, прилага, оценява и непрекъснато да подобрява системата за управление, чиито основни цели са да осигурява и повишава безопасността на ядрената централа.

Чрез декларираните политики за управление, ръководният персонал демонстрира ангажираност в разработването, прилагането, оценяването и непрекъснатото подобрение на системата за управление и насърчава участието на целия персонал в нейното прилагане и непрекъснато подобряване. За постигане на поставената си главна цел (безопасно, ефективно и екологично чисто производство на енергия при гарантирано качество и сигурност на доставките, в съответствие с националните и международни норми), ръководството на „АЕЦ Козлодуй" ЕАД е декларира прилагането на система за управление, която обединява всички изисквания към дейностите, изпълнявани от Дружеството. По този начин Висшето ръководството изразява своята ангажираност и подкрепа чрез:

- Определяне на стратегическите насоки за развитие;
- Определяне и огласяване на целите на политиките;
- Ясно определяне на принципите за реализиране на политики в конкретна област;
- Осигуряване на необходимата информация, средства и подкрепа на целия персонал за изпълнение на възложените задачи в съответствие с изискванията за поддържане на висока култура на безопасност.

В качеството си на стратегически обект „АЕЦ Козлодуй" поддържа високо ниво на ядрена безопасност, чрез осигуряване на необходима прозрачност при прилагане на най-високи стандарти, ясна стратегия и програма от мерки, включително вътрешни правила, необходими за осигуряване и поддържане качеството на всички дейности по експлоатацията на ядреното съоръжение. За постигане на поставената си главна цел (безопасно, ефективно и екологично чисто производство на енергия при гарантирано качество и сигурност на доставките, в съответствие с националните и международни норми) ръководството на атомната електроцентрала е декларирало прилагането на система за управление, която обединява всички изисквания към дейностите, изпълнявани от Дружеството. Системата функционира на базата на процесно-ориентиран подход с цел поддържане на взаимовръзките между процесите и дейностите за постигане на ефективност и ефикасност в управлението и оптимално използване на ресурсите за гарантиране на първостепенната роля на безопасността като основен приоритет за постигане на стратегическите цели поставени пред дружеството [1].

Системата за управление активно контролира изпълнението на процесите, с основен акцент на основните процеси свързани с безопасността. Тя гарантира, че процесите и дейностите се изпълняват съгласно всички изисквания на системата за управление без несъответствия. Наблюдението на процесите е важен механизъм за осигуряване на точна информация. Оценката използва наличната информация (в т.ч. показателите за самооценка) за да оцени и подобри процесите и тяхното протичане. По такъв начин системата за управление позволява процесите и техните дейности непрекъснато да бъдат наблюдавани, оценявани и подобрявани. Поради естеството на производството конфигурираната система, циклично повтаря и поддържа своето ефективно състояние. По безспорен начин това позволява точно определяне на отговорностите, повишаване на

ефективността, повишаване качеството на продуктите и услугите, модернизиране и непрекъснато подобрение на системата [4].

По този начин ръководството на Дружеството носи пълната отговорност за прилагането и непрекъснатото развитие на ефективността на системата за управление, гарантираща поддържането и повишаването на безопасността в „АЕЦ Козлодуй" ЕАД.

Политики в АЕЦ Козлодуй. За постигане на поставената цел и декларираните приоритети в различните области ръководството на „АЕЦ Козлодуй" ЕАД разработва и разпространява следните видове политики:

- Политика за управление на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на безопасността на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на сигурността на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на качеството на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на околната среда на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на здравословните и безопасни условия на труд на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на финансите и икономиката на „АЕЦ Козлодуй" ЕАД;
- Политика по обучението и квалификацията на персонала на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на пожарната безопасност на „АЕЦ Козлодуй" ЕАД;
- Политика по управление на човешките ресурси на „АЕЦ Козлодуй" ЕАД;
- Етичен кодекс на „АЕЦ Козлодуй" ЕАД.

Чрез тях ръководството на „АЕЦ Козлодуй" ЕАД отдава първостепенен приоритет на безопасността, както и стратегическите и преки цели за нейното постигане.

От направения анализ можем да обобщим че Политиките по управление са подходящи за целите и дейностите на организацията. Те изцяло отразяват ангажираността за изпълнение на изискванията на системата за управление. Подпомагат развитието и подобряването на култура на безопасност, чрез приложимите нормативни изисквания. Преглеждат се периодично с цел потвърждаване на тяхната актуалност. Политиките са разпространени, разяснени и доведени до знанието на целия персонал. По този начин ръководителите на всяко управленско ниво могат да участват, разработват, организират и реализират осъществяването на съответните планове за изпълнението на декларираните цели в политиките, както и да оценяват тяхното изпълнение чрез система от показатели. Всеки член на персонала е отговорен за приемането и прилагането на принципи на политиките в сферата на своята професионална реализация.

3. Заключение

Система за управление в „АЕЦ Козлодуй", представлява множество от взаимосвързани и взаимодействащи елементи за установяване на политики и цели, създаващи условия целите да бъдат постигнати по ефективен и ефикасен начин. Системата за управление обединява всички елементи на организацията в една обща система, позволяваща постигането на всички цели на организацията. Персоналът, оборудването и културата на организация, както и документираните политики и процеси са части от системата за управление. Процесите в организацията се разглеждат всички изисквания към организацията, установени в националното законодателство и

препоръките на стандартите за безопасност на Международната агенция за атомна енергия и други международни стандарти.

ЛИТЕРАТУРА:

[1] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

[2] Закон за безопасно използване на ядрената енергия, Обн. ДВ. бр.63/28.06.2002, изм. ДВ. (бр.7/19.01.2018).

[3] Наредба за осигуряване на безопасността на ядрените централи. Приета с ПМС № 245/21.09.2016 г., обн., ДВ, (бр. 76/30.09.2016).

[4] Описание на системата за управление на „АЕЦ Козлодуй" ЕАД.

Име на автора: докторант Петър Драганов Джоров
Месторабота: Катедра „Управление на системите за сигурност", Факултет по технически науки, Шуменски университет „Епископ Константин Преславски"
E-mail: Djorov_P@abv.bg

GEODESIAN CONTROL OF INFRASTRUCTURE OBJECTS KOZLODUY NPP

PETAR D. DJOROV

ABSTRACT: *"Kozloduy NPP" is a production plant for electricity, representing a complex system of constructed engineering and technical complex, including many functional facilities and infrastructure objects. They are located in the territory of the plant under certain technological rules and technological requirements with a significant degree of construction and density of infrastructure and engineering facilities.*

KEYWORDS:. *Infrastructure objects, engineering elements, monitoring, geodetic control.*

ГЕОДЕЗИЧЕН КОНТРОЛ НА ИНФРАСТРУКТУРНИТЕ ОБЕКТИ В АЕЦ КОЗЛОДУЙ*

ПЕТЪР ДР. ДЖОРОВ

АБСТРАКТ: *„АЕЦ Козлодуй“ е производствено предприятие за електрическа енергия, представляващо сложна система от изграден инженерно-технически комплекс, включващ множество функционални съоръжения и инфраструктурни обекти. Те са разположени на територия на централата по определени технологични правила и технологически изисквания със значителна степен на застроеност и наситеност на инфраструктурни обекти и инженерни съоръжения.*

1. Въведение

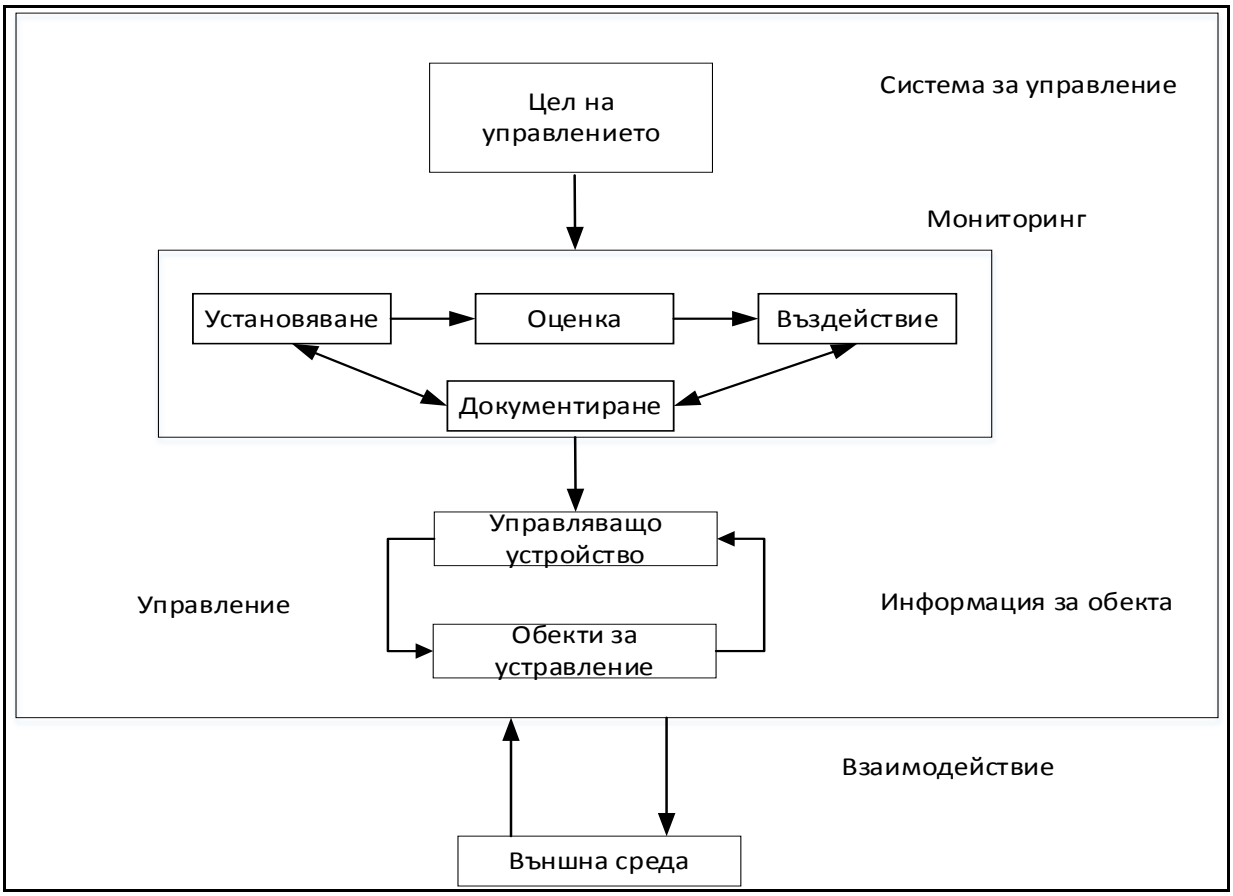
Геодезичният контрол в „АЕЦ Козлодуй“ се осъществява чрез мониторинг на инфраструктурните обекти и изграждащите ги елементи от инженерната инфраструктура. Мониторингът на инженерната инфраструктура има за цел провеждането на наблюдения преди всичко за физическото състояние на елементите и обектите находящи на територията на Дружеството като обхваща всички райони, пряко или косвено свързани с експлоатационната и ремонтна дейност, безопасността и физическата защита. Поради концентрацията на голям брой и различни по тип и размери обекти, на наблюдение и контрол се подлагат както строителни конструкции, складови бази, хидротехнически съоръжения, оборудване, надземни и подземни технологични елементи, инфраструктура и др., така и настъпващите в тях процеси или явления от естествената и изкуствена околна среда, които могат да им въздействат. Работата на технологичното оборудване, конкретните производствени дейности и състоянието на съоръженията са свързани с наблюдаването на различни параметри, характеризиращи експлоатационните и физически особености на инфраструктурните обекти и технологични елементи. В резултат на провежданите геодезически мониторингови дейности се получават големи количества разнородни данни. Тяхното пълноценно използване е необходимо за взимане на правилните решения от страна на експлоатационния, ремонтен, контролен и ръководен персонал в предприятието.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

В тази връзка целта на доклада е да се направи анализ на процесът за геодезичен мониторинг на инфраструктурните обекти в „АЕЦ Козлодуй“ и да се анализират основните мониторингови дейности на системата за геодезичният контрол в „АЕЦ Козлодуй“.

2. Геодезичен контрол на инфраструктурните обекти в АЕЦ

Провеждането на мониторинг е свързано с натрупване на информация, състояща се от количествени и качествени геодезични данни, тяхната обработка, анализ и интерпретиране. Управлението на системата за геодезичният контрол в „АЕЦ Козлодуй“ се осъществява с цел получаване на информация за наблюдаваните обекти, процеси или явления (фиг.1).



Фиг. 1. Управление на геодезичният контрол в „АЕЦ Козлодуй“

Управлението на геодезичният контрол се разглежда като процес, който преминава през четири фази съгласно действащата система за управление в „АЕЦ Козлодуй“, която отчита процесния подход и организационно-управленска структура обособена на функционален принцип с основните структурни подразделения. Изискванията на системата за управление се прилагат степенувано към продуктите (резултатите) и дейностите на всички процеси. Това спомага да се прецизира влиянието им върху безопасността и от там оптимално разпределение на необходимите ресурси за изпълнение. По този начин се създават условия за формиране и развитие на култура на безопасност при която безопасността е с най-висок приоритет и има най-голямо значение за дългосрочния успех на Дружеството.

Мероприятията за геодезичен контрол се осъществява в две основни направления:

- Мониторинг за установяване на деформационни процеси на хидротехнически съоръжения и строителни конструкции и изграждащите ги инженерни елементи;
- Поддържане на актуалното състояние на кадастъра и инфраструктурни обекти.

С цел да се осигури максимална сигурност, експлоатационна годност и технологично правилно използване на ресурсите на „АЕЦ Козлодуй“ се налага планирането и провеждането на дейности за наблюдение, контрол, оценка и управление на състояния, процеси и явления в инженерната инфраструктура. Тези дейности могат да се обобщят с понятието мониторинг на инженерната инфраструктура

Геодезичен контрол за установяване на деформации. Изследването на деформации е неразделна част от геодезичният мониторинг, необходим за експлоатацията на инженерните съоръжения в „АЕЦ Козлодуй“.

През своя жизнен цикъл всяко техническо съоръжение, подобно на всичко в природата, претърпява някакъв вид изменения под въздействието на различни по произход и характер фактори и сили. В резултат на това комплексно въздействие в конструкциите на съоръженията настъпват краткотрайни или постоянни геометрични изменения, които най-общо се наричат деформации. През периода на експлоатация неминуемо се натоварват различни части от конструкцията на ядрените съоръженията, което води до появата на абсолютни и относителни премествания. Определянето на деформациите дава възможност за следене поведението на конструкцията по време на периода на тяхната експлоатация, което позволява навременна реакция и взимане на превантивни мерки, предхождащи инцидент, авария, опасност или заплаха за конкретното съоръжение.

Изследването на деформации има важно значение за изучаване на поведението, функционалната и експлоатационна годност на строителни конструкции и съоръжения през целия техен жизнен цикъл, както и на земната основа, в която те са изградени.

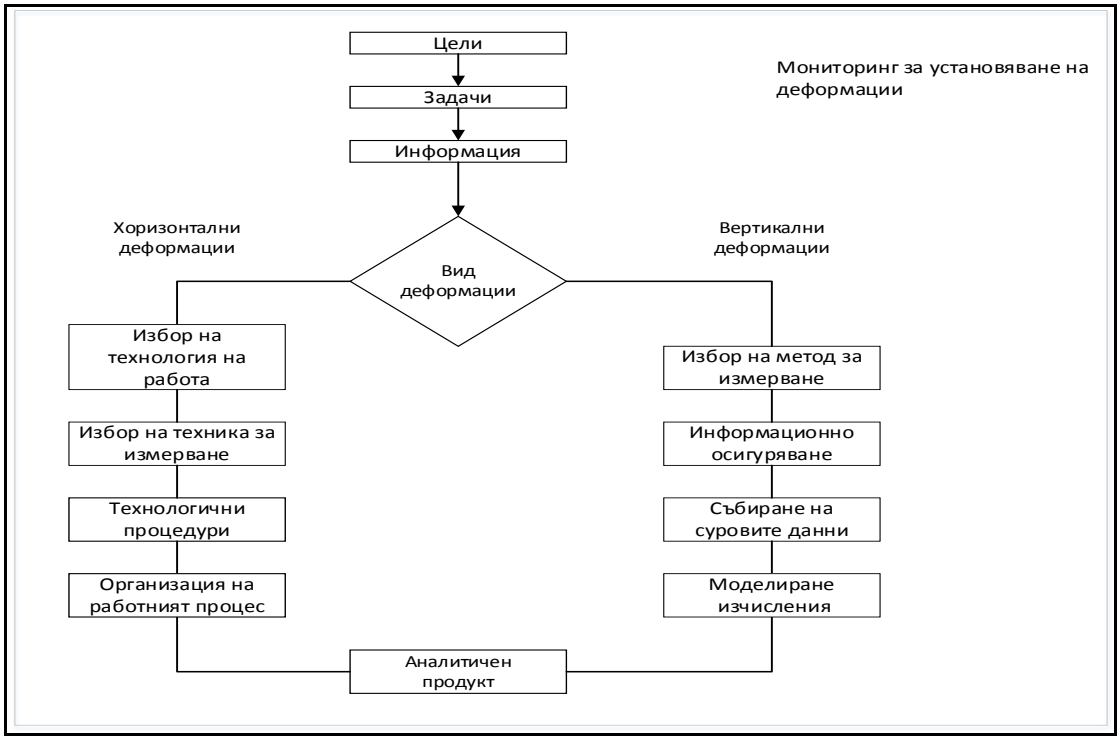
Друга важна цел, която се постига чрез изследването на деформации, е получаването на реална оценка за оказаното въздействие на комплекса фактори, влияещи върху наблюдаваните обекти. В резултат от провеждането на такива изследвания се осигуряват данни, които могат да служат при взимане на решения за въздействие на проблемни съществуващи съоръжения, преоценка на строителни технологии и проекти за бъдещо строителство или при проверяване на научни хипотези и модели за изследваните обекти.

В зависимост от геодезичният мониторинг и съоръженията в които възникват, на площадката в „АЕЦ Козлодуй“ се установяват два вида деформации - вертикални и хоризонтални деформации. За някои обекти се предвижда да се наблюдават пространствени деформации, т.е. едновременно вертикални и хоризонтални. Предмет на такъв мониторинг са например:

- Проекти за установяване на деформации чрез геодезически методи, изработени от специализирани проектантски организации, когато се отнасят до отговорни и сложни обекти и съоръжения;
- Технически решения за организиране и провеждане на изследвания за установяване на деформации, когато се отнасят до второстепенни обекти при пряко изпълнение на действащи инструкции, наредби, решения или протоколи от технически съвети за конкретни съоръжения;

- Разпореждане в резултат от заявка, подадена от подразделенията, експлоатиращи и или стопанисващи съоръженията, подлежащи на геодезичен контрол.
- Изграждане, поддържане и опазване на точки от опорни геодезични мрежи (ОГМ) за височинни и хоризонтални геодезични измервания;
- Стабилизиране, сигнализиране и опазване на мрежи от контролни точки по обектите, подлежащи на геодезичен контрол;
- Периодични контролни измервания на елементите от височинната и хоризонтална ОГМ на „АЕЦ Козлодуй" с цел проверка на устойчивостта на геодезическите точки от опорните мрежи;
- Периодични преки геодезични измервания на елементите от геодезическите мрежи за мониторинг на деформации, включващи опорни, контролни и контролирани точки;
- Документиране на първичните резултати от преките геодезически измервания и извършване на математическа обработка на геодезическите измервания;
- Съставяне на протоколи и отчети за систематизиране на данните, представяне на резултатите от провеждания геодезичен контрол в подходящ табличен и графичен вид, интерпретация на резултатите, получаване на изводи и заключения за развитието на деформационни процеси;
- Създаване и постоянно попълване на база данни за резултатите от провеждания геодезичен контрол по обекти с цел архивиране на събираните данни и информационно обслужване относно деформационните процеси на заинтересовани специалисти от проектантски, експлоатиращи и стопанисващи подразделения.

За мониторинг на деформационните процеси в „АЕЦ Козлодуй" се използват разнообразни геодезически подходи използвани в инженерната литература, добри практики и натрупан предишен експлоатационен опит, отговарящи на законовите изисквания, наредби, инструкции от национално ниво и произтичащите от тях политики и вътрешни административни за дружеството документи. Изборът и подборът на метода зависи от фактори, като основните от тях са необходимата точност на метода измерване, необходимата за целта измерителна апаратура, условия за работа, икономическата ефективност и др. (фиг.2).



Фиг. 2. Мониторинг за деформационни процеси в „АЕЦ Козлодуй“

Геодезичният контрол на инфраструктурните обекти и инженерни съоръжения, подлежащи на мониторинг, се провеждат чрез периодично извършване на преки геодезични измервания на определени геометрични елементи от геодезичните мрежи, включващи едновременно опорни и контролни точки. Периодичността на измерване се определя съгласно технически документи, инструкции, правилници, наредби и закони, регламентиращ мониторинговите дейности за всяко конкретно съоръжение или обект на мониторинг, чрез график за извършване на плановите дейности за установяване на деформации, изработен съгласно инструкция за геодезичен контрол.

Провеждането на геодезичен контрол за някои обекти е свързано с определени технологични процедури, като изпълнението на тези процедури определя времето и честотата на мониторинга. За такива обекти периодичността и времето за провеждане на геодезичния контрол се определя от ръководството на подразделението, експлоатиращо конкретното съоръжение [1].

Резултатите от анализа от геодезическите измервания се моделират и обработват математически, интерпретират се в зависимост от конкретния обект и служат за изходна информация за установяване на деформационни процеси в контролираните съоръжения (фиг. 3).

Фиг. 3. Анализ и моделиране на деформационни процеси в „АЕЦ Козлодуй“

След анализ на извършеният геодезичен контрол, се изготвя протокол с резултати от мониторинга на деформационните процеси за всеки конкретен обект. Аналитичният продукт се одобрява, документира, архивира и предоставя на съответните заинтересовани лица, съгласно действащите административни инструкции в „АЕЦ Козлодуй”. В протоколите за проведения геодезичен контрол се вписват следните данни:

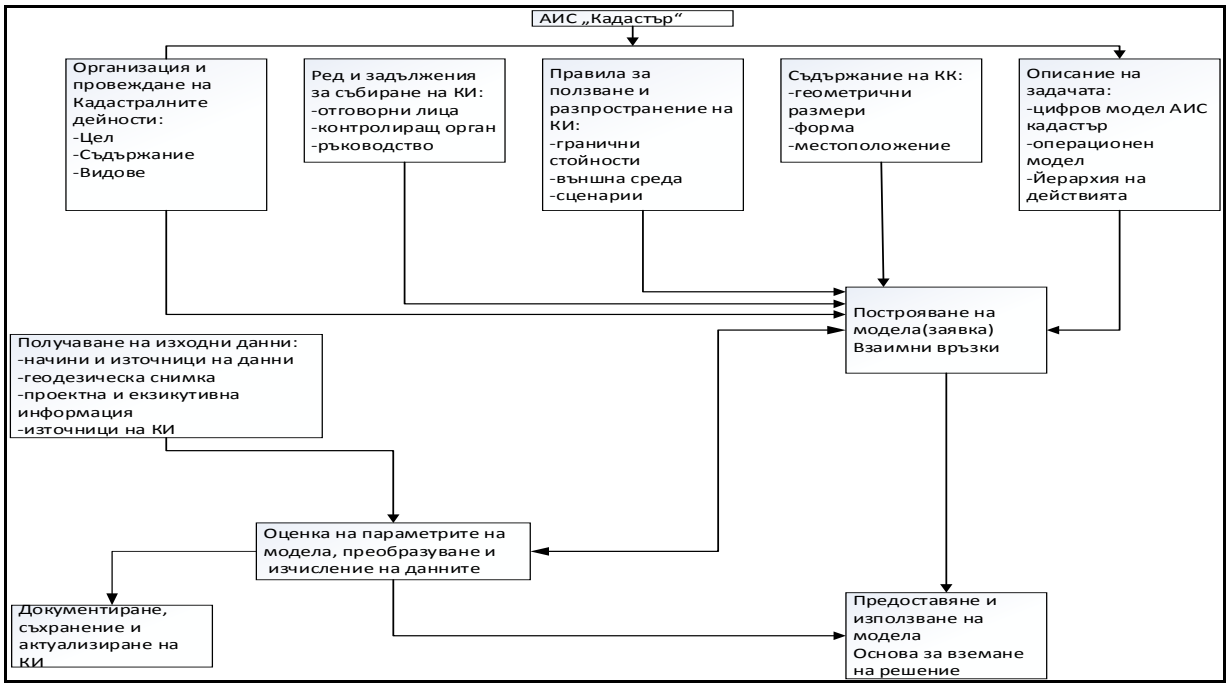
- Код и име на обекта на геодезичен контрол;
- Име на извършителя на геодезическите измервания;
- Дата на реализиране на геодезичния контрол;
- Използван метод и инструмент за извършване на геодезическите измервания;
- Статистически анализи на резултатите от проведения геодезичен контрол, като информация за границите и средните стойности на установените абсолютни и относителни деформации, констатации за характера и развитието на деформационните процеси, особености в деформационното поведение на конкретното съоръжение или контролна геодезическа точка, сравнение на получените стойности за установените деформации и допустимите стойности;
- Заключение, относно влиянието на установените деформации върху работоспособността на строителните конструкции и технологично оборудване.
- Като приложения към протоколите трябва се представят:
- Схема за разположение на контролните точки по конструкцията на наблюдаваното съоръжение;
- Таблици с измерените стойности на наблюдаваните величини;
- Таблици със стойностите на констатираните абсолютни и относителни деформации;
- Графики, представящи развитието на деформационните процеси във времето;

- Графики, представящи съпоставка на резултатите от провеждания контрол за взаимосвързани или характерни групи контролни точки (при необходимост).

Резултатите от дейностите при провеждане на геодезичен контрол се документират, съхраняват и предоставят, чрез поредица документи с взаимосвързано съдържание и различно предназначение.

Кадастрални дейности за поддържане на актуалното състояние на кадастъра и инфраструктурни обекти.

Кадастралните дейности имат за цел създаването и поддържането в актуално състояние на картен материал и база данни с кадастрална информация, отразяващи фактическото местоположение, геометричните и основни описателни характеристики на инфраструктурните обекти, всички подземни, наземни и надземни съоръжения от инженерната инфраструктура на територията на „АЕЦ Козлодуй”.



Фиг. 4. Алгоритъм на системата АИС „Кадастър“ в „АЕЦ Козлодуй“

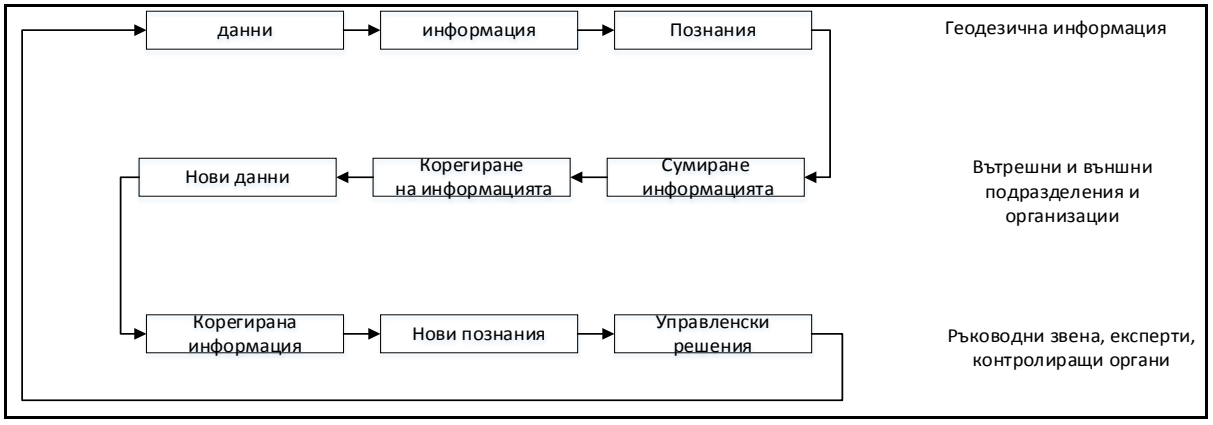
В експлоатационния период на „АЕЦ Козлодуй”, както на всяко промишлено предприятие основен технически документ е изпълнителният генерален план. Той се създава с цел да се документира действителното положение на елементите от инженерната инфраструктура - сгради, съоръжения, комуникации (надземни, наземни и подземни), благоустройствени елементи и релеф. По същество изпълнителният генерален план представлява комбиниран план, включващ кадастрален и топографски план за територията на обекта, както и кадастрален план на подземните проводи и съоръжения. Съгласно Закона за кадастъра и имотния регистър (ЗКИР) ведомствената кадастрална информация се събира в специализирани кадастрални карти, регистри и информационни системи. Организирането и провеждането на мероприятия за събиране на данни за инженерната инфраструктура се обобщава с термина кадастрални дейности. Те са обединени в автоматизирана информационна система АИС „Кадастър“, отговарящи на изискванията на ЗЗКИ, ППЗЗКИ, Наредба АИС, Наредба ФС, Наредба за КС, Наредба за ИС и създадените вътрешни инструкции за сигурност на информацията. Редът и начина на

събиране, създаване, съхраняване, изготвяне и предоставяне по съответният ред на системата АИС „Кадастър“ е представен на (фиг.4).

Ведомствените кадастрални дейности на територията на „АЕЦ Козлодуй” включват следните основни задачи:

1. Създаване и поддържане на Работна Геодезична Основа (РГО) за извършване на преки геодезични измервания необходими за събиране на кадастрална информация;
2. Създаване и поддържане на Работна Геодезична Основа (РГО) за извършване на преки геодезични измервания необходими за събиране на кадастрална информация;
3. Събиране на кадастрални данни (географски и атрибутни) за всички обекти от инженерната инфраструктура [2].

Мониторинг и потребители на геодезична информация. Процесът за мониторинг на инфраструктурните обекти, чрез Геодезичен контрол обуславя необходимостта от достоверно и детайлно познаване на инженерната инфраструктура в „АЕЦ Козлодуй“. Генерирането на големи количества разнородни геодезични данни и информация води до постоянна необходимост от обмен на информация, както между различните нива в организационната структура на Дружеството, така и между него и външни организации. По този начин обменът на информация се превръща в двустранен процес. Експлоатационни показатели и данни от мониторинга на инфраструктурата се предоставят вътре в организационната йерархия за нуждите на контрола и управлението. Между експлоатационните, инвеститорските, проектантските, ремонтните и строителните звена, или отделни такива организации, непрекъснато се обменят данни за инженерната инфраструктура, защото проектирането на ремонтни дейности, реконструкции и ново строителство е свързано с двустранен обмен на информация. След завършване на строителни работи изпълнителите предоставят изпълнителни планове и данни за актуалното състояние на инфраструктурните елементи вследствие на тяхната работата. Придобитата нова информация се предоставя за актуализиране на Кадастралната карта и попълването на базата данни, необходими за осъществяване на последващ геодезичен мониторинг (фиг.5).



Фиг. 5 Геодезична информация в следствие от мониторинга

Изхождайки от фактите за необходимостта от геодезичните данни, придобитата информация, постигането на ново познание необходимо за взимане на управленски решения, може да предположим че:

- Данните са неделима част от информацията, която описва свойствата и характеристиките на даден обект;
- Данните се превръщат в информация при която се разкриват скрити значения и стойности и характеристики;
- Данните се превръщат в информация, чрез събиране, обработка и анализ
- Информацията се получава чрез моделиране на данните за получаване на ново познание;
- Новото познанието е ценно, само когато потребителят на информация постига целите си за взимане на управленски решения.

По този начин можем да обобщим, че геодезичните данни и информацията за инфраструктурните обекти, се явяват ключови понятия в процеса на управление и експлоатация в „АЕЦ Козлодуй“. Обръщайки се към геодезичният мониторинг като част от процеса на управление, колкото информацията за наблюдаваните явления и произтичащите от тях процеси са повече разбираеми, толкова повече ще са познанията, които могат да бъдат в помощ на ръководството за постигане на целите на Дружеството.

3. Заключение

Инженерната инфраструктура в „АЕЦ Козлодуй” търпи непрекъснато развитие в периода на своята експлоатация, поради извършване на ремонти, реконструкции, модернизации и ново строителство. В случай, че измененията не се отразяват своевременно, в резултат на тези динамични промени, геодезичната информация за инфраструктурните обекти и изграждащите ги инженерни съоръжения остарява с бързи темпове. Колкото по-активно се реализират геодезичен мониторинг и контрол, толкова по-често ще се отразяват изменения в инженерната инфраструктура и съответно постъпващата информацията за нея. Информацията е полезна само когато тя е надеждна, както от гледна точка на точност, детайлност и изчерпателност, така и от гледна точка на актуалност. Динамиката в жизнения цикъл на инженерната инфраструктура изисква съответното динамично и непрекъснато поддържане в актуално състояние на кадастралните дейности. Този непрекъснат процес на поддържане на информация за инженерната инфраструктура е свързан с постоянен геодезичен мониторинг, осигуряващ пространствени данни и информация за инфраструктурните обектите и инженерни съоръжения.

От направеният кратък анализ на геодезичният мониторинг може да обобщим, че той изпълнява своето предназначение, защото чрез увеличаване на геодезична и кадастрална информацията се натрупват повече познания и опит, а това води до увеличаване степента на сигурност и поддържане на високо ниво безопасност в „АЕЦ Козлодуй”.

ЛИТЕРАТУРА:

[1] Инструкция за провеждане на геодезичен контрол на строителните конструкции, хидротехническите съоръжения и технологично оборудване в „АЕЦ „Козлодуй” ЕАД - Ид. № ХТС.ГК.ИН-008/02.

[2] Инструкция за провеждане на кадастрални дейности на територията на „АЕЦ „Козлодуй” ЕАД – Ид. № ХТС.ГК.ИН-011/02..

Име на автора: докторант Петър Драганов Джоров
Месторабота: Катедра „Управление на системите за сигурност“, Факултет по технически науки, Шуменски университет „Епископ Константин Преславски“
E-mail: Djorov_P@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 247 - 254 Problems of Security Systems

ESSENCE AND PECULIARITIES OF LOCAL SELF-GOVERNMENT

RUMYANA V. VASILEVA

ABSTRACT: *Self-management is a fundamental right of citizens and a principle of local politics. Local self-government is the level of democratic government closest to citizens. It allows them to participate in the local decision-making process.*

According to chapter seventh of the Constitution of the Republic of Bulgaria, the bodies of local self-government and local administration in the Republic of Bulgaria are the municipal council, the mayor of the municipality and the district governor. The municipal council is a local self-government body in the municipality, the mayor is a body of executive power in the municipality, and the district governor conducts the administration in the district, and in this sense he acts as a local representative of the central state power.

KEYWORDS: *Bodies of local self-government, local administration, mayor of the municipality, district governor, municipal council.*

СЪЩНОСТ И ОСОБЕНОСТИ НА МЕСТНОТО САМОУПРАВЛЕНИЕ*

РУМЯНА В. ВАСИЛЕВА

АБСТРАКТ: *Самоуправлението е основно право на гражданите и принцип на местната политика. Местното самоуправление е равнището на демократичното управление, което е най-близо до гражданите. То им позволява да участват в местния процес на вземане на решения.*

Съгласно глава седма от Конституцията на Република България органите на местното самоуправление и местната администрация в Република България са общинският съвет, кметът на общината и областният управител. Общинският съвет е орган на местно самоуправление в общината, кметът е орган на изпълнителната власт в общината, а областният управител ръководи администрацията в областта и в този смисъл той действа като местен представител на централната държавна власт.

1. Въведение

Държавата съществува и функционира чрез система от държавни органи. Процесът за изграждането им е сложен. На основата на Конституцията са извършени съществени изменения в системата на държавна организация и структура на държавните органи в съответствие с принципа за разделение на властите.

Държавният апарат е широка система, която включва в себе си държавните органи, административните структури, които ги обслужват и подпомагат и държавните институции.

Под орган на изпълнителната власт разбираме еднолично или колегиално звено, което притежава държавно властнически правомощия. Органите на изпълнителната власт са вид държавни органи и като такива имат сходни черти с останалите. Те осъществяват държавна власт. Органите на изпълнителната власт, както и всички държавни органи, имат установени предели, в които могат да упражняват властническите си правомощия. Те

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

осъществяват подзаконова дейност и действията им се извършват винаги въз основа и в изпълнение на закона.

Държавният апарат обхваща системата от всички държавни органи, която се състои от:

- органи на държавна и местна власт и самоуправление. Те имат законодателни функции;
- органи на държавната и местната администрация. Те имат изпълнителни функции;
- съдебни органи – такива са следователите и следствените служби, прокурорите и прокуратурите, съдиите и съдилищата.

Държавните административни органи в своята цялост образуват административния апарат на държавата. Това е апаратът на изпълнителната власт и местното самоуправление. Административният апарат е организираният сбор от държавни и местни органи, които са предназначени да осъществяват задачите на държавното управление и да развиват конкретна, изпълнителна творческа дейност. Административният апарат съдържа редица организационни нива и подразделения, административно – организационни единици, органи и учреждения. Административният апарат е организационния механизъм, чрез който се извършва административната дейност в държавата.

Характерна черта на административния апарат е йерархията на нивата и звената в него. Тази йерархия се проявява в подчинеността на актовете и действията на по-низшите звена на висшестоящите звена в административния апарат, както и във възможностите за контрол, упражняван от висшестоящите органи по отношение на низшестоящите.

Административната теория определя, че държавните административни органи се класифицират по вид, в съответствие с различни разграничителни белези.

В зависимост от това, дали органът е създаден по конституционен път, те се делят на: административни органи за които Конституцията изрично предвижда създаването и правомощията им, и органи, които изрично не са предвидени в Конституцията /конституционно и неконституционно устроени/. Чрез Конституцията се създават само основните административни органи – Министерски съвет, министрите, областните управители и кметовете. Административните органи, които не се създават въз основа на Конституцията, се създават на основата на различни законови или други актове. Такива са различни агенции или еднолични органи, като например органите на Министерството на вътрешните работи.

В зависимост от органите, които ги образуват административните органи се подразделят на: органи образувани от представителни органи на държавна власт или местно самоуправление. Тези органи са подконтролни и се отчитат на органите, които са ги образували /напр. Министерският съвет се образува от Народното събрание; заместник - кметовете на общините се избират от общинските съвети/. Друг вид са органите избрани пряко от населението /напр. кметовете на общини/. Отделен вид са и органите образувани от други административни органи /напр. Министерският съвет може да избира председатели на държавни агенции, на държавни комисии и изпълнителни агенции/.

Според териториалния обсег на правомощията си административните органи се делят на централни и териториални.

Централните административни органи осъществяват дейността си на територията на цялата страна. Техните актове и действия имат задължителна сила на територията на цялата страна, за всички части на държавата и за всички граждани и чужденци, намиращи се на територията на страната. В съответствие със Закона за администрацията централни

органи на изпълнителната власт са: Министерският съвет; министър – председателят; заместник - министър председателите и министрите.

Местни /териториални/ органи на изпълнителната власт са: областните управители и кметовете на общини. Техните правомощия имат ограничен териториален обхват вътре в страната. Актовете и действията им важат само за част от страната и имат по принцип задължителна сила само за жителите или за пребиваващите в съответното населено място.

Органи на изпълнителната власт са и: председателите на държавните агенции, държавните комисии, изпълнителните директори на изпълнителните агенции и ръководителите на държавни институции, създадени със закон или с постановление на Министерския съвет. Тези органи издават индивидуални административни актове.

Органите на държавна власт в Република България осъществяват непосредствено ръководство на съответната им администрация. Администрацията подпомага дейността на органите на държавната власт, но нейното основно предназначение е да предоставя публични услуги на гражданите.

Обхватът на държавната администрация включва:

- централна държавна администрация – обхващаща администрацията на законодателната власт /Народното събрание/; администрацията на изпълнителната власт /администрацията на Министерския съвет, министерствата, държавните агенции, администрацията на държавните комисии, изпълнителните агенции/; администрацията на съдебната власт /на следствието, прокуратурата и съда/; президентската администрация и администрация на институциите, независими от изпълнителната власт;
- териториална администрация – обхващаща областните и общинските администрации, администрациите на районите и кметствата;

Структурата на всяка от посочените администрации е правно регламентирана с устройствени правилници.

2. Изложение

Статутът и компетенциите на местните органи на изпълнителната власт зависи от териториалното деление на Република България. Тя понастоящем е разделена на общини и области.

Кмет и общинска администрация

Според чл. 5 от Закона за местното самоуправление и местната администрация (ЗМСМА) общината е основна административно-териториална единица, в която се осъществява местното самоуправление. Тя е юридическо лице и има право на собственост и на самостоятелен общински бюджет.

Орган на изпълнителната власт в общината е кметът. Той, както и кметовете на райони и кметства се избират пряко от населението за срок от 4 години при условия и по ред, определени с Изборния кодекс [2].

Правомощията на кмета са определени в ЗМСМА. Част от тях са:

- Назначава и освобождава от длъжност заместник-кметовете на общината, ръководителите на звената на издръжка на общинския бюджет, кметските наместници, служителите в Общинска администрация и налага предвидените от закона дисциплинарни наказания;
- Отговаря за опазването на обществения ред, като за осигуряването му издава писмени заповеди, задължителни за началниците на съответните полицейски служби;
- Организира и отговаря за изработването и изпълнението на общинския бюджет;
- Организира изпълнението на дългосрочни програми.

- Организира изпълнението на решенията на Общинския съвет като се отчита пред него.
- Организира изпълнението на задачите, които произтичат от законите и от актовете на Президента на Република България и Министерския съвет;
- Възлага изпълнението на свои функции на кметове на кметства, контролира дейността им и може да отмени техни актове.
- Организира и провежда действия по защита на населението при бедствия и аварии;
- Възлага или разрешава изработването на устройствени планове и техни изменения на територията на общината.
- Утвърждава устройствения правилник на Общинска администрация след приемането на структурата и числеността на персонала на администрацията;
- Осъществява правомощията си по придобиване, управление и разпореждане с общинско имущество [2].

В рамките на общините се изграждат и местни органи на представителната власт – Общински съвети. Те по своята същност представляват местен аналог на основния представителен орган на страната – Народното събрание. Общинският съвет е орган на местното самоуправление и се избира от жителите на общината при условие и по ред, определени от закона.

В своята дейност кмета и общинският съвет се подпомагат от *общинската администрация*. Тя се ръководи от секретар на общината, който отговаря за нейната дейност. Общинската администрация осигурява организационно - техническото обзавеждане на службите в общината. Структури от общинската администрация осигуряват деловодната дейност и документооборота в общината, както и съхраняването на общинския архив. В общинската администрация се създават структури за гражданска регистрация и административно обслужване, за поддържане в актуално състояние на избирателните списъци, за жалбите и предложенията на гражданите. Структурата на общинската администрация се определя с решение на общинския съвет. Общинската администрация е организирана в обща и специализирана администрации, състоящи се от дирекции, отдели и сектори. Ключова роля има секретаря на общината, който организира дейността на общинската администрация.

Областен управител и областна администрация

Областта е административно-териториална единица, в която се децентрализира държавната власт с оглед провеждането на ефективна държавна политика.

Областният управител като едноличен орган на изпълнителната власт в областта с обща компетентност, в съответствие с конституционно определените му правомощия, осъществява държавното управление в областта и осигурява съответствие между националните и местните интереси при провеждането на регионалната политика. Областният управител се назначава от Министерския съвет и се подпомага от заместник областни управители и областна администрация. Той е второстепенен разпоредител с бюджетни кредити към Министерския съвет. Твърде често ролята на Областния управител се преплита с ролята на областта като административно-териториална единица. Съгласно чл. 142 от Конституцията областта е административно-териториална единица за провеждане на регионална политика, за осъществяване на държавно управление по места и за осигуряване на съответствие между националните и местните интереси. Територията на Република България е разделена на 28 области. От особена важност е да се разграничат отделните етапи по реализирането на дадена политика: разработване, координация,

изпълнение и контрол между различните нива на управление и съответно правомощията на органите на изпълнителната власт във всеки един етап. Правомощията на областния управител са определени в Закона за администрацията. Наред с тях в още над 80 нормативни акта са предвидени редица функции и задачи.

В този ред на мисли правомощията на Областния управител могат да се определят в две основни насоки:

1) Правомощия по координация;

2) Правомощия по контрол.

Част от тези правомощия са детайлно и ясно регулирани от законодателството, със съответните механизми за тяхното осъществяване, имат реално приложение, съществува добра практика в съответните областни администрации. Други правомощия, предимно отнасящи се до координацията и взаимодействието, имат по-скоро декларативен характер. Те не са подплатени от конкретни, ясно посочени механизми и ред за упражняването им в съответните закони, нито има регламент за последиците от неосъществяването им. Първата и най-важна задача на областта, определена в чл.142 от Конституцията, е да провежда регионалната политика. Истината е, че българските области нямат възможност да осъществяват регионална политика, защото липсата на собствен ресурс е непреодолимо препятствие пред планирането и прилагането на регионални програми. Законодателството регламентира и отделни дейности, които са възложени за изпълнение от областния управител, които излизат извън сферата на неговата компетентност, очертана от Конституцията на Република България. Множество специални закони възлагат на областния управител несвойствените функции, които по-скоро го определят като „администрация", която подпомага осъществяването на правомощията на централните органи на изпълнителната власт. Това определено не съответства на конституционния статут на областния управител. Прегледът на правомощията на областния управител показва, че е необходимо да се оцени съществуващата законодателна уредба от гледна точка на това правомощията и отговорностите им да бъдат приведени в съответствие с логиката на управленската дейност. Съществуват сектори, при които на областните управители са възложени функции във всички етапи по разработването и реализирането на съответната политика-координацията, изпълнението, контрола. В други случаи на областния управител са възложени едновременно изпълнението и контрола.

Наблюдават се сериозни проблеми при взаимодействието на областния управител с териториалните звена на централната изпълнителна власт като:

- Несистемна и некоординирана дейност на областните управители и териториалните звена при решаването на регионални задачи;
- Некоординирани секторни политики на областно ниво;
- Невъзможност на областния управител да изпълнява правомощията си по координация, поради това, че териториалните звена са вертикално обвързани и йерархично подчинени на министерствата и агенциите;
- Липса на механизми, осигуряващи взаимодействието и координацията между областния управител и териториалните звена [4].

Областната администрация подпомага областния управител в осъществяването на неговите правомощия. Тя е юридическо лице на бюджетна издръжка със седалище – населено място, административен център на областта. Според характера на дейността, която извършват, административните звена в областната администрация са обособени в обща и специализирана администрация. Общата администрация осигурява технически дейността на областния управител, а специализираната администрация и дейността по административното обслужване на гражданите и юридическите лица. Специализираната

администрация подпомага и осигурява осъществяването на правомощията на областния управител. Областният управител може да създава по необходимост към дирекциите от общата и специализираната администрация отдели, а към тях сектори. Административното ръководство в областната администрация се осъществява от главен секретар, който се назначава от областния управител за срок от пет години. В областните администрации се създават и политически кабинети, в които се включват заместник-областните управители и началниците на звената за връзки с обществеността.

Гражданско общество

Поради това, че когато се взимат решения от местните органи на самоуправление често се засягат интересите на гражданите, от 1 януари 2004 г. в България влиза в сила Законът за омбудсмана, който урежда правното положение, организацията и дейността на омбудсмана.

Омбудсманът се застъпва с предвидените в този закон средства, когато с действие или бездействие се засягат или нарушават правата на свободните граждани от държавните и общинските органи и техните администрации, както и от лицата, на които е възложено да предоставят обществени услуги, както и от частноправни субекти.

Омбудсманът осъществява дейността си въз основа на правилник за организацията и дейността му. Правилникът се изготвя от омбудсмана, одобрява се с решение от Народното събрание и се обнародва в "Държавен вестник".

Дейността на омбудсмана е публична като в работата си се подпомага в от заместник-омбудсман.

Омбудсманът се избира от Народното събрание в условията на публичност и прозрачност за срок 5 години и може да бъде преизбиран на същата длъжност само за още един мандат.

В своята дейност, той е независим и се подчинява само на Конституцията, законите и ратифицираните международни договори, по които Република България е страна, като се ръководи от личните си съвест и морал. За омбудсман се избира български гражданин с висше образование, който притежава високи морални качества и отговаря на условията за избор на народен представител.

Дейността му се изразява в това, че той:

1. Приема и разглежда жалби и сигнали за нарушения на права и свободи от държавните и общински органи и техните администрации, както и от лицата, на които е възложено да предоставят обществени услуги.

2. Прави проверки по постъпилите жалби и сигнали.

3. Отговаря писмено на лицето, което го е сезирало в едномесечен срок, а ако случаят изисква по-обстойна проверка, този срок е три месеца.

4. Посредничи между административните органи и засегнатите лица за преодоляване на допуснатите нарушения и примирява позициите им [2].

В последно време в България започна формирането на т. нар. гражданско общество. Това ще рече, че гражданите започват да взимат пряко участие в местното самоуправление и формите за това са регламентирани както в Конституцията на Република България, така и в специалния Закон за допитване до народа, приет през 1996г. [8].

За пълноценното и ползотворно участие на гражданите в местната власт са предвидени:

1. Референдуми – допитвания до населението на територията на общината.

2. Подписки и петиции на граждани.

3. Участие в дейността на неправителствените организации и др. [1].

Прякото участие на гражданите в местното самоуправление е свързано да голяма степен с личностната мотивация и личните интереси на съответния гражданин. То осигурява постоянен диалогов режим и обратна връзка в системата на управление. Това спомага за развитието на местната демокрация и усъвършенстване на самостоятелността на местните органи. Най-ефективно увеличаване на възможностите за активно участие на гражданите в процеса на формиране на общинска политика може да се постигне чрез неправителствените организации. Те могат да съдействат за повишаване на информираността на населението по отношение на техните права и задължения, както и да координират взаимоотношенията между местната изпълнителна власт и населението. Неправителствените организации са и основния фактор, благодарение на който се изгражда активно гражданско общество.

Прякото участие на обществеността в процеса на взимане на решения може да улесни местната власт. Така местната администрация получава повече информация, с което намалява риска от взимането на неправилни решения и прави местното управление по-ефективно.

Освен това за подобряване връзките на населението с местната администрация е необходимо да се подобри и обслужването на гражданите. Хората трябва да повярват, че публичната власт работи за тях, спазва законите и съблюдава интересите им. За да има добро управление е необходимо оптимално разпределение на отговорностите по предоставяните услуги между различните нива на управление. Необходимо е още и оптимизиране на процесите в администрацията, ангажиране на служителите с проблемите на хората. Предвижването на документите да става от администраторите, а не гражданите да биват препращани безцелно, от служба в служба. За да се гарантират перспективите на устойчиво развитие на местно ниво, за да се повиши качеството на живот е необходимо да се инвестират значителни усилия и в работата с младите хора, за да се привлекат към участие в укрепване на местното самоуправление. Стимулиране на духовното израстване и създаване на благоприятни условия за максимално задоволяване на разностранните интереси на младите хора [4].

3. Заключение

Състоянието и ефективността на държавното управление протича в контекста на живота на конкретното общество в различни сфери, свързано е с постигането на различни цели и затова дейността на държавата като организация включва осъществяването на различни функции. Така състоянието и капацитета на администрацията е образ на жизнеността на държавното управление. Важно значение за тази функционалност е състоянието и жизнеността на административните структури [7].

Изключително важно е да се разработи концепция за реформа на областното ниво на управление. Тя следва да включва: промени в съществуващото административно-териториално устройство на страната; засилване ролята на областния управител при осъществяване на ролята на държавата по места; легитимност на ръководните органи – в следствие на избирането или назначаването им. В същото време е необходимо да се ускорят действията по конкретизиране на правомощията, които да бъдат възложени на кметствата, да се предприемат системни действия за стимулиране участието на гражданите в местното самоуправление [4].

ЛИТЕРАТУРА:

[1] Закон за допитване до народа.

[2] Закон за омбудсмана.

[3] Закона за местното самоуправление и местната администрация.

[4] Нейкова М. Иновации и добро управление на местно ниво, БСУ, 2013, стр. 161.

[5] Нейкова М. Реформата на областно ниво на управление-устойчиво регионално и местно развитие, Юридически сборник, стр.100.

[6] Кузманов, З., Видове контрол – характеристики. Юридически сборник т. XXIII, БСУ, Център по юридически науки, Б., 2016, с., ISSN: 1311-3771.

[7] Петров К. Публичната администрация и доброто държавно управление, УНСС, 2011, Статия, www.money.bg.

[8] Христов, Хр., Граждански контрол на сектора за сигурност. Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2016, стр. 161-173.

Име на автора: преп. докторант Румяна Веселинова Василева
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: r.vasileva@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 255 - 258 Problems of Security Systems

REGIONAL PROJECTION ON CURRENCY WARS - THE THREAT FOR THE FINANCIAL SECURITY OF REPUBLIC OF BULGARIA

STANIMIR ST. STANEV

ABSTRACT: *This paper investigates the effects of so-called "currency wars" for the financial security of the Republic of Bulgaria under the currency board arrangement. The thesis defended is that this is a form of external threat to the financial security of the country, as the artificial devaluation of a certain currency against the Bulgarian lev or the euro creates a competitive advantage and directly affects the macroeconomic indicators in a negative aspect. The consequences have a serious impact on the financial interests, which are a key element of financial security.*

KEYWORDS: *Currency wars, financial security, financial interests, competitive devaluations.*

РЕГИОНАЛНА ПРОЕКЦИЯ НА ВАЛУТНИТЕ ВОЙНИ - ЗАПЛАХА ЗА ФИНАНСОВАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ*

СТАНИМИР СТ.СТАНЕВ

АБСТРАКТ: *В настоящия доклад се разглеждат ефектите от т.нар. „валутни войни“ за финансовата сигурност на Република България в условията на валутен борд. Тезата която се защитава е, че това е форма на външна заплаха за финансовата сигурност на страната, тъй като изкуственото девалвиране на определена валута спрямо българския лев или евро, създава конкурентно предимство и пряко влияе върху макроикономическите показатели в негативен аспект. Последствията имат сериозно въздействие върху финансовите интереси, които са ключов елемент на финансовата сигурност.*

1. Въведение

Функционирането на всяка държава е динамичен процес в търсене на непрекъсната адаптация и равновесие между вътрешни и външни фактори. Отсъствието на такова равновесие, поражда опасност от реализиране на заплахи за националната сигурност и появата на организационни, институционални, финансови и друг вид кризи.

В съвременните условия на функциониране на светът, финансите се явяват основните инструменти за формиране на геополитическият ландшафт и определят истинската „мощ“ на една държава в глобален мащаб. Тази доминанта в световното развитие, преориентира и разбирането за сигурността, като налага и допълнителни стандарти за актуалност и коректност.

Преосмислянето, задължително трябва да е насочено към ролята на икономическото развитие, проектирано през геополитическото статукво и възможностите за експлоатиране на предимства и формиране на финансов потенциал. Това поражда и нови заплахи за финансовата сигурност с висока степен на сложност и неопределеност, непосредствено корелирани със състоянието и проблемите на глобалната и регионалната икономическа среда. Днешните анализи по различни проблеми на сигурността, все по-често изтъкват икономически/финансови интереси, като причина за военни ескалации. Валутните войни,

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

като начин за придобиване на конкурентно предимство, станаха неизменна част от функционирането на международната финансова система. Последствията, до които водят имат сериозно въздействие върху финансовите интереси на всяка страна- особено ако е в условията на валутен борд.

Разглеждането на явлението "валутни войни", преминава с обяснение на самото понятие. Терминът сравнително отскоро е обект на дискусия в академичните среди, като преди това се намираше в обръщение, основно в заглавията на различни вестникарски публикации. Често се поставя и знак на равенство между „валутни войни“ и "конкурентна девалвация", поради факта, че все още няма добре изградена теоретична база, съчетана с необходимия статистически анализ, и в момента концепциите, на които се изгражда са предимно на малкия емпиричен опит. Аналитичното разглеждане на валутните войни, трябва да премине през уговорката за противоречието му сред политици, експерти и учени. Сред многото опити за дефиниране на понятието, два подхода съдържат същностната еманация и могат да се считат за достатъчно достоверни. Първия подход разглежда валутните войни, като дейности на централни банки или правителства, чиято цел е да задоволят своите национални интереси, чрез механизмите на валутния пазар най-често, чрез координирани парични интервенции и добавяне на ликвидност в системата. Втория подход разглежда това явление, като умишлена девалвация на собствена валута, за да се стимулира износа и съответно икономиката на страната за сметка на чуждестранните партньори. Съществува и краен подход, третиращ валутните войни, като първа фаза на поредица от събития, водещи до военен конфликт: валутни войни- явен протекционизъм-търговски войни- военни конфликти.

Терминът "валутна война" е използван за първи път от бразилския финансов министър Гуидо Мантега през септември 2010 г. в отговор на неконвенционалната парична политика на Федералният резерв - политиката на количествени облекчения.

Въпреки, че тази фраза е прилагана през последните 8 години към експанзионистичната парична политика от страна на Федералния резерв и други централни банки, това до известна степен е погрешна концепция. Същността на валутните войни е умишлена намеса на дадена страна, за да се обезцени собствената валута и с това да се окаже благоприятен ефект по салдото на търговския баланс. По-слабата валута в сравнение с търговските партньори може да помогне за увеличаване на износа, свиване на търговския дефицит и намаляване на разходите за лихвени плащания по текущи държавни дългове. Тази практика на изкуствено обезценяване на местната валута стана изключително актуална след силния икономически спад през 2008 г. и намаляването на световната търговия с 12% в края на 2009 г. Повечето от водещите икономики предприеха стъпки в изкуствена девалвация на валутите си, което формира условията за началото на валутни войни.

2. Изложение

Заплахите за финансовата сигурност, първоначално най-често се проявяват под формата на кризисни ситуации в отделни елементи на финансовата система. Възприемат се като негативна тенденция или явление, което се случва във вътрешния или външния контур на системата и не може потенциално да доведе до загуба на сигурност. На по-късен етап те еволюират, като активно целенасочено действие на субект или група от субекти, които целят постигането на конкретни политически или икономически резултати. Това ги поставя в различен ракурс от традиционните заплахи за сигурността на страната, като изисква коренно различен подход и механизъм на взаимодействие между държавните органи и структури.

Заплахата за финансовата сигурност на Република България от провеждането на валутни войни, идва най-вече от рязкото влошаване на показателите на външнотърговския баланс - валутния израз на разликата в стойността на всички изнесени или внесени стоки през границата на страната и конкретно износът на България за трети страни. Пасивното салдо по този баланс, ако няма компенсации от други източници, води до дефицит в платежния баланс, като покриването на този дефицит е за сметка на валутните резерви.

Критичното намаляване на валутните резерви, влошава финансовата стабилност и е предпоставка за атака по валутния курс, т.е. на практика се явява заплаха за финансовата сигурност на страната. Поради факта, че брутните валутни резерви на страната са ограничени, като временни решения възникват:

- Емитиране на нов външен дълг за попълване на брутните валутни резерви;
- Търсене на други външни източници за чуждестранни валутни ресурси;
- Въвеждане на административни ограничения за намаляване на изтичане на чуждестранна валута.

Задълбочаването на намаляването на валутните резерви, води до промяна на валутния курс и евентуално до промяна на валутния режим. Съпътстващата девалвация ще доведе до стопяване на спестяванията на населението и икономическите агенти, и по-важното – намалява оценката на местния труд на международния пазар.

Всичко това компрометира и финансовата независимост на държавата, ефективността и конкурентоспособността на финансово-кредитната система и нивото на защита на финансовите интереси. Това, неизменно ще доведе и до загуба на материална основа за гарантиране на финансовата сигурност във всички сфери на финансова дейност, а оттам и на вътрешно политическа и социалната стабилност.

Особено актуално проблемите, които възникват при воденето на валутни войни звучат през втората половина на 2018 г. Налице е ярко изразена конфронтация по осите на икономическо противопоставяне: САЩ-Китай, САЩ-ЕС и САЩ- Турция, съчетано с търговски ограничения и допълнителни мита.

Пряко засегната от тази конфронтацията се явява и България. Българския лев е фиксиран спрямо еврото. Всяка валута, която реализира конкурентно предимство спрямо еврото и страната е търговски партньор на България, бонифицира износа си.

Отражение на тези констатации се наблюдават през периода януари - август 2018 г. където по данни на НСИ[†]износът на стоки от България за трети страни намалява с 22.9% в сравнение със същия период на 2017 г. и е на стойност 10 167.6 млн. лева. Основни търговски партньори на България са Турция, Китай, Сърбия, Съединените американски щати, бившата югославска република Македония и Руската федерация, които формират 52.7% от износа за трети страни. Само през август 2018 г., износът на стоки от България за трети страни намалява с 21.0% спрямо същия месец на предходната година и е в размер на 1 312.6 млн. лева. Успоредно с това вносът на стоки в България от трети страни през периода януари - август 2018 г. се увеличава с 4.6% в сравнение със същия период на 2017 г. и е на стойност 14 622.5 млн. лева (по цени CIF). Най-голям е стойностният обем на стоките, внесени от Руската федерация, Турция, Китай и Сърбия. През август 2018 г. вносът на стоки в България от трети страни се увеличава с 10.9% спрямо същия месец на предходната година и е в размер на 2 000.6 млн. лева.

Всичко това, ясно проектира и от състоянието на текущата сметка за 2018г., където се наблюдава ярко изразен дефицит за първото и второто тримесечие на 2018г.[‡]

[†] http://www.nsi.bg
[‡] http://www.bnb.bg/bnbweb/groups/public/documents/bnb_download/s_macro_indicators_a1_pdf_bg.pdf

Четири от посочените шест страни, които се явяват основни търговски партньори на страната се считат, като най-често провеждащи интервенции на валутния пазар за обезценка на своята валута, което потвърждава ролята на валутните войни, като заплаха за финансовата сигурност на страната.

3. Заключение

Последиците от валутните войни са реални и предимно негативни - обезценяващи се валути, повишена инфлация, липса на стимули за спестяване и спадащ жизнен стандарт. Основната и главна задача на държавата е да гарантира определено равнище на финансова сигурност, като прогнозира, и елиминира с помощта на административно-политическите си лостове, и средства за въздействие, възникването, и развитието на различни заплахи, особено тези, които имат потенциал да разстроят финансовия фундамент и преосмислят финансовата независимост.

ЛИТЕРАТУРА:

[1] Неновски Н., К. Христов, Банковата система в условията на паричен съвет, ИПИ, С., 1999.

[2] Неновски Н., К. Христов и Б. Петров (1999), “Два подхода към кризите на фиксираните курсове”, БНБ, Дискусионни материали, бр. 4.

[3] Неновски Н. (1997), “Теоретични основи на системните финансови кризи”, сп. Икономическа мисъл, бр. 2, стр. 3 – 21..

[4] Манчев Цв. (2001), “Финансови кризи и преструктуриране на финансовата система – теория, национална и международна практика”, докторска дисертация, Софийски университет “Свети Климент Охридски”, София.

[5] Sharov O. Monetary and currency wars as a factor of threat to national economic security/O.M.Sharov/Strategic Priorities. – No. 3.– 2013

[6] Mishkin, F., Understanding Financial Crises: A Developing Country Perespective, NBER WP 5600 / 1997.

[7] The Economist. How to stop a currency war. October 14 2010. URL http://www.economist.com/node/17251850.

[8] M. Wolf. Currencies clash in new age of beggar-my neighbour. Financial Times, September 29 2010. URL http://www.ft.com/intl/cms/s/0/9fa5bd4a-cb2e-11df-95c0-00144feab49a.html#axzz2NSFRK3AK.

[9] The Economist. Phony currency wars. February 16 2013. URL http://www.economist.com/news/leaders/21571888-world-should-welcome-monetary-assertiveness-japan-and-america-phoney-currency-wars.

[10] Brahmbhatt, M., Canuto, O., & Ghosh, S. (2010). Currency Wars Yesterday and Today. World Bank,Washington, DC. World Bank. http://openknowledge.worldbank.org/handle/10986/ 10116.

Име на автора: д-р Станимир Станчев Станев
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: stanimirststanev@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 259 - 271 Problems of Security Systems

OUTLOOK AND OPPORTUNITIES FOR IMPROVEMENT OF PRIVATE SECURITY SERVICES IN BULGARIA

TATYANA M. IVANOVA

ABSTRACT: *Over the last decade, the private security business, although not recognized in its integrity in Bulgaria, is becoming more and more professional as a result of our EU membership and the sector's drive to deliver high-quality service. Considering the important role of private security services in today's society, it may only be in the interest of society as a whole to find adequate solutions to limit the losses attributable to all trading parties in this industry to acceptable levels and / or levels which provide alternative financial sources to cover losses. It is also obvious that in order to find a long-term solution to the issues of critical responsibility, caused by terrorist attacks or military action, some form of clear legal framework in the EU or Bulgaria is needed for different sectors.*

KEYWORDS: *Private security services, security sector reform, Bulgaria legislation, possibilities for improving.*

ПЕРСПЕКТИВИ И ВЪЗМОЖНОСТИ ЗА УСЪВЪРШЕНСТВАНЕ НА ЧАСТНИТЕ УСЛУГИ ЗА СИГУРНОСТ В БЪЛГАРИЯ

ТАТЯНА М.ИВАНОВА

АБСТРАКТ: *През последното десетилетие бизнеса на частните услуги за сигурност макар и не признат в целостта му в България става все по-професионален в резултат и на членството ни в ЕС и на стремежа на сектора за доставяне на висококачествена услуга. Зачитайки важната роля на частните услуги за сигурност в днешното общество, може да бъде само в интерес на обществото като цяло, да се намерят адекватни решения за ограничаване на загубите, "навлечени" върху всички търговски страни в тази индустрия до приемливи нива и/или нива които да осигуряват алтернативни финансови източници за покриване на загубите. Очевидно е също, че за да се намери дългосрочно решение на въпросите за критичната отговорност, резултат от терористични атаки или военни действия, е нужна някаква форма на ясна правна рамка в ЕС, респективно и в България за различните сектори.*

1. Въведение

Частни услуги за сигурност – понятие, което до преди 5-6 години звучеше „еретично“ и непознато за нашата икономическа и социална действителност. Като най изчерпателна и точна се приема все повече дефиницията на **Carlos Marti Sempere[1],** която гласи:„*Индустрията на сигурност се разбира като индустрията, която доставя продукти и услуги конкретно използвани от хората, за да се идентифицира, подготви, предотврати, защити, отговори, намали, облекчи и справи със заплахите и последствията, които нежелани събития имат за обществото. Тези последици могат да бъдат обобщени по отношение на увреждане на живота на хората, здравето, имущество или други активи, включително информацията“* .

Поради голямото разнообразие на заплахи за обществото, технологии и решения за сигурност, сектора за сигурност се състои от фирми с много разнообразна природа, които

[1]Martí Sempere 2010, p. 4.

понякога само използват термина „сигурност“. Частната индустрия за сигурност генерира продукти, както и услуги, които могат да включват брави и сейфове, пожар и алармени системи, електронни системи за контрол на достъпа, електронно оборудване за наблюдение, бронирани и защитени превозни средства, охрана ,оборудване и облекла, огради за сигурност, както и консултации за сигурност.

“Услугата е всяка дейност, която води до удовлетворяване на потребности и желания, свързани с размяната на стойности и не води до форма на собственост върху получената стойност в смисъл на придобиване на материален продукт”.

Прайд и Ферул[2] смятат, че “Услугата се определя като нематериално демонстриране и продукти, които са резултат от прилагане на човешки и механични услуги към хора или предмети”.

Според други, за една от услугите от сектора с която най често се олицетворяват всички услуги от него, а именно частната охранителна търговска услуга е всяка законно разрешена дейност, свързана със задоволяване на определени потребности и е разрешена чрез лицензиране и регистрация.

В административно-правен смисъл понятието “ЧОД”(частна охранителна дейност) се употребява не в смисъл на дейност на всички недържавни органи, а само на недържавните правоохранителни органи,– като една от проявените форми на дейност на недържавните правоохранителни органи. Дефинициите клонят да рефлектират към полицейските аспекти на услугите, макар че в дейностите, които те изброяват, част от тези услуги са включени в зоната, която трябва да бъде разглеждана като част от по-широката дефиниция за частните охранителни фирми (ЧОФ), подобно на наблюдението или частната детективска дейност. Други дефиниции, на които се набляга особено, че по-голяма част от задачите си ЧОФ правят за печалба /като противници да служат на публичните интереси/. Някои от дефинициите под черта са специфична част от услугите, които ЧОФ доставят, като охранителни услуги, технически услуги, видеонаблюдение, информационен и рисков анализ.

Изследователи поддържат мнението, че ЧОФ правят заедно само вътрешната сигурност и защита, като противоположна на външната сигурност, която е територия на държавните военни и частните военни компании.

През погледа на тези вариации на дефинициите за ЧОФ може да се дефинират като: неправителствени организации или група от организации ,които доставят политики и услуги за вътрешна сигурност за определени клиенти, правителството или частни лица и организации с цел търговска печалба.

Точната роля на компаниите от бранша на частите услуги за сигурност зависи от различни фактори.

Първият фактор е наскоро приетият *нео-либерален модел* за публичния сектор, включващ изграждането на квази-маркет, представянето на бизнес мениджърски техники, конкурентоспособни продукти и въвеждането в частния сектор на дейности, привични за публичния. Тази поява на нео-либералното правителство е важен фактор за нарастване на броя на опериращите компании в този сектор.

Вторият фактор е нивото на демократизация и на законодателството в страните на прехода. Много от европейските страни са с бивше минало характерно с друг икономически и социален строй и все още са в процес на осъществяване на болезнени политически и икономически реформи.Точно след смяната на режима държавните институции и правната рамка бяха реформирани из основи и бяха леко разклатени.

[2] ПРАЙД, Ферул: **Маркетинг: концепции и стратегии**, издателство Форком

Ролята на тези компании зависи и от вида на заплахата и рискът срещу обществото. Растежът на отрасъла може да се намери и във вида на предлаганите услуги. Гражданските частни охранителни компании се смятат от някои за основно осигуряване на нощни пазачи и охрана за контрол на достъпа, което много фирми все още правят.

На различни места обаче цивилните частни охранителни фирми предлагат много по-широк кръг от услуги. Те включват услуги, свързани с транзита на пари в брой, както и движението и оценката на други ценности. Те също така провеждат различни форми на поверителни разследвания, включително скрити и скрити разследвания и сложни разследвания на измами. Частните следователи също могат да се ангажират във фундаменталните разследвания на лица, считани за чувствителни позиции, като една мярка за защита на активи, инфраструктура и информация от кражби, злоупотреби или вреди.

Други услуги, предлагани от фирмите са:(включително използване на видеонаблюдение и скрити системи), събиране и разпространение на разузнавателни данни, както и мониторинг, инсталиране и реагиране на различни видове охранителни системи, включително осигуряване на телохранители и тясна защита, защита на свидетели, контрол на тълпата, въоръжена охрана за обекти за ядрена енергия, форми на аларми.Различните форми на техническа сигурност:консултации, включително контрамерки за промишлен шпионаж и проследяване и възстановяване на откраднати активи. възстановяване на откраднати активи.

Частните служби за сигурност обаче не са ясно дефинирани хомогенни групи и варират от държава в държава по отношение на вида на предоставяните услуги и използваната терминология.Нарастващата роля на частните служби за сигурност в гражданското общество прави още по-важно създаването на подходяща култура и правни структури, които да улеснят спазването на националните и международните правила и разпоредби, включително стандартите за правата на човека.

Предвид обширното регулиране и надзор на обществената полиция в повечето държави, би могло да се очаква, че подобни мерки за регулиране и надзор ще се появят за частната индустрия за сигурност.В много държави за съжаление бързите промени изпревариха реакциите на държавните регулаторни органи, което доведе до редица проблеми. Без ефективно регулиране, частният сектор често не се отчита пред обществото като цяло, а необявената частна индустрия за сигурност може да улесни нарушенията на правата на човека и организираната престъпност.

Ефективното регулиране както на частните охранителни фирми, така и на отделните работници помага да се осигури професионално ниво на обслужване, основано на стандарти и очертани оперативни правомощия, като по този начин се повиши безопасността на общността и предотвратяването на престъпления, като същевременно се установи отчетността на компаниите и работниците съответните държавни органи и обществеността.

2. Анализ и характеристики на нормативните рамки за сектора на частните услуги за сигурност в рамките на ЕС и България

2.1. Европа

На 22.11.2010г Европейската Комисия одобрява „Вътрешна стратегия за сигурност на ЕС[3] в действие” с 41 конкретни действия, които да бъдат извършени пред следващите 4 години.

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:BG:PDF

В тази връзка тогава комисарят по вътрешните работи на ЕС – Сесилия Малмстрьом заяви: „Сега ние предприемаме общ подход за това как да се отговори на заплахите за сигурността и предизвикателствата ”.

Стратегията обхваща пет сфери, като ЕК ясно припознава необходимостта от повече публично частно сътрудничество, от експертните оценки и подкрепа от частния сектор за справяне във въпросните пет сфери а именно: „Тези действия и изискват тясна координация със страните членки и следва да се въвличат публично –частните партньорства , там където е приложимо”

В доклада на Дирекция Предприятия и промишленост на Европейската Комисия относно „Проучване на конкурентоспособността на Секюрити индустрията[4] ” от 15 Ноември 2009г се казва,че:„По отношение на признати класификации на промишлените дейности, охранителната индустрия е нито добре определена, нито лесна за установяване”. В действителност, производство и доставка на свързани със сигурността оборудване и системи, услуги и приложения, могат да бъдат намерени в широк диапазон на индустрията и услугите позиции, които обхващат както не-сигурността и сигурността на свързаните с това дейности.

В контекста на европейската външна политика ЕС е наясно, че частните компании от сферата на частните услуги за сигурност са част от системата за сигурност на отделните държави. Пак в същия доклад в анализа на авторите е разписана отделна глава, свързана със саморегулацията на бранша на частните услуги за сигурност в контекста на политиките на ЕС.

Саморегулацията се среща в различни форми и може да се види в индустрията или на ниво компания. Тя препоръчва да се ползват формите на ръководствата или наръчниците или етичните кодове, които полагат минималните стандарти на поведение за служителите. Саморегулацията се стреми да постигне повечето от заложеното в държавните наредби, и тези опити налагат да се прилага сигурен контрол за тези специфични дейности.

Спектърът на предоставяните от ЧОФ услуги е много широк, вариращ от логистични услуги до частни охранителни дружества които предоставят също така жизненоважни услуги в самите държави членки, като управление на затвори и патрулна охрана на инфраструктурни обекти; ЧОФ са били използвани в граждански и военни мисии в рамките на Общата политика за сигурност и отбрана (ОПСО) за охрана на делегации на ЕС;

Но като има предвид, че за да се възползват от предимствата, предлагани от ЧОФ, и за да се гарантира, че те могат да бъдат подведени под отговорност, на международно равнище следва да бъде въведена правна рамка с обвързващи механизми за регулиране и наблюдение, за да се регулира тяхното използване и да се осигури достатъчен контрол на дейността им още повече като има предвид, че частните охранителни дружества (ЧОД) са част от една промишленост, която е с подчертан транснационален характер и в която са замесени правителствени и междуправителствени участници, и като такава изисква цялостен подход към регулирането.

В сегашното регулаторно положение в този сектор се включват редица противоречиви правила, които варират значително в различните държави членки; предвид, че разнородните национални законодателства и възприетите от някои ЧОД правила за саморегулиране оказват слаб възпиращ ефект за предотвратяването на

[4] Проучване ЕК

злоупотреби, липсата на наказания, и могат да имат значително въздействие върху начините, по които ЧОД оперират.

Всичко това при наличието на факта че липсва одобрено определение за ЧОД, и в контекста на това, че услугите в областта на сигурността могат да бъдат определени като въоръжена охрана или защита на сгради, съоръжения, собственост и хора, всякакъв вид трансфер на знания с приложение в областта на сигурността и дейността на полицията, развитие и прилагане на информационни мерки за сигурност и други свързани дейности. По данни на ЕК, приблизителната стойност на пазара на продукти и технологии в областта на **сигурността на ЕС е между 26 и 36,5 милиарда EUR.**

Вътрешният пазар на ЕС обаче е силно фрагментиран, разделен от границите между държавите или дори между регионите. Като една от най-чувствителните области на политиката, сигурността е една от областите, в които държавите членки не са склонни да се откажат от националните си прерогативи.

Ето защо Европейската комисия[5] предложи програма за действие за укрепване на европейския отрасъл на сигурността. Заместник-председателят на Европейската комисия Антонио Таяни от предходният мандат на комисията , отговарящ за промишлеността и предприемачеството, заявява: „Настоящият фрагментиран пазар подронва конкурентоспособността на европейския отрасъл на сигурността. Липсата на „марка на ЕС“ е особено сериозен проблем, тъй като бъдещите ключови пазари на технологии в областта на сигурността няма да се намират в Европа, а в бързо развиващите се страни.“

По-специално, Комисията предлага следните мерки за създаване на истински вътрешен пазар за отрасъла на сигурността:

Приоритетът ще бъде преодоляването на фрагментираността на пазара на продукти и технологии в областта на сигурността на ЕС чрез хармонизиране на стандартите и процедурите за сертифициране на технологиите в областта на сигурността. На европейските организации по стандартизация ще бъде възложено да установят конкретни и подробни пътни карти относно следващото поколение технологии.

За да се преодолее фрагментираността на европейския вътрешен пазар, трябва да се предприеме следното:

Хоризонтално сътрудничество и координация в областта на сигурността, както в рамките на ЕС, така и между неговите институции и агенции, за да се гарантира пълната оперативна съвместимост на продуктите и процедурите, в съчетание с вертикална координация между различните равнища на действие;

Съвместно изготвяне на предвиждания, с цел определяне на обща споделена визия;

Система за управление, която включва публичния и частния сектор.

Необходимо е да се наблегне на по-доброто използване на полезните взаимодействия между (гражданската) сигурност и научните изследвания в областта на отбраната.

В препоръките от Наръчника към доклада на Женевския център за демократичен контрол на въоръжените сили („Наръчник за начало на реформа в секюрити сектора „Регулиране действията на частните охранителни фирми – състояние и перспективи”) в частта му, касаеща ЧОФ, се казва: „Законодателството[6] трябва да създаде система за лицензиране, която ясно определя вида на службите за сигурност, които могат да бъдат осигурени и които определят отношенията между и функции на частните доставчици на

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0233

[6] Recommendations for the regulation of domestic PMSC services within the CE p 35

сигурността и държавни такива. Освен това, съвместните работни споразумения между публичните и частните доставчици на услуги за сигурност могат да подобрят координацията и осигуряване на яснота в области като участието на частния сектор в областта на правоприлагането или други действия, процедури за докладване в полицията, както и ролята на полицията в прилагане на законодателството за частната охранителна дейност.“

За изпълнението на планираните от комисията мерки се явяват и предизвикателства които могат да бъдат обобщени като:

Съпротива от индустрията срещу промяната

В по-нерегулирана среда частните доставчици на услуги за сигурност и клиентски групи могат да имат силен икономически и политически интереси, които може да се компрометират с усилията за реформиране на сектора. Например, промяната може да бъде особено трудна, когато доставчиците са силни организации с организираната престъпност и политическите партии. Дори и при тези обстоятелства, е вероятно, че други фирми ще се възползват от подобрените регулиране и контрол, например, когато това би засилило тяхната легитимност. Важно е да се идентифицират онези компании, които ще се възползват от промяната, и да им се помага, например, организиране на частни сдружения за сигурност при търговия и при решаването на конфликтите на интереси и конкуренцията.

Точките на пресичане на държавния сектор и частните доставчици на услугите за сигурност

Разбиране на връзката между правителството и частния сектор за сигурност, и идентифициране на потенциални конфликти на интереси, са от изключително значение за развитието на програмите за реформи. Това не е нещо нечувано за висши държавни служители (включително тези, които отговарят за предоставяне на държавни търгове), да бъдат членове на борда на директорите на конкретни частни доставчици на сигурност, създаване на условия за корупция и злоупотреба с власт. Размиването на границите между доставчиците на полиция и частна охрана може да създаде конфликт на интереси, по-специално доставчиците на обществена сигурност обикновено са основен орган за прилагане правилата за частния сектор. Например, в една нерегулирана среда, е типично за полицейските служители да работят за търговски дружества за защита, когато са дежурни, като понякога използват от държавата издадено оръжие, или за частни и обществени доставчици на сигурност, за да се конкурират за договори или за персонала. Конфликтът на интереси може да възникне в рамките на големи компании, за които осигуряването на частна охранителна компания е един интерес от страна на много или е свързана с друга основна дейност бизнеса. Големите компании, които иначе са законни, като банки, могат да имат вътрешни разделения за сигурност, които съществуват, без правно основание.

Важно е да се изяснят ролите и отговорностите на обществени и частни доставчици на сигурността чрез националното законодателство и да се гарантира, че регулациите и лицензионните процедури се прилагат към дружества с вътрешни разделения за сигурност.

Частната сигурност като обществено благо

Разширяването на частна охранителна дейност предоставянето на разположение на тези, които могат да си позволят - това може да подкопае представата, че сигурността е обществено благо, и да попречи на достъпа на сигурността за бедните. Голямо предизвикателство е регулирането на сектора, така че да не се състезава със или да се приема за заместител на ролята на държавата в защита на обществото, а по-скоро го

допълва и освобождава публичните ресурси, които могат да бъдат използвани за подобряване на предоставянето на услуги за сигурност.

Частната индустрия за сигурност не е единна

За разлика от публично еквивалентния сектор, частната индустрия за сигурност се състои от множество отделни предприятия, които се състезават един срещу друг, за да предоставят на клиентите с най-различни услуги. Дори там, където търговските сдружения съществуват, те не могат в действителност да диктуват поведението на своите членове и съществуват толкова, за да защитават интересите на членовете си да управляват развитие на доброволни кодекси за поведение.

Такъв начин на развитие на разпространение на механизми или наръчници например не са само добавки към професионализма в сектора, но показват че неговото демократично управление е добро.

На базата на това в Становище ЕИКС[7] описва сектора на Европейско ниво като :

Сектора на частните услуги за сигурност на Европейско ниво е силно фрагментиран, разделен от националните граници на страните-членки на съюза. Мерките и технологиите в областта на сигурността могат да оказват въздействие върху основните права и свободи на хората, и често предизвикват страх от евентуално нарушаване на правото на личния живот .

Институционален пазар – купувачите са публични органи . Дори в области , които пазарът е с търговски характер, изискванията за сигурност продължават в голяма степен да се определят от законодателството .

Пазар със силно обществено измерение : сигурността е една от основните човешки потребности ; същевременно, тя е и високочувствителна област . Мерките и технологиите в областта на сигурността могат да оказват въздействие върху основните права и често предизвикват страх от евентуално нарушаване на правото на личния живот .

Оценката на услугите, предоставяни от ЧОД, се възпрепятства от липсата на последователност при докладването относно тяхното използване както от институциите на ЕС, така и правителствата на държавите членки; това само по себе си би трябвало да се дефинира като политика чрез която да се насърчават държавите членки и институциите на ЕС да предоставят въпросната информация по по-последователен и по-прозрачен начин, за да се даде възможност за правилна оценка на използването на ЧОД от съответните бюджетни органи и независими одитори; която да препоръчва активния ангажимент на парламентите и на недържавни участници в необходимите процеси на оценка, които са от решаващо значение за регулирането и надзора на този сектор.

Дейностите по анализиране и опитите по въвеждането на регулиране за ЧОД е в ход на много международни форуми, включително Форума за **Документа[8] от Монтрьо**, като ЕС беше избран в групата „Приятели на председателя“, като има предвид междуправителствената работна група с безсрочен мандат, създадена да разгледа възможността за изготвяне на международна регулаторна рамка относно регулирането, наблюдението и надзора на дейностите на частните военни и охранителни дружества, както и като има предвид, че Документът от Монтрьо е първият значим документ, в който се определят аспектите на прилагането на международното право към ЧОД; Другият значим документ е **Международният кодекс на поведение за частните доставчици на услуги в областта на сигурността** (ICoCA) определящ стандарти за отрасъла и все

[7] European Economic and Social Committee Security Industrial Policy Action Plan for an innovative and competitive Security Industry /* SWD/2012/0233 final */

[8] document de Montreux

повече се превръщащ се в инструмент за гарантиране на общи основни стандарти за този отрасъл в световен мащаб. Той е разработен от Асоциацията за ICoCA[9], която има за цел да насърчава, ръководи и контролира прилагането на ICoC и да стимулира отговорното предоставяне на охранителни услуги, както и спазването на правата на човека и на националното и международното право. Все пак трябва да се има предвид, че присъединяването към ICoC, която е неправителствена организация, регистрирана в Европа, в частна полза, става доброволно и срещу заплащане, като високите такси за членство не позволяват на всички ЧОД да станат членове на Асоциацията за Международния кодекс на поведение, от където произтичат и последствия касаещи оценката при контрола по спазването на кодекса и обективността и.

Комисията би трябвало да изготви „Зелена“ книга с цел привличане на всички заинтересовани страни от публичния и частния сектор на сигурността за широки консултации и обсъждане на процесите, за по-ефективно идентифициране на възможностите за пряко сътрудничество и за създаване на основен набор от правила за участие и добри практики; както и създаването на секторно специфични стандарти за качество на ЕС;

Но за да се определи обхвата на дейностите би ***трябвало определението за ЧОД да бъде изяснено, преди въвеждането на ефективно регулиране на тяхната дейност,*** тъй като липсата на такова определение може да създаде *„вратички“* в законодателството.

SWOT Анализ

СИЛНИ СТРАНИ

• Европа е дом на водещите световни частни компании в сектора на частните услуги за сигурност.

• Професионализацията: значителни инвестиции на частните услуги за сигурност - Фирмите са инвестирали значително количество усилия в разработването на схеми за качество и програми за обучение с цел повишаване на качеството на услугите за сигурност

СЛАБИ СТРАНИ

• Фрагментация на пазара на Секторът на частните услуги в ЕС произтичаща от различните национални подходи, законодателство и регулаторни среди за услугите за сигурност.

• Разпокъсаността също така предполага, че качеството на предоставяните услуги и оперативните разходи могат да се различават значително в отделните държави-членки.

• Ниски нива на заплатите и често нерегламентираното заплащане както и лошите условия на труд.

ПРЕДИЗВИКАТЕЛСТВА

• Готовност на клиентите да си да платят цена, която отразява на качеството на услугата и подходящо възнаграждение, отразяваща условията на труд на персонала по сигурността.

Икономическите условия: повишен натиск за спестяване на разходи по предоставяне на услугата.

• Условия за възлагане на поръчки: насърчаване на лоялната конкуренция както и "най-добрата стойност" подходи в ценовия задвижва пазара.

• Демографските промени / работна сила: трудности при набирането и задържането на служители / голямото текучество на персонал.

[9] ICoCA

• Професионализация на сектора: например професионално обучение и кариерно развитие.

• Обществените нагласи и правна рамка: особено по отношение на възможностите за засилване на ролята на частни услуги за сигурност в чувствителни области (напр. критичната инфраструктура и транспорт).

ВЪЗМОЖНОСТИ:

• Повишено усещане за несигурност: води до увеличаване на търсенето на сигурност в области, където несигурността расте.

• По-големи заплахи и рискове за сигурността:

геополитическите нива (местно, национално, международно) и от различни източници (престъпност, тероризма и т.н.)

• Демографски и социални развития: въздействие върху изискванията за сигурност: застаряващо население, индивидуализация на обществото, миграционни потоци и т.н. В съчетание с новите проблеми на сигурността от социални промени (например промишлено / икономическо преструктуриране,урбанизацията, новите видове престъпност, и т.н.)

• Пазарен растеж: намаляване на обществената / капацитета на полицията (напр. за публичните финанси ограничения) водещо до аутсорсинг и развитие на публично-частните партньорства за осигуряване на сигурността. Специфични сегменти на клиенти (например болници, училища, обществен транспорт и т.н.)

• Интернационализация/глобализацията : трансгранично предоставяне и установяване в рамките на единния пазар; желание на клиента за предоставяне на услуги на множество държави.Аспектите на устойчивостта и околната среда: нарастващото приемане на подхода на жизнения цикъл (например щадящи околната среда продукти, рециклиране, ниско потребление на енергия, ниска консумация на вода и т.н.)

• Специализация: повишаване на предоставянето на специализирани услуги за сигурност предоставя възможности за разширяване на пазара (т.е. по-голяма възможност за изнасяне на функции за сигурност)

2.2 БЪЛГАРИЯ

Към момента фактологическата обстановка за бранша за услугите за сигурност показва, че необходимостта да се направи такова ясно разписване на обхвата на бранша и оформянето му като отделен бранш услуги със специфични условия и отговорности и законодателна рамка е все по належаща. Състоянието е такова ,че от законодателна гледна точка за отделните дейности от бранша има отделни законови и подзаконови нормативни актове и още множество препратки към релевантни такива.

Частните услуги за сигурност по своята същност представляват съвкупност от материално-правни норми, които уреждат обществени отношения в сферата на изграждащото се гражданско общество. Проявява се като част от изграждащото се гражданско общество и би трябвало да е лоялна конкуренция в условията на пазарната икономика.

Секторът „Дейности по охрана и разследване “ е всъщност сектор ,който обхваща в себе си дейности които сами по себе си са в различни икономически дейности или пък са в обхвата на други такива като спомагателни .Към момента в Р. България има над 400 частни охранителни компании, осигуряващи услугата частна охранителна дейност. По данни на НСИ в тях са заети над 70 000[10] служители. Все по-осезателното организиране в този бизнес подпомага по-нататъшното утвърждаване на неговата легитимност.Но това не

[10] Данните са от НСИ и се отнасят само за ЧОФ код 80.10 и код 80.20 съгласно НКИД за 2014г

е коректната форма, предвид факта, че под определението частни услуги за сигурност би трябвало съвсем резонно да се погледнат и – проектиращите и изграждащите системи за сигурност, пожароизвестяване и пожарогасене, CCTV, мониторинг центровете, служителите по сигурността на информацията, GPS центровете и целия спектър от тези специфични услуги.

Видно от класификацията по НКИД, няма ясна и точна категоризация на дейностите, попадащи под сигнатурата „частни услуги сигурност“.

Те са разпръснати в различни сфери на икономически дейности, като това само по себе си води до деформираност и невъзможност за ползване на официална статистическа информация за развитието на бранша

Необходимостта от реформи и от дефиниране на сектора е крайно належаща

Състоянието на сектора към момента на анализа– недефиниран сектор, разпилян по различни икономически дейности, с липсваща и частична нормативна уредба и поради тази причина с невъзможност да се създаде основна емпирична база за изследването му от статистическа гледна точка.

Към момента кратката хронология на сектора свързани нормативна уредба по години и развитие на частната охранителна дейност като основен подсектор, на който се базира развитието на останалите подсектори:

1989 - 1993 – характерен с отсъствие на правна регламентация;

1993 - 1997 – текстове в отделни закони и подзаконови нормативни актове;

1997 - 2000 – единствено наредба за извършване на ЧОД;

2004 - приемане на Закона за частната охранителна дейност (ЗЧОД);

2004 - 2011 – ЗЧОД няколкократно претърпява незначителни промени в същността си – част от тях са свързани със съпътстващото законодателство в страната;

2011 – промени в ЗЧОД свързани с изискванията след приемането ни за член на ЕС и постановките на ДФЕС;

Нормативна уредба пряко или косвено влияеща върху част от подсекторите от Сектор Частни услуги за сигурност, а именно частна охранителна дейност и съпътстващи я дейности се изразява в:

Основния Закон - Конституцията на Р. България;

Търговски Закон;

Закон за частната охранителна дейност;

Закон за дейностите по предоставяне на услуги;

Закон за оръжията боеприпасите взривните вещества и пиротехническите изделия (ЗОВВПИ);

Закон за опазване на обществения ред при провеждане на спортни мероприятия;

Закон за обществените поръчки;

Закон за движението по пътищата;

Наредба № Із-2895 от 15.11.2011 г., издадена от МВР и МИЕТ;

Наредба I-121 от 24.06.2004 г. за реда за организиране на охраната при транспортиране на ценни пратки и товари, МВР и БНБ;

Наредба № Із-575 от 02.03.2011 г. за условията и реда за провеждане на курсове за безопасно боравене с огнестрелно оръжие, издадена МВР;

Наредба I-171 от 02.07.2001 г. за организацията и контрола по обезпечаването на сигурността на банките и небанковите финансови институции, издадена от министъра на вътрешните работи и управителя на БНБ;

Наредба № 9 от 04.12.2006 г. за придобиване на квалификация по професия "Охранител", издадена от министъра на образованието и науката;

Наредба № 7 от 2016 г. за системите за физическа защита на строежите, издадена от министъра на регионалното развитие и благоустройството;

Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценката на риска за тях, приета с ПМС № 256 от 17.10.2012 Сектора ДОР (или ако се съобразим с описаното в изключенията от Директивата за услугите чл. 2 параграф 2 буква „к“ то сектора трябва да е „частни услуги за сигурност“) и в него трябва да се включат следните подсектори:

- Посочените в сега действащия Закон за частната охранителна дейност в чл.5 услуги;
- Дейностите свързани с охраната с технически средства , в това число мониторинг центровете, реакция на сигнали, верификация на сигналите, автопатрули;
- Проектиране и изграждане на системи за сигурност, видеонаблюдение, пожароизвестяване и пожарогасене;
- Дейности по пожароизвестяване и пожарогасене;
- Консултанти по сигурността;
- Дейности по разследване.

Към момента всички останали съпътстващи дейности са „невидими“. Те са включени или в други икономически дейности (като консултантите по сигурността например) или са спомагателни за частните охранителни фирми. Първия опит за регламентация на тази непозната както за обществото така и за институциите дейност е направен през 1993г с включването в тогавашният ЗМВР на чл.81, съдържащ кратко определение за дейността на ЧОФ. Няколко години след това излиза първият реален акт (макар и под законов) касаещ пряко Частната Охранителна дейност- Наредба I-79 на МВР/08.06.00г.

С течение на времето както от страна на МВР така и на бизнеса се установява че Наредбата все повече не отговаря на реалностите и изискванията на бизнеса вече са на друго ниво и МВР предприема следваща стъпка Наредба I-14 за ЧОД.

До месец февруари 2004г бизнеса работи по нея – тогава се приема Закона за Частна Охранителна дейност. Към момента единственият ясен регулаторен режим, като изключим изискването дружествата да са регистрирани по Търговския закон, е само лицензионният режим за извършване на частната охранителна дейност. И за него може да се каже, че е непълен, предвид факта, че в по-голямата си част е ориентиран към физическата охрана и охрана на имуществото. Всички останали дейности не са обхванати от законови критерии. Това може да доведе до парадокс от типа: регистрирано по Търговския закон дружество да има мониторинг център с над 1000 точки и същевременно да не извършва частна охранителна дейност, защото той само наблюдава и приема сигналите. За това не се изисква лиценз за частна охранителна дейност. Друг е въпросът, дали ако има сигнал за аларма, той, например, няма да има договор с възложителя да му звъни по телефон или да го уведоми по друг начин. На практика, тази дейност не е регламентирана под никаква форма. Тя се води „спомагателна”, а в днешно време почти няма охранителна фирма без мониторинг център. Друг парадокс е изискването компаниите, които проектират, изграждат и инсталират системи за сигурност, да са регистрирани в Камарата на строителите в България и в Камарата на архитектите и проектантите в инвестиционното проектиране. Това са компании, които не се занимават само със строителство и ел. инсталации, а са компании, които работят специфична работа, свързана с обезпечаването на сигурността на работата на системите за сигурност и в последствие на частната охранителна компания, която ще поеме този обект за охрана. Като допълнение възниква и въпросът с квалификацията, изискванията към лицата,

опериращи в този сектор, както и конфиденциалността на поверената им информация. На практика, това са хората, които знаят в детайли, както разположението на системата, така и обекта, и собственика, и какво точно ще обезпечава системата.

В съвременните условия на частните охранители се възлагат основни функции както по профилактиката, така и по охраната на имущество, лица, мероприятия, ценни пратки и товари и самоохрана. С определянето на предмета на дейност се поставя декларативна основа на ЗЧОД. Обикновено функциите определят задачите, но при частната охранителна дейност, с оглед договорното начало, задачите, поставени на частните охранителни търговски дружества от възложителя, са основата за конкретизиране на функциите, които тя ще реализира. В практиката, наличните финансови средства или липсата им в повечето случаи, значително ограничават структурните и функционалните задачи с цената на по-малки или по-големи компромиси. Задачите и функциите на частната охранителна дейност са изцяло продиктувани от целите и конкретно формулирани от спецификата на охранявания обект и договорните отношения между възложителя и изпълнителя в лицето на охраняващото търговско дружество. За да се очертае още по-ясно предметът на ЗЧОД, е необходимо изясняването на конкретно допустимите способи за противодействие на противоправните посегателства, които могат да бъдат предупредителният способ е един от основно използваните чрез създаване на представа за сигурен и надежден режим на охрана. Това се постига чрез предотвратяването на опитите за посегателство, както и със силното своевременно противопоставяне и последващо разпространяване на информацията за това. Към предупредителния способ за противодействие се отнася създаването на работещ пропускателен режим за охрана на обекта и аналитичният способ на противодействие на престъпните посегателства състоящ се в постоянно събиране на информация за организираната престъпност и за собственото състояние на режима на частната охрана. Не се изключва взаимният обмен на информация между държавните и частните охранителни структури. Законът за частната охранителна дейност е в сила повече от 10 години. Неговото приложение обаче повдига множество въпроси, които не са уредени в закона или, макар да са уредени, тяхната уредба е крайно незадоволителна.

Философията на закона, за огромно съжаление е морално остаряла – тя се базира на опита на органите на държавната власт през 90-те години на XX в., като този опит предполага приемането на този наистина рестриктивен (от стопанска и икономическа гледна точка) закон.

Законодателят така и не е отчел, че обществените отношения през тези близо 10 години са се променили коренно и от един бизнес, който е трябвало да бъде контролиран строго, ЧОД се е превърнала в нещо доста по-различно – в икономическа дейност, в която са заети над 100 000 човека (по неофициални данни – за съжаление не се води официална статистика на лицата, които са заети в бранша „Частни услуги за сигурност”), в която вече има професионализъм и принципи. Точно заради това ЗЧОД е морално остарял закон, който следва да бъде отменен и на негово място да бъде приет нов, актуален със новите социални и икономически изисквания закон, който да очертае пътя за развитие на бранша.

3. Проблеми и предложения за решения. Пътна карта за реформа в сектора на частните услуги за сигурност.

Изводи [11]**:**България[12] – сектора все още не е започнал процеса по реформа ,независимо от неговото силно развитие както като икономическа дейност, така и като

[11] За нуждите на доклада е направено ограничение в периода на изследването на законодателството до 2016г.

заетост и като се има предвид че той се явява основен партньор в сферата на сигурността на държавните органи. Липсва дефиниране и определяне сферите и случаите на секторно самоуправление, на съвместни пълномощия на държавните и браншовите структури и на еднолично държавно администриране в индустрията.

Прекомерни неясни регулации в свързано законодателство и подзаконови нормативни актове, създаващо условия за „сив „сектор, неспазване на пазарни и законови изисквания. Основните репери за реформата в сектора са:

Първо – ясно очертаване на услугите попадащи под тази сигнатура; към момента те не са описани като терминология , което от своя страна води до разпиляване на компаниите и невъзможността им да бъдат обединени в браншови организации и да бъдат представлявани , идентифицирани и защитавани.

Второ – създаване на законодателна база, след анализ на нормативната налична, свързваща и обединяваща определени сигнатури; За отделните направления и бизнес дейности има различни нормативни и поднормативни актове, които понякога водят до противоречиви тълкувания и не са функционални.

Трето – създаване на условия за бизнес и изисквания към лицата оперирящи в този бранш; Липсата на такива от своя страна води до нарушена бизнес среда, нарушено качество на услугите, нарушен контрол и последици.

Четвърто – Улесняване на организацията за взаимодействие и контрол на сектора както помежду си така и със съответните отговорни институции.

Пето – създаване на условия за плавен преход към единна регулация в сектора - след определянето на неговия обхват и терминология.

ЛИТЕРАТУРА:

[1] Martí Sempere 2010, p.

[2] ПРАЙД, Ферул: Маркетинг: концепции и стратегии, издателство Форком

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:BG:PDF;

[4] Проучване ЕК

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0233

[6] Recommendations for the regulation of domestic PMSC services within the CE p 35;

[7] European Economic and Social Committee Security Industrial Policy Action Plan for an innovative and competitive Security Industry /* SWD/2012/0233 final */

[8] document de Montreux

[9] ICoCA

[10] Данните са от НСИ и се отнасят само за ЧОФ код 80.10 и код 80.20 съгласно НКИД за 2014г

[11] За нуждите на доклада е направено ограничение в периода на изследването на законодателството до 2016г.

[12] БСК Секторен анализ на дейности по „Охрана и разследване“ съавтор: Татяна Иванова

Име на автора: докторант Татяна М. Иванова
Месторабота: Военна академия „ Г. С. Раковски“, факултет „Национална сигурност и отбрана“ и Изпълнителен директор на Индустриален Клъстер „Сигурност“, София, Ул. Владайска 29.
E-mail: tatyanaivanov09@gmail.com

[12] БСК Секторен анализ на дейности по „Охрана и разследване“ съавтор: Татяна Иванова

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 272 - 284 Problems of Security Systems

ISLAMIC RELIGIOUS FUNDAMENTALISM AND EXTREMISM

TIHOMIR I. SOLAKOV, HRISTO A. HRISTOV

ABSTRACT: *In Bulgaria, there are real threats with the resulting national security risks of a lasting establishment of Islamic fundamentalism and radicalism, which require comprehensive, targeted and preventive measures to control, curb and prevent the activity being carried out, causing extremely serious consequences for the security of the state.*

KEYWORDS: *Islamic fundamentalism, religious extremism, intolerance, radicalism, hostility, reislamization, Muslim community, minorities, risk groups, national affiliation and national identity.*

ИСЛЯМСКИ РЕЛИГИОЗЕН ФУНДАМЕНТАЛИЗЪМ И ЕКСТРЕМИЗЪМ*

ТИХОМИР И. СОЛАКОВ, ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *В анализите на водещите мюсюлмански научно-изследователски центрове е посочено, че понятието „фундаментализъм“ произхожда от американско-евангелистката църква. В своите изследвания те акцентират върху процеса на проектиране на идеологията посредством влиянието на християнското общество в Северна Америка върху мюсюлманските общества на Изток. Западната наука и политика въздействат социално и политически върху ислямския свят, който възприема и адаптира идеята за фундаментализма в свой инструментариум*

1. Въведение

Религиозен фундаментализъм

Спорен е въпросът кога възниква фундаментализмът. Според изследователят Грахам фундаментализмът за пръв път се появява като термин в европейските анали през късното Средновековие, но неговата употреба остава ограничена[1]. В изследването си „Ислямската заплаха – мит или реалност“ Джон Експозито казва, че християнската интерпретация на термина „фундаментализъм“ ни отвежда към „движение в протестантството през XX век, което набляга на буквалното интерпретиране на Библията като основа на християнския живот и учение“[2].

Президентът на Библейския институт в Паскола Питър Рюкман характеризира фундаментализма като втора реформация, правейки аналогия с отхвърлянето на принципите на доминация на Светия престол във Ватикана в немските територии от Мартин Лутер и Томас Мюнцер[3].

Фундаментализмът изцяло е разгледан от Джефри Хайдън като продукт на североамериканската евангелистка традиция, определен като безпрецедентна религиозна виталност на американското общество от края на XIX век, което е и първопричината за появата му[4].

В анализите на водещите мюсюлмански научно-изследователски центрове е посочено, че понятието „фундаментализъм“ произхожда от американско-евангелистката

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

църква. В своите изследвания те акцентират върху процеса на проектиране на идеологията посредством влиянието на християнското общество в Северна Америка върху мюсюлманските общества на Изток. Западната наука и политика въздействат социално и политически върху ислямския свят, който възприема и адаптира идеята за фундаментализма в свой инструментариум. Например в анализите на пакистанската „Джаамат ал ислами“ се изтъква фактът, че САЩ не трябва да обвиняват ислямския свят за развитието на фундаментализма, тъй като тази радикална политическа доктрина с теоцентристки произход се формира именно в американската политическа мисъл[5].

В световната енциклопедична литература се налагат няколко типа определения на понятието „фундаментализъм“:

-В справочника Рандом Хаус е дадена следната дефиниция: „Протестантско движение, което поставя акцент върху непогрешимостта на Библията в областта на вярата.“

-Авторите на Уебстер дефинират феномена като: „Движение или поведение, което възприема като императив стриктното придържане към множество базисни принципи.“

Двете дефиниции реално маркират развитието на фундаментализма в качеството му на политико-религиозна доктрина и модел на поведение, което бихме определили като средство за постигане на определени политически цели. Принципно фундаментализмът фокусира в себе си многопластова материя, в която се открояват две нива по отношение на политическата теория – едновременно средство и цел в множествеността на политическите парадигми[6].

В монографията си „Терор с разсъдъка на Господа. Глобалната поява на религиозно насилие“ Марк Юргенмайер се базира на анализа за мотивацията на фундаменталистите като „религиозни терористи“, които са личности, притежаващи един необикновен недостатък, тъй като взимат твърде на сериозно религията[7].

Според Рутвен думата „фундаментализъм“ включва екстремизъм, сектарианизъм, идеологически пуританизъм. Макар много религиозни активисти (особено евангелистките движения в християнството и исляма) да вярват, че имат универсална мисия да трансформират или покръстят света, всички религии трябва да се изправят лице в лице с „проблемите на произхода си“ от малки църковни общества, срещу срамния факт, че спасители и пророци са мълвели божествени думи на определени езици и пред относително малки групи от хора на определени исторически кръстопътища. Религиозното многообразие и глобализацията са част от съвременността. Те предполагат избор, подхранвайки съмнението, че може да съществува повече от един път към Спасението (дори може би нерелигиозен път). Напливът на фундаменталистки движения или движения на религиозно Възраждане, на който ставаме свидетели в много части на света, е отговор на глобализацията или по-конкретно – на притеснението от мисълта, че съществуват други начини на живот, различни от тези, определени от версията на божеството на определена група“[8].

Понастоящем разбирането за фундаментализма в най-общи линии се свързва с религията, където често мотивация са насилието и терорът. Намирането на тясна връзка между минало и настояще при тълкуването за естеството на фундаментализма обосновава извода, че протича несъзнателно проектиране на методи и средства, наложени със сила в настоящето, които са заимствани от миналото. Имайки предвид гореизложеното, може да се заключи, че във фундаментализма по същество има сблъсък за елиминиране на минало и възприемане на традиция.

Фундаментализмът има проявление и се отнася за: християнството; юдаизма; индуизма; исляма, където стои по-остро. Според К. Леви-Строс социалните групи

изпитват сериозни „трудности да понасят ставащото все по-близко, дори интимно присъствие на хората от други култури поради увеличаване заселеността на териториите“. Ученият смята, че отделните членове на обществото, социалните групи, културите се нуждаят от дистанция. И когато по необходимост тази дистанция изчезва, възникват всевъзможни видове патологични феномени[9].

През последните години понятието фундаментализъм най-често се свързва с ислямската религия, а оттам се разглежда ролята, връзката и предпоставките за възникването и разпространяването на ислямския фундаментализъм като ислямски тероризъм. Последното не се поражда от исляма като религия, а е в резултат на едностранчиво представяне на ислямската религия, където като особеност може да се приеме омразата, ненавистта, нетърпимостта към неверниците, към всички хора, които са различни, притежават друга религия, етническа принадлежност, култура и т.н.

С ислямския фундаментализъм се свързват действията на представителите на радикалния ислям, които притежават характерни черти:

- възприемат джихада като въоръжена борба срещу неверниците, като по този начин се допуска многоаспектното понятие „джихад“ да се сведе до едно от своите значения и да се изключат останалите;

- стремеж на представителите на радикалния ислям да създадат световен халифат, имайки предвид подражаване на форма на държавно управление и устройство, познато в далечното минало;

- приемането на шериата за единствен законодателен източник. Радикалните ислямисти си поставят за задача да приведат в съответствие с шериата правните системи на страните, в които се установяват на власт.

При фундаментализма е важна идеологията с екстремистка насоченост, служеща на интересите на своите създатели, които могат да бъдат националистически, етнически, социални, религиозни интереси, оправдавайки терористичните им действия. Екстремистката идеология, основана на рационалността и на съзнателно подготвените и осмислени аргументи не е идеология, а в нея присъстват ирационални моменти, които в своето единство служат за обяснение и оправдание на разрушителните действия. Погледнато по този начин на екстремистките идеи, от които се ръководят терористите се вижда, че те са измамни и нереални.

2. Изложение

Същност и идеи на екстремизма

Според Румян Русев понятието „екстремизъм“ е разглеждано като сбор на идеи и възгледи, представляващи абсолютна непримиримост и отричане на всичко противоречащо или различаващо се.

Екстремизмът се разглежда още и като:

- система от норми, правила и идеи, тотално противоречащи на осъзнатите и приети от човечеството ценности;

- съвкупност от продължени до абсурда идеи и възгледи от разпространените в обществото идеологии и религии, които независимо от общата фразеология, не могат по никакъв начин да бъдат отъждествявани;

- своеобразна обществена патология, девиантна психологическа установка, анормална реакция, насочена против социалната практика и живота[10].

При изследването на понятието „екстремизъм“ Румян Русев стига до извод, че „независимо от използването на словосъчетания като „ляв“, „десен“, „ислямски“, „арменски“, „кюрдски“, „латиноамерикански“ и др. в съчетанието с екстремизъм или

тероризъм, по никакъв начин не се отъждествяват феномените с идеологиите и религиите, от които е заимствана фразеологията[11]“.

От друга страна Збигнев Бжежински през 1994 г. посочва, че „Екстремизмът и тероризмът са обективни обществени феномени, които могат да бъдат изучавани и реално да бъдат ограничени в обществото[12]“.

В своята книга Патрик Кенеди развива теорията за екстремизма като обществено явление, което отдавна не е само научен факт, а присъства в ежедневието на всички общества. „Той е една от тъжните характеристики на нашето време. Поради факта, че феноменът не е групов, конфесионален или национален, а световен, при анализа му ще подходя адекватно на величината му[13]“, сочи Бжежински.

Според професор Зигмунт Бауман „на глобалните проблеми са необходими общи отговори[14]“.

По отношение на екстремизма няма общопризнато определение, нито съществува единно мнение докъде са границите му и при какви условия с висока степен на достоверност може да бъде използвано. В обществото съществуват интуитивни представи за екстремизма, оприличаващи го на аморфен обществен феномен, явяващ се труден и политически опасен.

Според Румян Русев в определен смисъл това състояние е дори поощрено от удобството на политическата целесъобразност, от моментния интерес в правото, от острата необходимост за легитимиране на действия, но също така и от безразличието. Безспорно е, че всички тези влияния съществуват, но те едва ли са основни. За да се дефинира един такъв ярко изразен негативен феномен, какъвто е екстремизмът, най-малкото е необходимо да съществува консенсус в света, ако не по всички или по много въпроси, то поне за няколко жизнено важни. Днес човечеството би могло вече да посочи консенсуални въпроси, които могат да бъдат обобщени в няколко групи[15]:

- съхраняване на живота на земята;
- стремеж за съхраняване и развитие на осъзнатото и достигнатото в историческата еволюция разбиране за човешката свобода;
- съхраняване на крехкото екологично равновесие на планетата, съхраняване на перспективата пред новите поколения;
- поддържане на баланс и съотношения в световната икономика, предопределящи тенденцията на ръст, стремеж за съхраняване на духовността, намаляване на страданието, усъвършенстване на международното право и разширяване на периметъра му;
- туширане на кризисните колебания в световната финансова система;
- стремеж за съхраняване на държавните граници и търсене на самоопределение в техните пространства.

В същото време човечеството е далеч или все още не е постигнало консенсус по такива групи въпроси като: разпределение и ползване на жизнени, в това число и природни ресурси; параметри на неравенството; допустими средства за налагане на интересите; недопустимост на войната; общи основи на духовността; модел на усъвършенстване на демокрацията; параметри на новия световен ред и др.; признаване на очевидната тенденция за глобализация.

В такава реална ситуация, в която консенсуалността присъства, но не е преобладаваща, легитимно обяснение на общозначим феномен като екстремизма е възможно, ако границите му бъдат съобразени с тези консенсуални въпроси. В противен случай ще се върнем към дихотомията на комунизма и капитализма, на развития и беден свят, на „белите“ и „червените“ и т.н. Познато състояние, в което с екстремизма се

съотнасят само другите. В противен случай обяснението на феномена ще има не общо, а групово национално или в най-добрия случай –коалиционно значение.

Но в този случай би изглеждало като епитет, а не като цялостна характеристика. Нищо чудно, че от десетилетия двете противоборстващи идеологически системи адресираха екстремизма към противостоящата страна и търсеха идейните корени на феномена у противника[16]. Един явно ненаучен тезис и субективен стремеж, довел до отсъствието на един в достатъчна степен приемлив възглед за определянето на екстремизма.

Опитът за изследване на проблема „екстремизъм“ е проектиран върху признаването на реално съществуваща тенденция, която е обективна необходимост и е свързана с глобализацията на света.

Моделът на обществената среда, в която се прави опит за определяне на екстремизма, означаваме като „полития“. Това понятие е използвано като работно и изразява вътрешните взаимоотношения и съотношения в обществата (политическите режими) или тези между тях. Става дума за съотношението и взаимоотношението между такива групи образувания, които могат да бъдат обобщени като справедливи и правилни[17].

Справедливи, в смисъл на удовлетворяващи интересите, възгледите и моралните норми на мнозинството.

Правилни, в смисъл на осъзнато приетите компромиси със собствените възгледи и норми с цел функциониране на обществото и неговото съхраняване[18].

Възгледът за политията като форма на управление, подчинена на интересите на мнозинството, е приет от Аристотел[19] и доразвит от модерните философи, като целта на управляващите е общата полза чрез реална интерпретация на съотношението справедливи и полезни правила. Център на координатната система, позиционираща политията в реалните измерения на справедливото и полезното е конкретното съдържание, влагано към тях от членовете на всяко общество. Това многообразие на ценности и най-вече тяхното съотношение създава палитрата на политиите в света.

Терминът „толерантни общества“, в които справедливостта е не само доминираща, но заема преобладаващата част от пространството е използван като аналог на термина „полития“.

За екстремизма се смята, че сам по себе си е сбор от идеи, чиято реализация се базира на адекватно на тях поведение, като в резултат на тях се достига определено състояние. Предходното е вследствие на факта, че не съществува нито универсално познание, нито универсална оценка на феномена екстремизъм, което е и основанието да не се търси абсолютно определение, тъй като стремежът е да разглеждаме еволюцията на гледните точки до достигането на степен на консенсуалност от човечеството като цяло[20].

Приема се, че по основните въпроси, по които е очертана приемливата граница и зад която са изключенията, се намира екстремизмът. В този смисъл и при условие, че общопризнатите граници на консенсуалните въпроси не са съизмерими и идентични, можем да говорим и за различен вид екстремизъм. Общоизвестни са различията в обществото между етичната и правната граница, съществуването на значими разлики в оценките и в праговете на допустимост в отделни групи, общности и страни. Затова международният екстремизъм може да бъде отнесен като понятие само извън границите на общоприетите международни норми, а политически екстремизъм като понятие извън границите на допустимите политически норми.

Екстремизмът, разглеждан като идея, поведение и състояние, би могъл да бъде разграничен от други обществени феномени посредством съпоставянето му с тях. Логично е да се търси място на екстремизма извън периметъра на други феномени и дори извън най-радикалните, но вписващи се в реализираните „леви“ и „десни“ модели на света, в това число и религиозни. Всъщност се прави разлика между крайни (в смисъл радикални и фундаменталистки) идеи и екстремизъм, като те трябва да се разграничават категорично.

Игнорирайки съвременното разбиране за справедливост, а оттам и човешкия живот, екстремизмът се гради на теория и е насочен към унищожаване на установените правила от действащата политическа система, което се явява като:

- отхвърляне на основни и общоприети човешки ценности;
- стремеж за смяна на политически модел с друг, подчинен на насилието и свързан с игнорирането на осъзнатите норми на живот.

Достигането на състояние, което предполага осъществяването на условия за безнасилствено разрешаване на конфликтите между различните идентичности и за прогрес е идеята за хомогенизирането на света, която е разглеждана не като загубване на идентичността[21].

Радикализъм – етапи на радикализация

По въпроса за същността на радикализма учените са достигнали до консенсус, че радикализацията е феномен, при който липсва праволинейност, обвързан по-скоро от контекста на съответната ситуация, при който социологическите, политическите, религиозните и психологическите фактори играят в еднаква степен ролята на задвижващи механизми. Тя е резултат от конвергенцията между „пътя“ на отделния индивид и система от убеждения (вяра, религия), оправдаваща прибягването до насилие, което може да бъде изострено от възприятието за заплаха по отношение на нечия идентичност или морални ценности и подклаждано от социалните мрежи (лице в лице или онлайн).

В теорията се приема, че радикализацията е динамичен, многопластов, многообразен феномен, който възниква в пресечната точка между индивидуалните „подтикващи“ фактори (биографична предразположеност и лична траектория, вътрешна мотивация, преживени лични драми) и такива фактори, които имат „притегателна сила“ (излагане на идеологии и набиране на нови последователи). Често чисто ситуационни фактори като структурни и свързани с обкръжаващата среда условия, заедно с групови фактори и динамични събития, могат да допринесат за ускоряване или да играят ролята на катализатор за този процес. Структурните фактори сами по себе си не могат да обяснят в достатъчна степен радикализацията, тъй като ударението следва да се постави по-скоро върху това как благоприятстващата среда се отразява върху индивида и взаимодейства с него. Пропагандата и набирането на нови последователи често са катализаторите на това взаимодействие.

Процесът на радикализация протича на ниво индивид, група, общност и на ниво общество и често определени каузални фактори и събития, имащи ролята на задвижващ механизъм, резонират и „работят“ на посочените три нива едновременно. Например лишенията от определени блага може да повлияят както върху конкретен индивид, така и върху цели обществени групи; международни събития (примерно конфликтът в Сирия), може да резонират както с индивида, така и на ниво група и да играят ролята на катализатор, за да подтикнат индивидите да прегърнат радикални идеи.

В издаденото през 2016 г. от Център за изследване на демокрацията „Ръководство за практици в областта на разбиране, оценка и мониторинг на процесите и насоките на развитие на радикализацията“ се предлага и разглежда модел на анализ на факторите и процесите на радикализация, водещи до насилие, протичащ на три нива:

Макро ниво, тоест, ролята на правителството и обществото вътре в страната и извън нея, радикализация на общественото мнение и политическите партии, напрегнати отношения между мнозинството и малцинствените групи, особено ако става дума за обособени етнически групи [26], живеещи извън историческата си родина (чуждестранни диаспори), липсата на социално-икономически възможности за цели обществени сектори, която води до мобилизация и радикализация на недоволните и би могла да приеме формата и на тероризъм. Макро нивото по-нататък е свързано и с международните отношения, слаба интеграция, а едновременно с това влияе и върху процесите на глобализация и модернизация.

Мезо ниво, тоест, по-широка радикална среда – поддържащо, дори съучастническо социално обкръжение, което служи като сплотяващ елемент, „липсващата връзка“ с широкото поддръжничество на терористите, респ. групи от огорчени или страдащи от определена несправедливост, които на свой ред може да радикализират част от младежта и да се достигне до формиране на терористични организации или до конкретни актове на тероризъм. Мезо нивото или социалното ниво, по-нататък е свързано с въпросите на социалната идентичност, социалното общуване и на груповите процеси.

Микро ниво, тоест, индивидуалното ниво (личностни характеристики и опит), което включва личностни проблеми, неуспешна интеграция, чувство за отчуждаване, маргинализация, дискриминация, липса на близки, унижение (директно или индиректно), стигматизация и отхвърляне, често комбинирани с морално оскърбление и желание за отмъщение (възможно е да се касае и за отмъщение в името на някой друг)[22].

Практиката е извела няколко примерни етапа, през които преминава радикализацията. Изводите са направени въз основа на конкретни наблюдения върху биографиите и дейността на конкретни терористи.

Условно радикализацията преминава през следните етапи:

1. Етап на т.нар „Предварителна радикализация“

На този етап индивидът е повлиян от вътрешни или външни фактори: криза на идентичността, фрустрация, лична травма, дискриминация, чувство за несправедливост, натиск от семейството или общността, липса на умерен дебат, среща с харизматичен лидер и др. Най-често се касае за психологически дефицити на индивида, усещането за изолираност, като в този случай той е мотивиран да търси място и хора, сред които да се чувства приет и оценен.

2. Етап на т.нар „Идентифициране“ или приемане на идеологията

Обикновено в този начален етап пред индивида се разкриват позитивните страни на дадената доктрина, която той приема, като дори произтичащите от нея актове на насилие се възприемат като оправдан и логичен отговор на определена неправда. Това е етапът, в който индивидът започва да се отдалечава от досегашния си начин на живот. Засилва се чувството, че приятелите му не го „разбират“, но това чувство не предизвиква притеснение, защото е обкръжен от нови хора, негови „братя“ по мироглед, с които споделя еднакви ценности и идеологии. В новата група, където се чувства „избран“, индивидът постепенно придобива нова социална идентичност, която го изолира от останалия свят, като засилващото се чувство за групова принадлежност подсилва мотивацията и вярата му. При този етап груповата динамика играе особено важна роля. Макар да е вече приет в новата група, понякога индивидът все още се чувства „чужд“ и това го стимулира да докаже предаността си към общността или идеологията, като извърши нещо „изключително“, включително престъпление или акт на насилие.

3. Етап на т.нар „Индоктриниране“ (системно обучение)

След като индивидът е приел радикалната идеология, духовните водачи започват да му възлагат конкретни задачи и започва да губи предишната си критичност. Лидерът на групата е безспорен авторитет и всичко, казано от него се приема за „чиста монета“. Възлагането на отговорности в групата повишава усещането за съпричастност и значимост у индивида. Лидерите на общността повишават идеологическата подготовка на новоприетия и го подтикват към подобряване на физическата форма. Целта на тази системна индоктринация на индивида е той да изгуби всяко чувство за рационалност, да се отдаде и да повярва в живота, който го очаква в бъдеще, ако е праведник, вместо в земното битие.

4. Етап на „Действие за каузата“

На този етап се цели извличането на максимална полза от радикализираните лица, като те биват ангажирани в дейности, в които са използвани конкретните им умения и познания. Например те могат да станат проповедници или вербовчици; възможно е да извършват престъпни и/или насилствени актове, включително да участват в бойни действия, самоубийствени атентати и др. Преминаването през този етап е свързано с външна изява на протичащите у индивида психологически процеси. Именно в този момент могат най-ясно да се идентифицират външните признаци на радикализацията.

Условно тези признаци са разделени в няколко групи:

1. Свързани с личността:

- придобиването на псевдоним, обикновено от религиозните текстове, което показва съпричастността към конкретното религиозно течение;
- промяна в стила на обличане, избор на дрехи, характерни за членовете на конкретната религиозна общност, които често пъти са нетипични за обществото;
- промяна на физическата външност, обръсване на главата или пускане на дълга коса или брада. Един от най-характерните външни белези за радикалните ислямисти е дългата брада с къси мустаци.

2. Свързани с поведението:

- стремеж към контакти с водачи на радикални религиозни групировки;
- промяна в религиозните практики – индивидът става по-стриктен в спазването на религиозните ритуали, заради което се пренебрегват съществени ежедневни занимания от водения преди това живот – посещение на училище, ходене на работа и др.;
- участие в закрити събития, обикновено след молитва, когато в молитвения дом остава по-тесен кръг от „доверени“ лица. При тези събирания не се обсъждат религиозни теми, а и актуални геополитически и социални събития и влиянието им върху религиозната общност, като се планират ответни реакции срещу тях;
- ползване на интернет форуми с радикално съдържание. Там индивидът намира и „сродни души“, а също и лица, които би могъл да радикализира;
- промяна в модела на пътуване или престой в специфични райони, където жителите споделят крайните възгледи;
- възхвала на мъченичеството и насилието. Тук не се търси приемливо оправдание, а насилието се възприема и като личен път, който следва примера на тези, които вече са се „преселили“ в отвъдното по „най-богоугоден“ начин;
- увлечение по екстремни или силови спортове;
- социална изолация – отбягване на училището, младежки клубове, концерти и др.;
- използване на радикална или специфична терминология, която не е общодостъпна;
- извършване на незначителни престъпления като символ на неуважение към установени правила в обществото като вид „бунт“ срещу него;

- незачитане на светската власт чрез демонстративно неуважение към нея (следва се максимата „Властта идва от Бога, а не от хората“).

3. Свързани с идеологията:

- отричане на нововъведенията в религиозните вярвания и практики и ненавист към по-умерени течения в религията;

- емоционална ангажираност към каузи, които често пъти касаят пряко индивида (примери: палестинско-израелският конфликт, военният конфликт в Сирия и др.);

- отричане на научните достижения и теории до ниво на абсурдност за останалите членове на обществото. Това е един от най-очевидните признаци, свързани с вътрешните убеждения на индивида.

Интерес представляват специфичните похвати за радикализация. Накратко, методите, които се използват за радикализиране на индивида са:

Метод на „угнетяването“

При този похват се използват фотоси или видеоматериали, в които се представя страданието на цивилни граждани (косвени жертви на даден конфликт), предимно деца и жени. Така индивидът се подтиква към ответна реакция при използване на състраданието и чувството му за справедливост.

Метод на сугестията

Значимо средство в ислямистката пропаганда са така наречените „Нашии“ – песни, в които под емоционално въздействащ музикален съпровод се повтарят многократно едни и същи фрази. Често пъти нашите са вплетени във видеоклипове, в които се показват определени кадри, включително на загинали „мъченици“. С това се цели въздействие върху подсъзнанието. Автосугестията е цел на ритуалните религиозни практики. Конкретно мюсюлманските религиозни обреди предполагат петкратната молитва, в която едни и същи действия и едни и същи фрази се повтарят многократно и това води до самовнушение.

Метод на насилието

В затворените религиозни групи или в тренировъчните лагери на терористите често пъти се прибягва до насилие спрямо тези, които показват признаци на разколебаване. Така се пречупва волята им.

Практиката обособява радикализираните лица в три групи:

1. Саморадикализирали се лица

При тях основна роля имат личните причини и социалната изолация. В търсене на идентичност тези индивиди попадат на крайни идеи, които ги привличат. Това най-често става чрез интернет.

2. Радикализирали се под влиянието на външни фактори

Представителите на тази група са се повлияли от проповедници или от груповата динамика на радикална общност. За катализатор обикновено служи външнополитическо събитие, обсъждано подробно в групата или коментирано от духовния лидер.

3. Конвертити (приели друга религия)

Тук може да се говори за съчетание между предните две групи. Тази група радикализирани лица носи голям риск, тъй като у тях желанието да докажат силата на вярата си е много голямо.

Срещу радикализираните лица като сложен и многопластов феномен трябва да бъдат използвани методи на противодействие както на национално, така и на международно ниво[23].

Фактори, влияещи върху средата за сигурност и обуславящи възникването на екстремизъм

Наличието на обособени групи или общности, които търсят и създават условия за радикална изява извън съществуващите в демократичното общество ценности, принципи и легални механизми за социален просперитет се свързва с най-крайно проявление на екстремистка активност. Формирането на такава среда за Република България е риск, свързан с външни деструктивни въздействия върху определени специфични в етнорелигиозно и културно отношение категории от населението. Превръщането на осъзнатите различия във фундамент, върху който се изграждат позициите на отрицание на културните и цивилизационни особености на другите представлява пряка потенциална заплаха, защото води до проява на агресия спрямо тези, които изповядват отричаните ценности. Част от общностите, възприели отрицанието са кланово организирани и съществува възможност членовете им да станат заложници на интересите на лидерите си. Интересът и стремежът на последните е да не допуснат интегрирането им в нацията, тъй като ще загубят властови ресурс. Специфичен похват в тази насока често е превратното тълкуване на историята и/или на религиозни постулати.

Външното деструктивно влияние и вътрешните посегателства срещу конституционно установения ред създават допълнителна уязвимост на средата за развитие на екстремизъм, насочени към степента на интегрираност на нацията. От първостепенна важност остава проблемът с дезинтеграцията на съвременната българска нация, като в този процес кризите с различен характер играят роля на катализатор [26]. В страната ни функционира сравнително успешен етнически модел, като правната уредба в областта на обществените отношения „държава – общности“ е всеобхватна и съобразена с международните и европейски актове. Във връзка с последното са създадени множество концепции, програми, проекти и структури, предназначени да обезпечат интеграционните процеси [26]. Инертността и продължителността при преодоляването на дезинтеграцията във време, в което липсва развита икономика, допълвана от перспективно ориентирана активна политика на културен синтез, води до запазване на актуалността на екстремизма като рисков фактор за националната сигурност.

В условията на икономическа криза и проблеми в традиционните вероизповедания, нетрадиционни религиозни деноминации, секти и окултни течения правят опити за привличане на последователи посредством емисари. Основният риск тук е свързан с популяризирането на практики, представляващи заплаха и предизвикващи напрежение сред местното население поради агресивната пропагандна дейност.

Емисарите, явяващи се като представители на различни религиозни радикални течения и нетрадиционни религиозни деноминации, не представляват пряка опасност за националната сигурност, но с действията, посредством които прокламират идеологията си, допълнително способстват за дезинтеграцията на етносите. Разпространението на идеологиите на различните религиозни радикални течения и нетрадиционни религиозни деноминации се извършва в зависимост от социално-икономическото естество и възникващите от това предпоставки.

Дейността на крайно леви и крайно десни екстремистки структури също съдържа рисков потенциал. Аналозите на крайно десните формации в Република България, на фона на нарастващото влияние на крайно десните формации в Европа, се явяват маргинални образувания без реална политическа тежест и обществена подкрепа. През годините е наблюдавано известно активизиране на крайно левите и анархистичните групи, но към момента, поради липса на ресурс и поддръжка, проявите им не реализират търсения от тях

ефект. Последното не изключва възможността събития и действия на подобни структури в съседни страни да се използват като модел и в Република България.

Дейността на нелегитимни политически формирования на етническа и религиозна основа е друг фактор за възникване на екстремизма, водещ до пряко въздействие върху средата за сигурност. Числеността им е крайно ограничена и активността им е непостоянна, въпреки че антибългарските им изяви съдържат рисков потенциал в няколко направления, посредством:

- целенасочени действия пред международни форуми и официални представители на правозащитни институции. Все по-често темата за наличие на „национални малцинства“ и свързани с тях нерешени въпроси се включва в официални документи, отразяващи обстановката в страната ни;

- извършване на проверка на нагласите и възможностите за реорганизиране на политическото представителство на отделни общности в България.

Опитите за структуриране на „паралелни“ общества и власт сред кланово организирани общности и групи, които са с нисък социален и образователен статус оказват влияние върху средата за сигурност посредством нехомогенност и конфликтен потенциал. Членовете им принципно не разполагат с достатъчно ресурси за преодоляване на цикличността „бедност – необразованост – липса на социална реализация – бедност“, като в условията на икономическа и финансова криза, безработицата и безперспективността се превръщат в субект на религиозни течения, чиито идеи се прокламират с помощта на емисари и имат деструктивен характер.

Описаните по-горе процеси и тенденции в социалната сфера се проектират в липса на синхрон в действията на етно-религиозните и културни елементи и имат устойчив характер, създавайки предпоставки за проявление на рискове за националната сигурност в насока:

а.) ерозиране на единството на нацията, като съществува вероятност крайният негативен резултат да бъде разпадът на националната общност, вследствие на възприемането на религиозни и етнически характеристики за идентификационен маркер при самоопределението за принадлежност, вместо единното гражданство, общата територия и др.

Имайки предвид предходното, действия, съдържащи високорисков характер са насочени към:

- българската група в етнодемографската структура на обществото, чрез намаляване на относителната тежест на промяна на числеността на едни етноси чрез „приобщаване“ към тях на представители на други, както и чрез стимулиране на обособяването на несъществуващи етноси;

- капсулиране и изолация на отделни групи в обществото, обособени по етнически или религиозен признак, водещо до задълбочаване на паралелно протичащите процеси;

- обвързване на религиозния и/или етническия елемент с чужд национализъм, което има все по-голямо значение за етнонационалната идентификация и активно се използва от външни фактори за възприемане на чуждо национално самосъзнание.

б.) нарушаване на демократичното функциониране на обществото и институциите и на конституционно установения ред, което се свързва с:

- действия от страна на лидери на етно-религиозни общности на местно или на национално ниво, целящи политико-икономическа „самореализация“, в това число посредством и чрез поява на нови образувания на основата на „етнонационализма“ и дори на „религиозния национализъм“.

- нерегламентирана религиозно-просветна дейност, извършвана от лица и организации, използвайки религията за политически цели, посредством която проповядват антидемократична идеология от всякакъв вид и позиции.

в.) нарушаване на основни права и свободи на гражданите, което се явява потенциален риск от нарушаване на установените отношения между различните религиозни общности в страната, съдържащи действия на основата на расизма и ксенофобията. Предизвикването на инциденти с български радикални структури и последвало демонстративно „овладяване“ на конфликтите представлява риск.

3. Заключение

Независимо от степента и етапите на развитие, всички тези процеси влияят негативно върху защитата на националната сигурност, тъй като увреждат интеграционния потенциал на държавата и обществото. От предходното произтичат и възможностите на държавата и обществото да се справят с предизвикателствата във вътрешен и външен план. По този начин се създават условия за реализация на чужди за традиционните вероизповедания идеологии чрез формирания потенциал за влияние и въздействие върху вътрешнополитическата обстановка. Това се отнася основно до възможностите за манипулирано направляване на поведението на значителната етническа и на социално нехомогенните общности в страната ни.

ЛИТЕРАТУРА:

[1] Graham, G., Fundamentalism, http://www.newfun2/htmlBack

[2] Джон Еспозито, “Ислямската заплаха – мит или реалност”- стр. 13

[3] Ruckman, P., Fundamentalists and Fundamentalism, Part One, http://www.fundamentals.htmlBack

[4] Hadden, J., Fundamentalism, http://www.virginia.orgBack

[5] Fundamentalism and Islamic Movement, The Secretary General, Jamaat Islami, Lahore, Pakistan, http://www.webmaster.jamaat.orgBack

[6] Чуков, В. Етимологична ретроспекция на религиозния фундаментализъм

[7] Jurgenmeyer, M., Terror of the Mind of God, The Global Rise of Religious Violence, Berkley, University of California Press, 2 000, p. 289.Back

[8] Рутвен, М. Фундаментализмът. София, 2006, стр.44- стр.49

[9] Беседа с Клодом Леви-Стросом К. фон Барлевска и Г. Наумовы. В: Вопросы философии, 2009, № 5, стр.74

[10] Русев, Р., „Тероризъм в Турция”, Сиела, 1997г., с.175.

[11] Русев, Р., „Тероризъм в Турция”, Сиела, 1997г., с.175-176.

[12] Вж. Бжежински З, „Извън контрол”, С. 1994г.

[13] Виж, Кенеди П, „Залеза на демокрацията”, Обсидиан. 1995г.

[14] Виж, Бауман З, Глобализация, С. 1999г.

[15] Русев. Р, Анатомия на екстремизма, С. 2001г., стр.18-стр.19.

[16] Генри Э., Против Терроризма, М. 1881 г.; Генри Э., Терроризм инеофашизм, М. 1981 г.Блишенко И., Жданов В., Международно-равовая борьба с терроризмом, журнал"Правоведения", 1985, бр.1.; Васечкин Н., От революционной фразы к безрассудномуавантюризму, М. 1986 г.;

[17] Джон Р, „Теория на справедливостта”, С. 2000 г., стр. 19-стр.143.

[18] Низбет Р., Стремежът към общност, С. 1992, стр. 37-стр.74.

[19] Вж. Аристотел, Политика.

[20] Русев. Р, Анатомия на екстремизма, С. 2001г., стр.96.

[21] Джон Р, „Теория на справедливостта”, С. 2000 г., стр. 19-стр.143.

[22] Низбет Р., Стремежът към общност, С. 1992, стр. 37-стр.74.

[23] Вж. Аристотел, Политика.

[24] Dzhekova Rositsa, Moravec Ludek, Mancheva Mila, Stoynova Nadya,Anagnostou Dia, Understanding, Assessing and Monitoring Radicalisation Risks and Trends / guidelines for practitioners/, Edited by Lindsay Clutterbuck, independent senior expert on (counter)radicalisation and (counter)terrorism,Center for the study of democracy, September 2016г.

[25] Цветков, Т., Софийски форум за сигурност, „Радикализъм и младите”, 2016г., стр. 6-18.

[26] Savov, I. Some aspects of legislative system of the institutes migration and readmission in the European Union, International conference - Law and Security in migration process and the consequences of the migration crises, Nikola Tesla University, Beograd, 2017, ISBN 978-86-6113-046-5, p. 265-277.

Име на автора: д-р Тихомир Иванов Солаков
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail:
Име на съавтора: доц. д-р инж. Христо Атанасов Христов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, началник на катедра „Управление на системите за сигурност“
E-mail: h.a.hristov@shu.bg, hristov63@abv.bg

NATIONAL AND CORPORATE SECURITY

TSVETELINA I. METODIEVA

ABSTRACT: *The notions of security, safety, risk and security are related to a particular subject of interest for two or more subjects. The level of security, safety and security is determined by the hierarchy of the object of interest for competing subjects. The nature of the problem addressed in the report allows us to confine ourselves only to the level of "state security" for which the state is the object of interests and to the level of "security of the group of individuals," for which one of the objects of interest is the corporation.*

KEYWORDS:. *Safety, risk, corporate safety, threat.*

НАЦИОНАЛНА И КОРПОРАТИВНА СИГУРНОСТ*

ЦВЕТЕЛИНА И. МЕТОДИЕВА

АБСТРАКТ: *Понятията сигурност, безопасност, риск и защитеност са свързани с определен обект на интереси за два и повече субекта. Нивото на сигурността, безопасността и защитеността се определя от йерархията на обекта на интересите за конкуриращи се субекти. Характерът на разглеждания проблем в доклада дава възможност да се ограничим само с нивото „сигурност на държавата“, за което обект на интереси е държавата, и с нивото „сигурност на групата от индивиди“, за което един от обектите на интереси е корпорацията.*

1. Въведение

Понятията сигурност, безопасност, риск и защитеност са свързани с определен обект на интереси за два и повече субекта. Нивото на сигурността, безопасността и защитеността се определя от йерархията на обекта на интересите за конкуриращи се субекти. Професор д-р Николай Слатински, подрежда в една опростена (понеже служи за онагледяване и включва само най-съществените връзки и взаимоотношения), но много добре разбираема [18] „Схема отделните нива на сигурността“. Това е показано на фиг. 1.

Фиг. 1. „Схема отделните нива на сигурността“ подредена от професор д-р Николай Слатински.

* Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Така той разглежда понятието, като го свежда до пет нива на сигурност: Сигурност на индивида, сигурност на групата от индивиди, сигурност на държавата, сигурност на общността от държави, сигурност на света. Авторът подчертава, че подредбата от първо до пето място не прави нивата повече или по-малко важни, като всяко от тях има свое специфично значение. [1]

Характерът на разглеждания проблем в доклада дава възможност да се ограничим само с нивото „сигурност на държавата“, за което обект на интереси е държавата, и с нивото „сигурност на групата от индивиди“, за което един от обектите на интереси е корпорацията. За тези две нива понятията сигурност, безопасност и защитеност се определят като национална сигурност, национална безопасност, национална защитеност (защитеност на държавата) или корпоративна сигурност, корпоративна безопасност, корпоративна защитеност (защитеност на корпорацията).

В свой доклад доц. д-р Доника Диманова засяга основните тенденции в рисковете, опасностите и заплахите за национална сигурност. [2] Там констатира, че основните функции на държавата е гарантиране защитеността и сигурността на гражданите, което може да се затрудни, ако е нарушено нормалното и функциониране.

Категориите държава и корпорация се нуждаят от изясняване на техните структуроопределящи компоненти, т.е. такива, които определят системните свойства на държавата и корпорацията. „…държавата е обединено в народ общество, заседнало върху определена територия и подчинено на една самопроизводна, суверенна и правно принудителна власт". [3]

За държавата структуроопределящи компоненти са население, територия, власт, която е суверенна и легитимна.

„Територията е онази строго определена част от земната повърхност, с принадлежащото й въздушно и водно пространство, върху която се простира върховната власт на една държава“ [4].

В своя статия доц. д-р Георги Торнев [5] описва населението, като съвкупност от хора, живеещи организирано в общество, на територията на дадена държава, в определен период. Характеризира се с брой и структура.

Суверенът е субектът, ръководещ държавата. Може да бъде монарх, президент, а в случая с България - разделяне на властта на законодателна, изпълнителна и съдебна. Осъществява се чрез система от органи, предвидени в Конституцията и законите.

„Суверенитетът е характерно качество на държавната власт. Той е състояние на независимост на държавната власт спрямо друга власт, както в границите на държавата, така и извън нея“. [6] Следва да се отбележи, че участието на държавата в определени съюзи (Европейски съюз), конфедерации и други води до загуба на част или на пълен суверенитет.

Легитимността изисква упражняване на властта според установените закони и правила, нейното публично одобряване от управляваните граждани и признаване от други легитимни актьори на международната сцена.

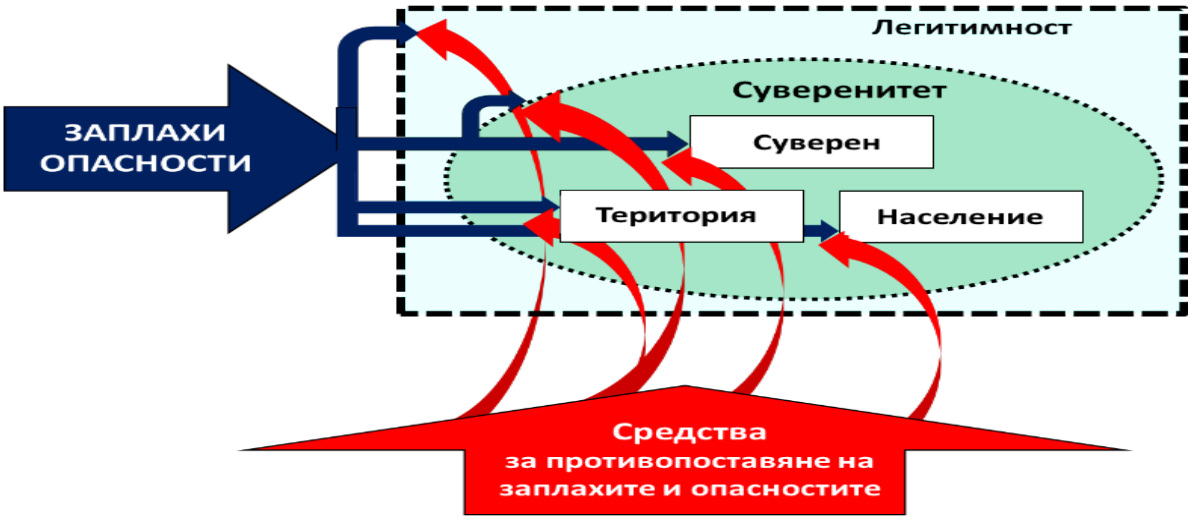
„Целите на държавата се осъществяват чрез нейните функции. Най-общо, понятието функция означава работа, дейност, кръг от задължения на органи и лица. Функциите са дейности, но ограничени по характер едни от други. Те изразяват спецификата на задачите, които изпълнява държавата в съответствие със своите непреходни и временни цели“. [7] Функциите на държавата биват: регулационно-управленска - регулира, посредством правото, обществените отношения, в които взема участие; охранителна, която е свързана със самосъхранението както на самата държава, така и на цялото

общество. Чрез правни норми от организиращ, превантивен и санкционен характер, държавата осигурява:

- реда и спокойствието в страната, гарантира живота, здравето и имуществото на гражданите, интересите на другите правни субекти;
- икономическата сигурност - без да се намесва пряко в проявите на частната инициатива и в отношенията на собственост (извън държавна), държавата помага за регулиране на тези отношения чрез икономически лостове - данъчна система, валутна политика, мита, банково дело, стимулации и пр.;
- културна политика- със специфични методи пряко организира и ръководи отделни направления, подпомага и съдейства на други, комбинира усилия и с участие на институтите на гражданското общество.

Освен посочените вътрешни функции тя има и друга външна функция. Към нея се включват направления, свързани с отбраната на страната, осъществяване на външно-икономически задачи, външната политика, интеграционни процеси с участие на страната“. [8]

Задължителното съществуване и функциониране на посочените структуроопределящи компоненти, изисква те да бъдат защитени от конкретни заплахи и опасности, които се развиват във времето. За тази цел на фиг. 2 е посочено, как суверенът реализира част от функциите на държавата, като използва различни средства.



Фиг. 2. Структуроопределящи компоненти за държава, нуждаещи се от сигурност и безопасност

Средствата са политически, икономически, информационни и военни (силови). За корпорацията структуроопределящите компоненти са активи (собственост), човешки ресурси, дейност (водеща до печалба), управление и репутация (търговска марка). Всеки от изброените компоненти е необходим за съществуването на корпорацията или за нейното целенасочено функциониране.

Активът е ресурс, контролиран от предприятието в резултат на минали събития, от който се очаква бъдеща икономическа изгода. Активите могат да бъдат материални, нематериални и финансови; дълготрайни и краткотрайни. [9]

Човешки ресурси е термин, използван да опише персонала - хората (служителите), които обхващат работната сила на дадена организация.[10] Неговият състав се определя

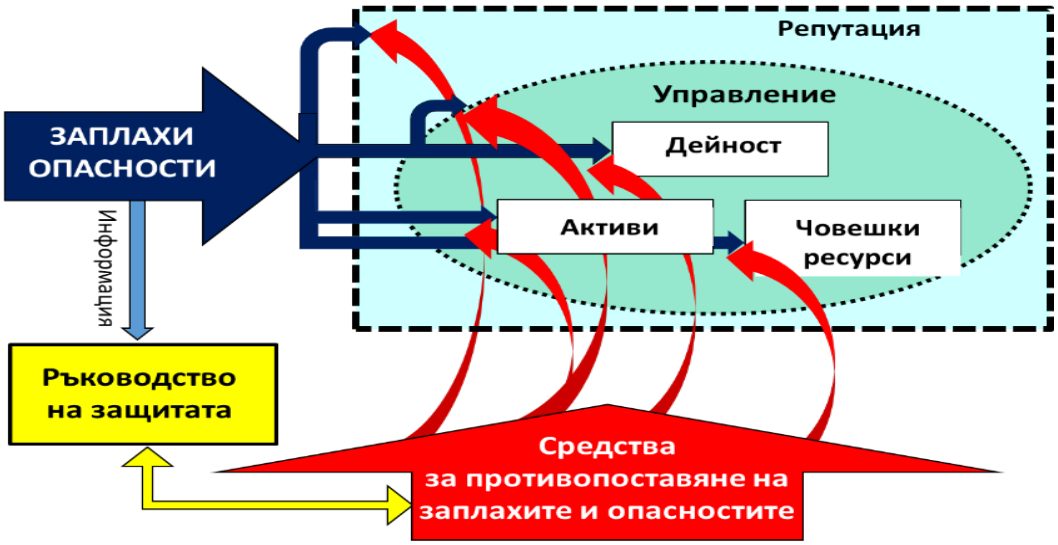
от функциите, които изпълнява в хода на дейността на корпорацията. Заетите се подразделят още по професии, специалности и квалификация.

Всички дейности в една корпорация могат да се представят като „верига за създаване на стойност“- Майкъл Портър „Конкурентно предимство“.[11] Те се разглеждат като основни и спомагателни и водят до формиране на печалба.[12] Тя е краен резултат от дейността на корпорацията и представлява разликата между приходите от дейността, финансовите и извънредните приходи, от една страна, а от друга - разходите за дейността, финансовите разходи, извънредните разходи и корпоративните данъци. Печалбата е абсолютен показател, който характеризира количествено дейността на корпорацията.

„Корпоративното управление включва отношенията между управляващите компанията, корпоративното ръководство, акционерите и заинтересованите лица. Доброто корпоративно управление трябва да осигурява подходящи стимули за преследване на цели, които са в интерес на компанията и акционерите, и да улеснява ефективния контрол, с което да насърчава фирмите към ефикасно изразходване на ресурсите“.[13]

Корпоративната репутация [14] е мнението на обществото за корпорацията, нейния външен образ, който се формира с течение на времето в съзнанието на заинтересуваните страни, въз основа на опита от взаимодействието с нея и оценката на нейната икономическа, социална и екологична дейност. До голяма степен репутацията се дължи и на търговската марка. Тя включва всички характеристики, които правят стоката конкурентоспособна. [15]

На фиг. 3 е изобразена необходимостта от условие за съществуване и функциониране на корпорацията е посочените структуроопределящи компоненти да бъдат защитени от съществуващи и потенциални заплахи и опасности.



Фиг. 3. Структуроопределящи компоненти за корпорация, нуждаещи се от сигурност и безопасност

По аналогичен начин, с известно прецизиране на структуроопределящите компоненти, могат да бъдат представени обектите на интереси на останалите три нива на сигурността.

Необходимо е да се уточни разликата между заплаха и опасност за компонентите на държавата и корпорацията. В някои източници тя се разглежда като различна степен на конкретност на техния източник. В други - в очакваното време на проявление.

Резултатът от това действие (заплашвам) е заплахата - закана, обещание да се причини на някого (на нещо) щета, загуба, недобро.

Заплахата да се разгласят компрометиращи сведения (верни или лъжливи) се нарича шантаж.

Опитът да се придобие чуждо имущество чрез заплаха се нарича изнудване. Заплахата по своята същност е разкриване на намерение.[16]

Съществуването на заплахи (явни или скрити) означава, че е възникнало противопоставяне на субекти за ценност, която е в състояние да удовлетвори техните потребности. Ценността може да бъде един или няколко от структуроопределящите компоненти на държавата (корпорацията). Тази ценност е обект на конфликта. В зависимост от характера на обекта на конфликта той може да бъде за ресурси (активи), статут, власт.

Според това кои са субектите конфликтът за разглежданите две нива на сигурност може да бъде междуличностен, между личност и група, между групов, междудържавен.

Съществуват конфликти от типа спор, противоборство или война. Възможните конфликтни ситуации, когато един и същ конфликт може да премине етапите спор, противоборство, война, а на всеки от тях страните да се възприемат различно - като опоненти, противници, врагове.

При определянето на заплахите за корпоративната (националната) сигурност е важно да бъдат отчетени вероятните интереси на всички заинтересувани страни, по всеки от структуроопределящите компоненти на корпорацията. Например, вариант на интересите на заинтересувани страни от външната среда по отношение на активите и пасивите на една корпорация са показани на фиг. 4.

Още по-детайлна ще бъде картината, ако се представят активите и пасивите като дълготрайни, краткосрочни, материални, нематериални и финансови.

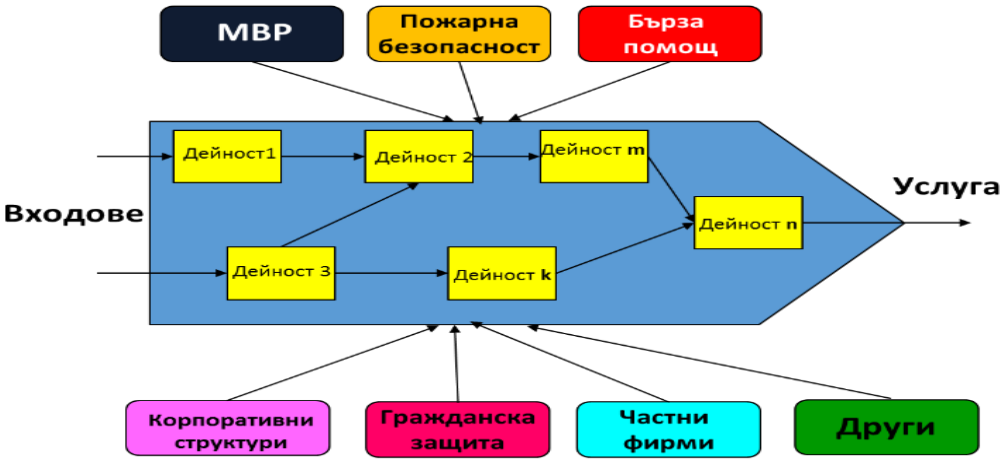
По аналогичен начин се определят заинтересуваните страни от външната среда и вътрешното пространство за всеки структуроопределящ компонент.

Фиг. 4. Заинтересувани страни от външната среда по отношение на корпоративните активи и пасиви

Като се отчетат интересите на корпорацията и тези на заинтересуваните страни, следва да се определят функциите на системата за корпоративна сигурност, т.е. спецификата на задачите, които изпълнява. Такива могат да бъдат управленска, информационна, защитна, възстановяваща, разследваща, комуникативна,

обучаваща/възпитаваща. Тези функции могат да се реализират от система, елементите на която не са само от състава на корпорацията, а и от държавни и частни структури (от полицията, пожарна безопасност и защита на населението, бърза помощ, частни охранителни фирми, детективски фирми, адвокатски кантори и други), развърнати в различни населени пунктове.

На фиг. 5 е представена дейността на такава система (с мрежова структура), която се организира за определен времеви интервал в процес, реализиращ съвкупност от функции и предоставящ съответната услуга, насочена към защитаваните корпоративни компоненти.

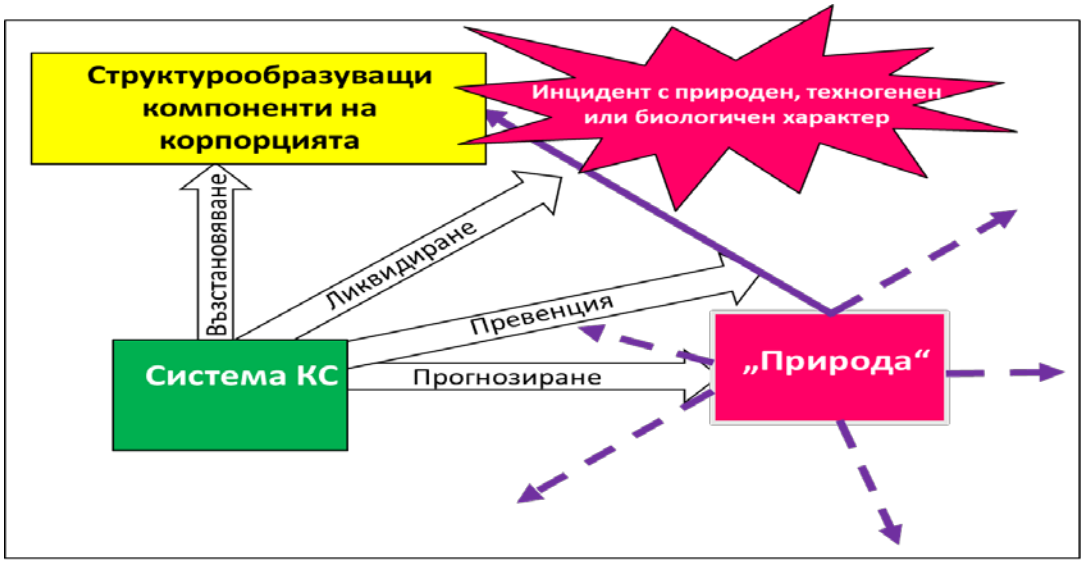


Фиг. 5. Процес организиран с част от система за корпоративна сигурност (с мрежова структура)

След като бъдат определени заплахите, следва да бъдат оценени рисковете за корпоративната (националната) сигурност. Това означава да бъдат определени вероятностите за реализиране на заплахите и очакваните поражения, щети, загуби, неправомерни разходи и др., които ще нанесат. Определянето на рисковете може да бъде количествено или качествено. Ако рисковете са неприемливи и разходите за въздействие по тях се вместват в предвидения бюджет, се пристъпва към тяхното управление. По този начин се постига сигурност на корпорацията.

Значението на опасявам се е боя се, страхувам се [17]. Опасността е възможност да се случи нещо неприятно, беда, щета от причинител, който няма интерес от това, т.е. причиняването на беда не е негова цел (ако изобщо причинителят има някакви цели). Този вид причинител на щети, беди (инциденти) ще наречем „природа“. Инцидентите от такъв вид източници на опасности могат да бъдат с природен характер (земетресения, наводнения, пожари и др.), с техногенен характер (аварии, предизвикани от ненадеждна техника, недостатъчна квалификация или небрежност на персонала при изпълнение на функционалните му задължения и др.) или с биологичен характер, като особена част от тези с природен характер (нездравословни условия на труд, епидемии, болести и др.).

За опасностите на фиг. 6 наблюдаваме, че не всички могат да се предвидят. Техният източник няма цел. Корпоративните компоненти попадат случайно в обсега им и е най-вероятно да има и други потърпевши от тяхната реализация).



Фиг. 6. Структура на въздействие на „природата“ върху компоненти на корпорацията

С провеждането на предвидените действия - прогнозиране, превенция, ликвидиране, възстановяване, се управляват рисковете за съответните опасности. По този начин се постига безопасност на корпорацията.

Въведените понятия сигурност и безопасност не са самоцел. Те се налагат от различните подходи, използвани при тяхното моделиране и управление: теорията на игрите - за заплахите, и теорията на статистическите решения - за опасностите.

Защитеността на корпорацията е обединяващо понятие на сигурността и безопасността на корпорацията. За да се избегне компенсирането на рисковете за сигурността с тези на безопасността, е наложително да бъдат използвани и трите понятия едновременно [18].

Предлага се работно определение на корпоративна сигурност: динамично състояние на защитеност на жизнено важните компоненти срещу вредни за корпорацията интереси, което гарантира, със зададена вероятност нейната цялост и функциониране.

Състоянието на защитеност е в пряка връзка с динамиката на текущите и прогнозираните заплахи за жизненоважните компоненти от външната среда и вътрешното пространство. Това състояние пряко зависи от отделяните ресурси за поддържане на възможностите на функциониращата система за корпоративна сигурност (определят допустимата горна граница на състоянието на защитеност, над която разходите са неоправдани), а също и от склонността на топ мениджмънта да поема риск, т.е. долната граница за състоянието на защитеност (под която вероятността за защитеност се обезсмисля).

В статията си „Национална и корпоративна сигурност“ доц. д-р Георги Торнев разглежда работното определение на корпоративна безопасност, като: динамично състояние на организираност в действията и резервираност на необходимите елементи срещу опасности, което гарантира, със зададена вероятност, устойчиво функциониране и поддържане на целостта на корпорацията.

А за свързващото понятие корпоративна защитеност: динамично състояние на цялост и устойчиво функциониране на корпорацията в условия на потенциални и реализирани заплахи и опасности.

Може да се направи изводът, че заплахите и опасностите не са синоним. Те са резултат от въздействието на различни източници.

3. Заключение

Източниците на заплахи са целенасочени субекти и прилагат различни методи за защитаване на интересите си.[18] Противодействия им се от системата за корпоративна сигурност. Препоръките за разумно поведение по време на конфликт се правят чрез използване на „теория на игрите“. За целта се разработва математичен модел - „игра“ с определени правила.

Източниците на опасности са с различен произход (техногенен, природен, с особено внимание на част от него - биологичен). Те не са злонамерени, нямат конфликтен характер. Липсата на противодействие от тяхна страна налага използването на „теория на статистическите решения“. Действията на източниците на опасности пораждат неопределеност на ситуацията. За намаляването на тази неопределеност в известни граници са необходими статистически данни за състоянието на „природата“.

Освен за нуждите на моделирането на процесите за управление на сигурността и безопасността въвеждането в употреба на тези понятия ще позволят да се разграничат ясно две различни по характер дейности - регулиране на конфликти и управление на непрекъсваемостта на дейността (с някои изключения).

В свой доклад доц. д-р Христо А. Христов прави следното заключение, че може да се приеме сигурност за една социална система (човек, организация, общност, общество, държава, общност от държави) тогава, когато основните идеали, ценности, потребности и интереси на системата не са подложени на никакви въздействия (абсолютна безопасност) или незастрашени от съществуващи въздействия, които социалната система да не е в състояние ефективно да неутрализира (защитена безопасност), контролира (относителна сигурност) или управлява (трансформационна сигурност) [19].

ЛИТЕРАТУРА:

[1] Слатински Николай, http://nslatinski.org/?q=bg/node/320

[2] Диманова Д, Рискови фактори и заплахи за сигурността в България, Трета международна научна конференция „Наука, образование, иновации”, 21 – 23 май 2014, Шумен,

[3] Въведение в правото. Теории за държавата. http://www.bg-pravo.com/2009/08/blog-post_464.html

[4] Въведение в правото. Граници и състав на държавната територия, http://www.bg-pravo.com/2009/08/blog-post_9135.html

[5] http://www.academia.edu/28690163/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%8F_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0_%D0%B8_%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0_%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82.docx – 2 стр.

[6] Въведение в правото. Държавен и народен суверенитет, http://www.bg-pravo.com/2009/08/i.html

[7] Въведение в правото. Функции на държавата, http://www.bg-pravo.com/2009/08/blog-post_4046.html

[8] Въведение в правото. Функции на държавата, http://www.bg-pravo.com/2009/08/blog-post_4046.html

[9] http://www.bg-ikonomika.com/search/label/Корпоративно счетоводство

[10] http://bg.wikipedia.org/wiki/Човешки_ресурси

[11] Michael E. Porter, Competitive advantage, The free press New York London Toronto Sydney Singapore

[12] http://bg.wikipedia.org/wiki/печалба

[13] Баева Б., Корпоративното управление: от правна норма към управленска практика - относно етапите в еволюцията на корпоративното управление, УНСС – катедра “Международни икономически отношения и бизнес"

[14] Саакова Л. В., Гавришин К. В., Управление корпоративной репутацией на основе парадигмы устойчивого развития http://www.m-economy.ru/art.php?nArtId=3662

[15] В. Балева, Търговска марка и/или бренд (brand), УНСС, катедра „Маркетинг и стратегическо планиране", http://alternativi.unwe.bg/alternativi/br25/5.pdf

[16] https://ru.wikipedia.org/wiki/угроза

[17] Lhttp://www.academia.edu/28690163/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%8F_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0_%D0%B8_%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0_%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82.docx

[18] Христов Х., Теоретични подходи относно проблематиката на сигурността. Научна сесия 2013г., Сборник научни трудове част 2, Обществени науки, организация, управление и методика на обучението във висшите училища, стр 180.

Име на автора: Цветелина Илиева Методиева
Месторабота: Асистент в катедра „Управление на системите за сигурност", Факултет по технически науки, Шуменски университет „Епископ Константин Преславски"
E-mail: tsvetelina.metodieva@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 294 - 297 Problems of Security Systems

GRADUATION OF ILLEGAL BEHAVIOR

VESELIN VELKOV

ABSTRACT: *A number of definitions of the unlawfulness of an action are controversial and provoke contradictory views. Behavior combines actions and omissions of the individual, especially in relation to the environment. It reflects its ability to change its actions under external or internal factors and has a huge adaptive meaning. Legality and acceptability are both separate and interrelated behavioral features governed by legal and social sciences.*

KEYWORDS: *Destructive processes, state system, public relations, corruption.*

ГРАДАЦИЯ НА НЕПРАВОМЕРНОТО ПОВЕДЕНИЕ[1]

ВЕСЕЛИН ВЕЛКОВ

АБСТРАКТ: *Редица дефиниции за неправомерността на дадено действие са дискусионни и провокират противоречиви мнения. Поведението обединява действия и бездействия на индивида, особено във връзка с околната среда. Отразява способността му да изменя действията си под влияние на външни или вътрешни фактори и притежава огромно приспособително значение. Правомерността и приемливостта са както отделни, така и взаимосвързани поведенчески характеристики регулирани от правната и социална науки.*

1. Въведение

Според юридически тълкувания поведението се регулира от правните норми и се нарича юридически факти. С юридическите факти са свързани и правоотношенията в правото. Те са обществени отношения, които са регулирани чрез правна норма. За да се прояви регулиращия ефект на правната норма е необходим юридически факт. Правоотношенията представляват правна връзка, която винаги е конкретна, защото съществува между конкретни субекти на правото.

2. Изложение

В българското законодателство са откроени две големи групи, в зависимост от това дали са резултат от дейността на човека или се проявяват без човешка намеса. Първата група юридически факти, която е по- голямата, е известна като „юридически деяния“. Касае се за съзнателно целенасочени човешки прояви, в резултат на които се проявява действието на съответната правна норма. Наричат се деяния, защото осъществяването им може да бъде извършено както с действие, така и с бездействие. Юридическите деяния могат да бъдат правомерни- такива които са в съответствие с предписанието на правните норми, и неправомерни- които им противоречат. Неправомерните са известни с общото наименование- юридически простъпки. Градацията е на база степента на обществена опасност на неправомерното поведение. С най- висока такава се отличават престъпленията, следват административните отношения, дисциплинарните нарушения и гражданско- правни диликти.

[1] Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски.

Втората група юридически факти са юридическите събития. Те са факти от действителността, с които правото свързва определени последици, но не са резултат от човешка дейност- напр. падане на гръм, мълния, довело до пожар и вреди върху нечий имот.

Според социалната класификация на поведението, то може да бъде общо, необичайно, приемливо или неприемливо. Хората оценяват приемливостта на определен тип поведение въз основа на социални норми, които регулират поведението, упражнявайки по този начин социален контрол.

Обективното рамкиране, определяне и диференциране на противоправната същност на поведението /съгласно възприетите правни и социални норми/ ще доведе до извеждане на точни критерии, въз основа на които институциите ще разработят програми за ранна идентификация на рискови нагласи сред служителите.

Неправомерното поведение е основния генератор на деструктивни процеси, обуславящи ниското качество на функциониране на държавната система и се явява пречка пред икономическия и социален просперитет.

Не обхванати в пълна степен, в правен аспект са следните деяния определяни като неприемливи и обществено нетърпими, но не съставляващи правонарушения /престъпления/ – привилегии и подаръци

Според авторски колектив на „Корупцията в 100 отговора“[2] правомерността на „подаръка“ и даването и приемането на същия не е престъпление, когато “дарът“ е под формата на цветя и бонбони или други дребни вещи/например фирмени календари или химикалки/. В случая се приема, че става дума за нормална и традиционна у повечето народи по света изява на благодарност към лекаря, който ви е лекувал, или учителя на децата ви. В някои законодателства съществува паричен еквивалент на подаръка, който обаче липсва в българското право.

Опит за поставяне на граница, на размера, на получаваните подаръци е видим в текст от Правилника за организация и дейността на Народното събрание[3], според който депутатите нямат право да задържат за себе си подаръци, когато са над една десета от месечното им възнаграждение. Всички подаръци над тази сума депутатите трябва да предават в Народното събрание. Всяка година народните представители са длъжни да попълват декларация, че не са получавали в качеството си на депутати подаръци на стойност над една десета от основните им месечни възнаграждения. На практика това означава, че депутатите трябва да описват всяка година какви подаръци са получили и кои от тях са предали в парламента.

През юли 2000 г. в Министерския съвет е обсъдена възможността за въвеждане горна граница от 50 лева за разрешени подаръци за държавни служители.

С приетия от правителството Кодекс за поведение на служителите в държавната администрация[4], обаче не е предвиден какъвто и да е праг. В същото време не е заложена и норма, която изрично да забранява приемането на подаръци. Единствено в чл.8, ал.2 от Кодекса е записано, че „служителят не допуска да бъде поставен във финансова зависимост или друга обвързаност от външни лица или организации, както и да иска и да приема подаръци, услуги, пари, облаги или други ползи, които могат да повлияят на

[2] „Корупцията в 100 отговора“, Коалиция 2000, © 2004, Център за изследване на демокрация, стр.21

[3] Чл. 149, ал.1 и ал. 2, Раздел 2“Етични норми на поведение“ , „Правилник за организацията и дейността на народното събрание“, в сила от 02.05.2017 г., Обн. ДВ. бр.35 от 2 Май 2017г., изм. ДВ. бр.34 от 20 Април 2018г.

[4] Кодекс за поведение на служителите в държавната администрация, Приет с ПМС № 126 от 11.06.2004 г. Обн. Дв. Бр.53 от 22 юни 2004г., чл. 8, ал.2 и 3

служебните му задължения, на неговите решения или да нарушат професионалния му подход по определени въпроси“, а пък в ал. 3, че „служителят не може да приема подаръци и облаги, които могат да бъдат възприети като награда за извършване на работа, която влиза в служебните му задължения“. Нещо, което може да се тълкува и, че вън от горните хипотези държавният служител би могъл да получава подаръци, услуги, пари, облаги или други ползи.

В Наказателен кодекс и Наказателно-процесуален кодекс липсва правна регулация на даването и приемането на подаръци. На институционално ниво опити за превенция и дефиниране на неприемливия характер на деянието е посочван в Етични кодекси и наредби.

Добра формулировка на „неетичния характер“ на даването и получаването на подаръци фигурира в „Кодекс за поведение“[5] на "Фонд мениджър на финансови инструменти в България" ЕАД. Във вътрешните правила на Фонда са посочени минимални стандарти за всички служители с оглед предотвратяване на ситуации, които биха могли да поставят почтеността на дружеството под съмнение. Със задължителното уточнение, че нарушаването на етичния кодекс по отношение регулацията на подаръци не представлява престъпление /тъй като отсъства в НК и НПК/ се приема[6], че визираните действия съставят вътрешно административни нарушения. Посочен е финансов праг от 30 евро, като е уточнено, че „надхвърлящите този размер подаръци, които не могат да бъдат отказани в интерес на деловите взаимоотношения, следва да бъдат дарени на благотворителни организации“. Предвиден е интересен текст[7], препращащ към отношенията на служителите на Фонда с представители на държавни институции и изключително точно отразяващ обществените нагласи по отношение на публичните длъжности – *„Лицата, заемащи публични длъжности, представителите на публични институции, членовете на обществени услуги или органи, и политиците са упълномощени да работят за общественото благосъстояние. Следователно, те не трябва да получават подаръци, покани или други парични подаръци, които биха могли да поставят под съмнение тяхната независимост от бизнес интереси или които, било то пряко или косвено, са насочени лично към тях.“*

Въпросът с получаването, даването, размера и формата на „подаръка“ е бил под регулация още в Османската империя. В Отоманския наказателен закон, който е в сила за България до 1896 г.[8], подаръка е синоним на подкуп, като обаче този термин не се е използвал. Вместо това, в него фигурира думата „взятка„: „ всичко, което се взима и дава под каквото и да е било име, за да се постигне една цел“. За „взятки“ са се приемали и „подаръци, малки или големи, дадени под каквото и да е име или предлог, освен обикновените подаръци, които се дават по сватби и тържества на правителствени слуги от страна на жени или мъже.“

3. Заключение

Отъждествяването на даването и получаването на подарък с „подкуп“ е опасно, ако не се отчитат културните и социални нрави и обичаи. В общия случай преобладава

[5] Кодекс за поведение на "Фонд мениджър на финансови инструменти в България" ЕАД, Раздел 1.11, стр.6, 7, 8

[6] От автора на Доклад „Градация на неправомерното поведение“

[7] Кодекс за поведение на "Фонд мениджър на финансови инструменти в България" ЕАД, Раздел 1.13 – „Парични подаръци на представители на публични институции“

[8] Ползван е цитат на авторите на „Корупцията в 100 отговора“, Коалиция 2000, © 2004, Център за изследване на демокрация, стр.24

мнението, че даването на подарък/дарение е израз на лична воля и свободен избор на даващия. По- специфичен е анализа по отношение на вземащия/получаващия, ако същия упражнява професия с концентрация на завишена обществена „благодарност“ – напр. педагози и медици

ЛИТЕРАТУРА:

[1] Асоциация „Прозрачност без граници”, Индекс за възприятие на корупцията за 2016г., http://transparency.bg/bg/transp_indexes/.

[2] „Корупцията в 100 отговора“, Коалиция 2000, © 2004, Център за изследване на демокрация, стр.21

[3] Чл. 149, ал.1 и ал. 2, Раздел 2“Етични норми на поведение“ , „Правилник за организацията и дейността на народното събрание“, в сила от 02.05.2017 г., Обн. ДВ. бр.35 от 2 Май 2017г., изм. ДВ. бр.34 от 20 Април 2018г.

[4] Кодекс за поведение на служителите в държавната администрация, Приет с ПМС № 126 от 11.06.2004 г.

[5] Обн. Дв. Бр.53 от 22 юни 2004г., чл. 8, ал.2 и 3

[6] Кодекс за поведение на "Фонд мениджър на финансови инструменти в България" ЕАД, Раздел 1.11, стр.6, 7, 8

[7] От автора на Доклад „Градация на неправомерното поведение“

[8] Кодекс за поведение на "Фонд мениджър на финансови инструменти в България" ЕАД, Раздел 1.13 – „Парични подаръци на представители на публични институции“

[9] Ползван е цитат на авторите на „Корупцията в 100 отговора“, Коалиция 2000, © 2004, Център за изследване на демокрация, стр.24.

Име на автора: докторант Веселин Велков
Месторабота: Катедра „Управление на системите за сигурност“, Шуменски университет „Епископ Константин Преславски“
E-mail: vkvelkov@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Information, Technical and Economical
CONFERENCE PROCEEDING, v. 2, pp. 298 - 303 Problems of Security Systems

IDENTIFICATION AND MANAGEMENT OF OPERATIONAL RISKS IN COMMERCIAL BANKS

ZHANETA ST. GEORGIEVA-PANAYOTOVA

ABSTRACT: *Operational risks are difficult to determine, measure, and evaluate impact, as they are perhaps one of the most comprehensive, as they accompany almost every transaction, transaction, or event in a bank's everyday life.*

The effectiveness of commercial banks is largely associated with high financial standing, net profit, good reputation, but also no less important is its resilience to external and internal operational risks and the ability of the organization to deal with minimal losses

KEYWORDS: *Operational risk, risk management, controlling.*

ИДЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ НА ОПЕРАЦИОННИТЕ РИСКОВЕ В ТЪРГОВСКИТЕ БАНКИ

ЖАНЕТА СТ. ГЕОРГИЕВА-ПАНАЙОТОВА

АБСТРАКТ: *В протичащите в световен мащаб икономически процеси от съществено значение е определянето на влиянието на пазара върху дейността на търговските банки. Това включва и определяне вида и степента на риска и оценка на влиянието върху основната дейност на банките. Тъй като дейността на всяка икономическа структура е интензивен процес, търпящ промени, продиктувани от средата, то неговото състояние може да бъде определено, както и да бъдат предвидени вероятните изходи от прилагането на дадено управленско решение.*

1. Въведение

Рискът е възможност за претърпяване на щета или загуба според Робин Кандал. Също така е и всеки неочакван изход от настъпването на дадено действие или решение. Рискът също така е настъпването на събитие, което оказва влияние върху дейността на цялата организация и последствията от събитието. Въпреки, че риска се характеризира с несигурност, то определено двете понятия не се припокриват напълно. А именно, различието произтича от факта, че по отношение на несигурността не бихме могли еднозначно да определим вероятността от настъпване. При оценката на риска определяме количествено резултата от прилагането на дадено решение и вероятността от настъпването му, както и величината и последствията от неговата реализация.

Оперативните рискове са тези, които не се отнасят до пазарните и кредитните рискове. Според Базелския комитет по банков надзор, оперативния риск е "пряк или косвен риск от загуби, произтичащи от неадекватни или неправилно организирани вътрешни процеси, отнасящи се до хора и системи, дължащи се на външни събития".

2. Изложение

Акцентирането на вниманието върху операционните рискове и тяхното въздействие е продиктувано до голяма степен от масовото навлизането на банковите услуги в ежедневието ни чрез електронните канали за обслужване, лесния достъп до банковите инструменти и тяхното популяризиране.

Оперативният риск с персонален характер е свързан с квалификацията на служителите, достъпа им до информация, работната среда и управленската структура, преднамерени или неумишлени действия, водещи до риск за банката. Негативен би бил резултата от допускането на грешки при осъществяване на оперативната дейност на банката поради некомпетентност на персонала, недобър мениджмънт или ако структурата загуби лица, заемащи водещи управленски позиции.

Рискът с организационен характер е налице най-често при недобра структура на организацията и взаимовръзките между отделните структурни звена, отдели, както и дейността на вътрешния контрол, планирането, счетоводното отчитане и т.н.

Предметно-техническите операционни рискове произтичат от техническата обезпеченост на банката и възможностите за осъществяване на ежедневния обем операции, извършвани чрез системите за обработка на данни, доброто ниво на защита на компютърната техника, комуникации, недостъпност или недостоверност на данните и т.н.

Рисковете, свързани с отношенията с институциите, физическите и юридически лица, клиенти на банката, нейните акционерите, банков надзор и регулаторни органи, медии.

Материални са всички рискове, свързани загуби в следствие на природни бедствия като наводнения, пожари, земетресения и т.н [5], [6].

Анонсирайки основните групи рискове в зависимост от техния характер, бихме могли да заключим, че риск за самата банка представлява на първо място е самата тя като организация и начина, по който реагира или не на вътрешните и външни заплахи.

Оперативните рискове често се срещат при операции с по-високо изразена степен на сложност на предлагания от банката продукт, изискващи ниво на компетенции на персонала. Често пряко замесените в измамата лица са разполагали с надеждна вътрешна информация, ползвали са се с доверието на управляващите и колегите си и провокирани от личен материален интерес са нарушили своите правомощия. Лицата, ангажирани с вътрешния контрол не са съумели или ненавременно са реагирали на заплахата. И резонно достигаме до въпроса дали правилно е определен и оценен риска от настъпване на загуби за финансовата институция, адекватни ли са били действията на лицата, отговарящи за сигурността и какви мерки би следвало да бъдат предприети за недопускане на повторни вреди за организацията [5], [6].

Нерядко след събитието се установява, че е налице преплитане на функциите между служителите и лицата, осъществяващи втория контрол, т.е липсва разграничаване между контролните и оперативни функции. Използваният софтуер предполага забавяне в отчитането или непълно отразяване на операциите, което създава предпоставки да бъдат укрити и задържани във времето данни за извършени злоумишлени вреди. Предоверяването към служител, група лица или убеждеността в съвършенството на използваните технологии също е съществен момент, изискващ допълнително анализиране. Подценяването на дейността на структурите, ангажирани с осигуряването на мероприятия по контрол, превенция и противодействие на заплахи за банката, често е причина организациите да бъдат изложени на риск [5], [6].

Операционните рискове е трудно да бъдат определени, измерени и да им бъде направени оценка на въздействието, тъй като те са може би едни от най-всеобхватните, тъй като съпътстват почти всяка операция, сделка или събитие в ежедневието на една банка. При търговските операции в дадена финансова институция съществува пряка зависимост между степента на предприетия риск и очакваната доходност, като респективно по-високият риск би допринесъл за по-добрата доходност от дадена сделка. Операционните рискове от друга страна не са повлияни от подобна зависимости или от

волатилността на пазарите, а възникват вътре в корпорацията.

В изследване на Базелския комитет по банков надзор, изследващо рисковите събития в дейността на търговските банки, водещо място заемат злоупотребите в клоновите подразделения на банките. Това е показано на фиг. 1.

Фиг. 1.

При вземането на реални решения в условията на риск се използват методите на изследване на операциите. Рационалната теория на риска се основава на оптималността на решенията, а именно да бъде избрана най-подходяща алтернатива, която да увеличи доходността, полезността на вземащия решения. Моделът е изцяло математически и се абстрахираме от характеристиките на отделната личност, неговите убеждения, способности, емоции и т.н.

В последните две десетилетия дейността на банките до голяма степен придоби публичност чрез осигуряване на достъп до финансовите им доклади, информация за собствениците на капитала и мениджмънта, както и информация за основните събития и процеси в организацията, тяхната инвестиционна политика и т.н. Оценката на въздействието на операционните рискове е съществен фактор за определяне на рейтинг на дадена банкова институция.

Прилагането на международните стандарти за определяне на изискуемия размер на капитала за покриване на загубите вследствие операционни рискове изисква от банките прилагането на базов подход ,стандартизиран индикатор и усъвършенствани методики за вътрешна оценка и управление на риска.

Базовият индикатор е предпочитан при приблизително 40% от финансовите организации, останалите два метода са с приблизително сходни тежести.

Разпределението на трите основни подхода за оценка и управление на операционните рискове в международен мащаб. Това е показано на фиг. 2.

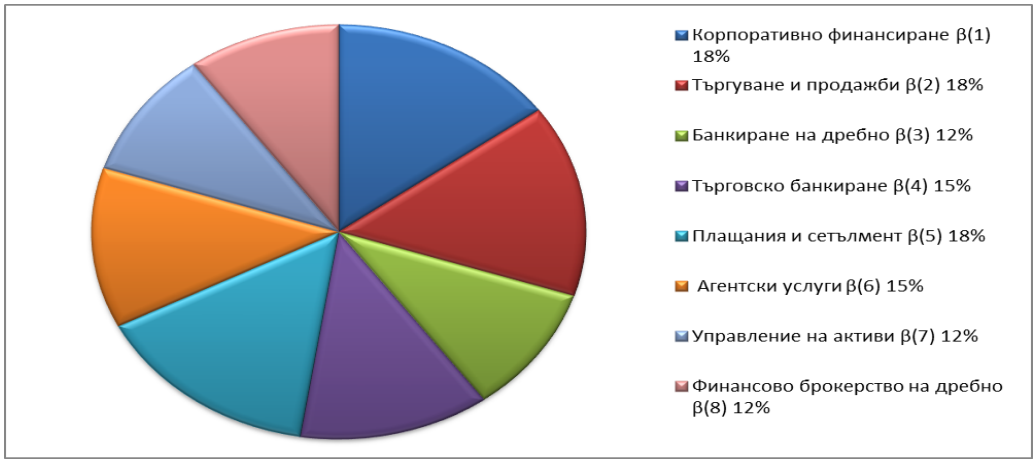
Фиг. 2.

Подходът на базисния индикатор предполага пряка зависимост между предприетите операционни рискове и мащаба на дейност на дадената банка. Резервите, които би следвало банката да осигури, за да посрещне операционен риск се изчислява по следния начин. Капиталовото изискване за операционен риск представлява сумата на брутния доход на банката за i – та година умножен по α / константа равна на 15%, фиксирана от Базелския комитет за банков надзор/ и разделена на n / броят на последните 3 години, през които банката има положителен брутен доход/. Методът е значително опростен и приложим за по-малки финансови структури, където не се прилагат методики за оценка на операционните рискове. Недостатък на този метод е невъзможността да се изследват причините за възникване на операционните рискове.

Стандартизираният подход отчита едновременно няколко избрани от банката направления и отчита за всяко едно от тях необходимите резерви, които би следвало да бъдат заделени, като стойността на капиталовото изискване е средно аритметична на обобщените рискови експозиции по дейности за последните три години. Т.е. базиран на годишния брутен доход по групи дейности за предходните три години и коефициент β1-8 - фиксиран процент, определен от Базелския комитет.

Коефициент β1 съгл. Базелския комитет за банков надзор, определящ нивото на регулативния капитал по Бизнес линии на база брутния доход. Това е показано на фиг. 3.

Тази класификация е единна за всички, които я прилагат и основно е насочена към структури, които осъществяват дейност в относително по-голям брой направления и същевременно все още не са създали собствена методика и структури, ангажирани с управлението на операционните рискове.



Фиг. 3.

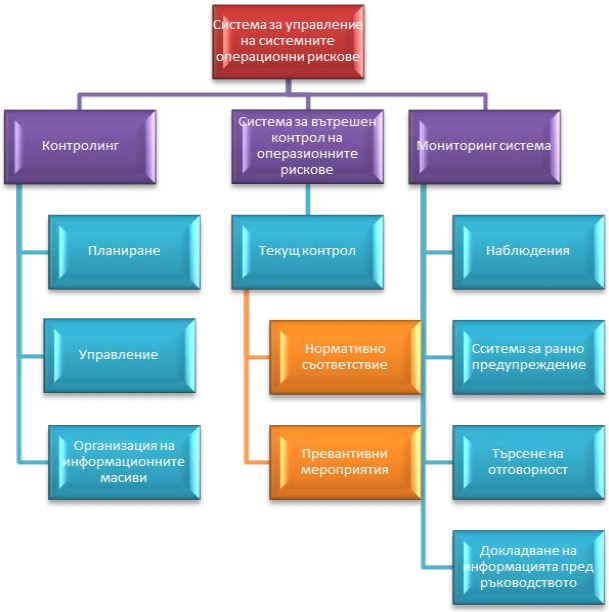
Вътрешни усъвършенствани системи, разработени в унисон с регулациите на пазара. В големите банкови организации, гаранция за ефективността на системата за управление на риска е участието на мениджмънта, както и наличието на процедури и инструкции, съобразени с приоритетите на организацията, осъществяването на надзор и системен вътрешен контрол. Необходимите минимални изисквания по отношение на резервния капитал се определят като сума на очакваните и инцидентни загуби, настъпили вследствие на операционни рискове. Тъй като голяма част от финансовите институции предпочитат да заделят действително минимални резерви, това от своя страна изисква да инвестират в създаване на структури за управление на риска, разработване и прилагане на сложни и прецизни методики за идентификация и управление на операционните рискове.

Ръководителите на банките неминуемо носят отговорност за утвърждаването и прилагането на стратегия за управление на риска. А специализираните звена разработват методики, процедури за управление и оценка на риск, вътрешни нормативни актове и инструкции, които да гарантират интегрирането на системата на менажиране на риска в ежедневната дейност на банката. Риск-управленията определят нивата на допустимия за банката риск, изготвят методики за ограничаването му, а също така следят за прилагането на системата и отчитането на рисковите събития..

Системата за управление на рисковите процеси в дадена банкова организация, е базирана на основата на три ключови сегмента - контролинг, система за вътрешен контрол на операционните рискове и система мониторинг и превенция. Би могла да бъде онагледена по следния начин. Това е показано на фиг. 4.

В Европа по данни на The Joint Forum "Operational risk transfer across financial sectors", загубите в следствие операционни рискове съставляват над 60 % от общия размер на щетите. Това е причината през последните години, голяма част от усилията на банките да бъдат насочени за управление и овладяване на операционните рисковете, а също така и да бъдат заделени не малко средства за създаване на специализирани звена.

Въвеждането на високотехнологични системи за наблюдение, ранно известяване и превенция на злоупотреби е до голяма степен ключово за недопускане и минимизиране на загуби, както финансови, така и репутационни.



Фиг. 4.

Внедряването на системата за управление на риска, изисква създаване на бази данни с исторически точна информация за характера и степента на рисковите събития, въвеждани на ясни и точни правила за работния процес по видове операции и направления, данни от мониторинг системите, както и перманентен контрол върху документалното отразяване на дейността в банковите институции.

3. Заключение

В заключение ефективността на търговските банки, се свързва до голяма степен с присъден висок финансов рейтинг, постигната нетна печалба, добрата репутация, но също така и с не по-маловажно значение е нейната устойчивост на външни и вътрешни операционни рискове и способността на организацията да се справя с тях, претърпявайки минимални загуби.

ЛИТЕРАТУРА:

[1] Basle Committee on Banking Supervision, “The Quantitative Impact Study for Operational Risk: Overview of Individual Loss Data and Lessons Learned”, January 2002.

[2] Beekman, Frank, “Application of the Loss Distribution Approach to quantify Operational”, Maribor 2008.

[3] European Commission, “Executive summary of the impact assessment”, Commission staff working paper, SEC(2011) 950 final, Brussels, 20.7.2011.

[4] The Joint Forum "Operational risk transfer across financial sectors" August 2003.

[5] Dimanova, D., Kuzmanov, Z. Measuring and assessing risk. SocioBrains, international scientific online journal publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63 – 69, Issue 32, April 2017.

[6] Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, ISSN 2367-5721. www.sociobrains.com. Issue 36, august 2017, pp.67-73.

Име на автора: докторант Жанета Станимирова Георгиева-Панайотова
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“

MATTEX 2018, Volume 2, part 1 SECTION Student (Information, Technical and
CONFERENCE PROCEEDING, v. 2, pp. 304 - 309 Economical Problems of Security Systems)

CORRUPTION IN THE PUBLIC SECTOR

ANASTASIA G. HRISTOVA, NURAY M. IDAETOVA

ABSTRACT: *The political reform, although intuitively associated with our current tasks often regarded corruption as isolated degenerate phenomenon caused by a few greedy crooks whose arrest and eventual conviction will solve the problem.*

KEYWORDS: *Corruption, Public sector.*

КОРУПЦИЯ В ПУБЛИЧНИЯ СЕКТОР

АНАСТАСИЯ Г. ХРИСТОВА, НУРАЙ М. ИДАЕТОВА

АБСТРАКТ: *Политическата реформа, въпреки че е интуитивно свързана с настоящите ни задачи, по-често разглежда корупцията като изолирано, изродено явление, причинено от няколко алчни мошеници, чието задържане и евентуално осъждане ще разреши проблема.*

1. Въведение

След като се съгласим, че проблемите с точното дефиниране на политическата корупция се пораждат от съперничещите си концепции за природата на политиката, необходимо е да приемем и факта, че поддаването на западната арогантност или културен релативизъм също е в противоречие с единодушието по въпросите за природата на политиката, тъй като така се подкопават основите на евентуално съгласие между теориите на публичната длъжност и публичните интереси. Остава ни проблемът за нормите и стандартите за политика, които трябва да приемаме [11].

Първата необходима стъпка е да се направи разграничение между политиката и другите сфери и видове разпределение, размяна и вземане на решения. Един от начините е политиката да се възприеме като особен вид отношения, различни от останалите - например общностни, пазарни, роднински или тези между патрон и клиент. Макар и да е трудно да се прокара граница между въпросните видове отношения, бихме могли да ги противопоставим на базата на идеално-типични отношения [11].

Общностните отношения пораждат спонтанна солидарност, чиито корени се крият в роднинските и групови взаимоотношения. По своя характер те са предписани - принадлежността не се определя от волята, а от „природата".

Размяната в рамките на такива взаимоотношения е често силно символична, натоварена с фактори като уважение, доверие и статут. Нарушаването на нормите на размяна или на управляващите отношения от страна на членовете на групата е срамен акт и предизвиква съответните наказания или искания за ритуално прочистване.

Членовете на такива групи търсят уважение, което се постига с помощта на конформизъм, а водачеството се крепи на традиции и статут [11].

2. Изложение

Пазарните отношения включват разпръсната конкуренция между фирми или индивиди, които са формално равнопоставени, но влизат в такива взаимоотношения с цел

реализиране на максимална печалба. Отношенията в рамките на пазара са изцяло инструментални: мотивите на отделните индивиди са ясно насочени към максимално задоволяване на интересите им. В идеалния случай икономическата размяна води до печалби, които са измерими и еднократни; не се поемат ангажименти за бъдещи транзакции и не се създават постоянни отношения. В условията на чисто пазарна размяна фамилните и групови отношения се вземат предвид дотолкова до¬колкото биха донесли някакви предимства на индивида. При такива условия няма място за водачество, тъй като липсва стремеж за колективна дейност, а цялата необходима координация се осъществява от цените [11].

Ето как Гелнър описва отношенията патрон-клиент:

Патронажът е несиметричен и се гради на неравенство на властта: той се стреми да създаде разширена система; да е дългосрочен или поне неограничен от една единствена сделка; да се характеризира със специфичен дух; и макар не винаги неморален или незаконен, да остане извън общоприетите официални норми на морала в съответното общество... Това, което прави едно общество патронажно, е не самото наличие на този синдром, а неговата стабилна и доминираща позиция във вреда на другите принципи на социална организация [1].

Системите патрон-клиент са най-разпространени там, където е налице ненапълно централизирана държава, несъвършена бюрокрация или несъвършен пазар. Патронът действа като средство за набавяне на стоки и услуги, от които се нуждае клиентът и които не могат да бъдат осигурени от държавата или пазара; клиентът обикновено плаща за услугите, извършвани от неговия патрон с готовността сам да извърши услуга по желание на патрона. Размяната не е симетрична тъй като патронът притежава значителна власт и влияние, а клиентът - малко или никакви; но патронът повишава статута си и често печели много по-осезателно и от факта, че поддържа в клиентите си чувство на зависимост и задълженост. Политиката е свързана с изкуството да се управлява. Политическите отношения не са нито общностни, нито пазарни по своята същност - макар че имат нещо общо с тях [11].

Както и общностните отношения, те предполагат наличието на йерархически ред и създаването на модел на власт; за разлика от тях обаче, легитимността им не зависи изключително и само от традициите и правилата на солидарност. Оправдаването на политическата власт се нуждае от по-широка претенция за легитимност. Политиката се различава от пазара по това, че макар и да търси сделка в процеса на борбата за легитимност, тази сделка не се смята за специфичен акт на държавата, а се приема като създаващо prima facie право на власт, с което по легален път може да упражни принуда. Следователно тези, които управляват, очакват управляваните от тях да са съгласни не защото от това ще произтекат максимални печалби, а заради претенциите си към правото на власт и признаването на това право от страна на гражданите.

Истинската политическа власт не се гради нито на заплахите от наказание, нито на убеждаването в процеса на спора, а на признаването от гражданите на правото на заповядващия да управлява [2].

Развитието на властта от дейност на един отделен индивид до публична функция се характеризира и с разширяване на критериите за легитимност от едноличната воля на владетеля до колективния и публичен възглед за уместността на дадено действие и неговия резултат. Силата на аргумента, че управлението трябва да се съобразява с публиката, се дължи на факта, че характерът на обсъжданията, в които са ангажирани участниците, е по-различен от тези в едно гражданско общество или домакинство. Оправдаването в рамките на публичната сфера се дължи не на силата и властта на нечии

индивидуални предпочитания, а на по-всеобхватни принципи, извлечени от правото и общото благо. Основното различие между политическата власт и другите форми на отношения и размяна е това, че тя се позовава на публичните стандарти за оправданост и уместност [11].

Некомпетентността може да се оприличи на вид корупция. Тя обаче не поставя под въпрос гореспоменатото разграничение - може да доведе до конфликт, но не го обявява в сърцето на политическата система. Както видяхме, факторите, смятани за централни в поддържането на подобно разграничение варират и могат да бъдат яростно оборени в различните политически системи. Нещо повече - много дейности, наложени от закона или незабранени от него, могат да доведат до ерозия на това разграничение и до избухването на конфликт. Ето защо е необходимо да се запознаем с едно ядро от случаи на корупция, в които незаконността и подмяната на частни и публични интереси присъства съвсем съзнателно, както и с една друга група по неясни случаи, при които са необходими по-сложни заключения за това дали изобщо и до каква степен са покрити различните критерии [11].

Подобен по-широк анализ трябва да бъде допълнен от факта, че корупцията се различава от другите форми на деструктивно политическо поведение, защото тя подкопава разграничението между частни и публични проблеми и интереси [11].

Най-често даваните аргументи за функционалността на корупцията са тези, засягащи икономическото развитие. В своята статия изхождам от схващането, че политическият ред в една държава е в най-общи линии подходящ за условията в тази държава. Очевидно е обаче, че това не винаги е така. По-голяма част от обществата на социалистическите държави в Източна Европа бяха неефикасни и дълбоко разядени от корупция - естествен резултат от ограничените възможности на хората да постигнат поставените цели или извършат дадени услуги без системно да нарушават правилата [3]. При такива условия, корупцията бе еднакво полезна както за икономиката, така и за запазване на политическата стабилност - макар и в кратки и умерени срокове. В такива случаи обаче е налице такова разминаване между официалната и неофициална култура, че става повече от ясно, че политическата система на авторитарното разпределение е в по-голямата си част абсолютен хаос и единственото условие да се приложи на практика е държавата да обяви война на обществото. На практика, в различните сфери политическото разпределение отстъпва място на скритата пазарна икономика, или по-често - на други видове размяна, например патриархално или клиентелистко. Подобно подчинение може и да доведе до икономически прогрес, но може и да предизвика политически промени. Процесът си има своята цена: макар че не се стига до открит конфликт, пораждат се прикрити форми на господство на отделни групи и индивиди над други и съществува опасността корупционни, но полезни действия да се разпространят до такава степен, че възстановяването на политическия ред на нови основи да стане почти невъзможно [11].

Нещо повече - твърденията, че корупцията е полезна, са подчертано обезпокоителни на места, където политическата култура съществува само на думи и където впоследствие разкритието на прикрити действия може да доведе до санкции. При подобни условия на места, където изглежда няма друга алтернатива, освен да се включиш в даване и вземане на подкупи, спекулата и т. н., рядко се стига до истинска пазарна икономика в разменните отношения. Напротив, размяната се усложнява - желанието на човек да се включи в дадена дейност означава, че другите имат за него информация, която би предпочел те да не използват, за което той плаща определена цена. В този смисъл гореспомената форма на размяна подчертано се различава от законните пазарни отношения. В резултат при сделката се плаща цена, независимо от това, че изходът й остава отворен - участниците в

сделката остават изложени на действията на другата страна, както и на потенциални бъдещи последици [11].

Колкото по-близки в своето отношение към политическия ред са участниците, толкова по-малък е проблемът. Две страни, които нарушават правилата и го правят с еднакво нежелание, плащат еднаква цена при размяната. Но ако зад гърба на едната стои цял синдикат на организирана престъпност, а другата търси еднократна размяна извън системата, на която по принцип си остава вярна, то тогава истинската цена, която се заплаща, може да се окаже съвършено различна. Под натиска на обстоятелствата, хората могат да се ангажират с дейности, които според тях нямат особени бъдещи последствия. От една страна, подобни сделки може и да са полезни за икономическото развитие или за размразяването на една политически обречена икономика, но от друга те са и предпоставка за възникването на отношения, при които дадени групи могат систематично да определят поведението на други в бъдещето. Не е лесно да се прикрие едно опетнено минало [11].

На практика присъствието на умерена и широко разпространена корупция изисква от хората да рискуват бъдещия си имунитет - подобен риск обаче невинаги е оправдан и те се превръщат в жертви на тези, които държат за тях информация, която биха искали да задържат в тайна. Нещо повече - създават се предпоставки за несъобразяващите се с едно бъдещо наказание да се опитат да блокират изграждането на каквато и да е система, която би могла да им поиска отговорност за минали действия - и това важи не само за тези, които се придържат към неполитически разрешения на проблемите, но и за онези, които имат интерес да избегнат всякакво политическо разрешение, което би ги накарало да плащат за миналите си деяния. Съюзите между мафиотски групировки и политици с общи интереси в избягването на определени видове контролни механизми и публична отговорност могат да породят и слаб политически контрол в една държава [11].

Политическата реформа, въпреки че е интуитивно свързана с настоящите ни задачи, по-често разглежда корупцията като изолирано, изродено явление, причинено от няколко алчни мошеници, чието задържане и евентуално осъждане ще разреши проблема. Някои са определили това като „моралистична" концепция за корупция, в която, както във всяка морална позиция, има ясен виновник и със заклеймяването му нещата се оправят. Подобна, за съжаление, е ситуацията с повечето готови рецепти и нещата често не са (ако изобщо някога са) толкова прости [11].

Публичната администрация още в основополагащите си принципи се е посветила на установяването и поддържането на „доброто управление" - това изглежда достатъчно настоятелна подкана за изучаване на корупцията. Като изключим рядкото формално съгласие, общо взето потвърждаващо правилото, тази подкана изцяло се отхвърля.

Така учените в областта на публичната администрация са дори по-нехайни в това отношение от своите колеги политолози, нехайство, което, както Симча Върнър допуска, „се дължи преди всичко на аксиоматичното вярване на предишните учени, че американската публична администрация е морална по самата своя същност" [4].

Литературата по публична администрация бърза назидателно да посочи с пръст към чужбина, цитирайки примери за разпространена политическа корупция в развиващите се страни. Всъщност някои автори смятат, че корупцията осигурява важни възстановителни стимули и всекидневни допълнителни печалби в периода на политическото развитие на дадена нация. Според тях възможността за лично облагодетелстване чрез публична корупция привлича квалифицирани служители на иначе непривлекателната и неблагодарна чиновническа работа, подтиква една иначе мудна административна система

към своевременни действия, необходими за икономическото развитие и се явява като социализиращ фактор за лишените от права части на политическата система.

Взета за чиста монета, функционалната интерпретация е донякъде правдоподобна и привлекателна с твърдението, че корумпираната администрация е само следствие от тежките времена и голямото напрежение. Но функционализмът, присъщ на тази интерпретация, също така предполага, че когато постигне напредък в т. нар. процес на политическо съзряване, една нация някак по естествен път ще се отърси от практиките на корупция, подобно на непослушните деца, които се превръщат в отговорни възрастни хора. Историческият опит, за съжаление, още веднъж убедително показва, че това е далеч от истината [11].

Когато публичната администрация реши да се захване с корупцията в Съединените Щати, нейните препоръки се основават главно на модела на моралността и следователно могат да се разглеждат като наивно оптимистични и неефективни: според тях, една нова наредба или главен инспектор на едно място, преработен кодекс на поведение на друго или Закон за етика в управлението привидно биха върнали органа-нарушител в правилната административна насока и направление [11].

Убедителна илюстрация за неохотата на политолозите и публичните администратори за системното изучаване на корупцията е, че единствената книга, която подробно анализира политическата корупция, е написана от икономист - Сюзан Роуз-Акерман. Роуз- Акерман формулира обосновката на своята работа с възхитителна прямота: „Каквито и да са другите проблеми, обществата очевидно не използват единен, последователен метод за вземане на разпределителните решения". Корупцията е само един, макар и несанкциониран метод, сред многото други. Основавайки се на наличието на пазарни сили (т.е. икономическа конкуренция) и - на икономически жаргон - на желанието на „корумпирани длъжностни лица да придобият целия (икономически) излишък, създаден от определена програма", Роуз-Акерман разглежда податливостта на много политически системи към корупция, състояща се от различни типове и комбинации законодателство, обединени от определен интерес групи и бюрократични апарати [5]. Също така тя изследва и традиционните за всеки набор от ситуации решения, показвайки като цяло тяхната икономическа погрешност. Разбира се, има известна елегантност и безпристрастие в това да се разисква „оптималното количество корупция" от гледна точка на „пределните обществени разходи" [6], [7].

Едно строго икономическо гледище за корупцията би се оказало непълно и оттам неадекватно, защото фокусът върху корупцията ще е „в рамките на един модел на рационален индивидуален избор и ще обръща малко внимание на цялостното влияние върху обществото" [8]. И пак на икономически жаргон, „полезността" на един икономически анализ на корупцията не може да бъде пренебрегната, но той е ефективен само „маргинално".

Роуз-Акерман завършва книгата си с откритото признание, че личните и политическите ценности пречат на аналитичното вникване в корупцията, което нейната дисциплина осигурява в най-голяма степен от гледна точка на това какво да се направи, за да се минимизира корупцията: „Опитът да се приложат икономически методи за обобщаване на политологични проблеми в крайна сметка ни принуждава да признаем ограниченията на икономическия подход сам по себе си. Макар често да могат да намалят стимулите за корупция, информацията и конкуренцията не могат напълно да заместят личната почтеност на политическите актьори" [9], [11].

3. Заключение

Накратко, икономиката изглежда неспособна, а политическата наука като че ли не желае да се сблъска с въпросите, поставени от политическата корупция и което е по-съществено, отказва да се изправи пред въпроса какво може да се направи, за да се ограничи корупцията и последствията от нея. Може би донякъде е изненадващ и фактът, че и юридическата наука не се представя по-добре. След преглед на правната литература Дениъл Лоуънстийн заключава, че „каквито и да са пропуските на социалните учени в това отношение, те бледнеят пред тези на юристите, които изцяло пренебрегват проблема" [10], [11]. Макар че ще използваме идеите на споменатите по-горе дисциплини, критерият за политическата уместност е онзи, към който това изследване се стреми.

ЛИТЕРАТУРА:

[1] Ernest Gellner и John Waterbury (редактори), Patrons and Clients In Mediterranean Societies, (Лондон, Duckworth, 1975).

[2] Авторитарните отношения не почиват нито на здравия разум, нито на властта на този, който командва: общото между страните е йерархията, чиято справедливост и легитимност се признава и от двете и в която и двете имат предопределено място." Hannah Arendt, Between Past and Future: Six Exercises in Political Thought, (Harmondsworth, Penguin, 1992), стр. 93.

[3] Това наистина се случи в някои части на Русия, след като комунистическата система започна да се разпада - виж Leslie Holmes, The End of Communist Power: Anti-Corruption Campaigns and Legitimation Crisis (Карлтън, Мелбърн, Melbourne University Press, 1993).

[4] Simcha B. Werner, „New Directions in the Study of Administrative Corruption," Public Administration Review, Vol. 43, No. 2 (March/April 1983). p. 146.

[5] Susan Rose-Ackerman, Corruption: A Study in Political Economy (New York: Academic Press, 1978, съответно отр. 1 и 92.

[6] Вж Fred W. Riggs, Administration in Developing Countries (Boston: Houghton Miffin, 1964); виж и Joseph S. Nye, Jr., „Corruption and Political Development," в изданието на Samuel P. Huntington, Political Order in Changing Societies (New Haven, CT: Yale University Press, 1968); и Michael Johnston, „The Political Consequences of Corruption," Comparative Politics, Vol. 18, No. 3 (July 1986), стр. 459-477.

[7] As in Klitgaard, Controlling Corruption (Berkeley: University of California Press), стр. 26.

[8] Nas et al., „A Policy-Oriented Theory of Economics," стр. 108.

[9] Rose-Ackerman, Corruption, p. 216.

[10] Daniel H. Lowenstein, „Political Bribery and the Intermediate Theory of Politics," UCLA Law Review, 34, No. 4 (1985), стр. 785.

[11] Център за изследване на демокрацията. Корупция и антикорупция. 2003 г. ISBN 954-477-102-6.

Име на автора: Анастасия Георгиева Христова
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.
Име на съавтора: Нурай Метинова Идаетова
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.

DISSEMINATION OF NARCOTIC SUBSTANCES IN THE PUBLIC AREA

AYSEN B. BASRI, DZHANSU E. MUSTAFOVA, ELITSA B. VASILEVA

ABSTRACT: *The term "narcotic" is derived from the Greek. It is believed to have been used for the first time by the ancient physician Hippocrates in the form of "narcozis" (narcosis) to designate substances with paralytic action. Today the term covers a large number of substances and agents united by one: they affect the nervous system. Their action may be blocking or paralyzing - such as painkillers; may be stimulating, exacerbating senses such as caffeine or some doping, and may cause illusions and hallucinations.*

KEYWORDS: *Corruption, Narcotic, public sector, security, terrorism.*

РАЗПРОСТРАНЕНИЕ НА НАРКОТИЧНИ ВЕЩЕСТВА В ОБЩЕСТВЕНОТО ПРОСТРАНСТВО

АЙСЕН Б. БАСРИ, ДЖАНСУ Е. МУСТАФОВА, ЕЛИЦА Б. ВАСИЛЕВА

АБСТРАКТ: *Понятието "наркотик" произлиза от елински. За пръв път се смята, че е използвано от древния лекар Хипократ във формата "ναρκωσις" (narcozis - наркоза) за обозначаване на вещества с паралитично действие. Днес понятието обхваща голям брой вещества и агенти, обединени от едно: въздействат върху нервната система. Действието им може да е блокиращо или парализиращо - като например болкоуспокояващите; може да е стимулиращо, обострящо сетивата, като на кофеина, а и могат да предизвикват илюзии и халюцинации.*

1. Въведение

Понятието "наркотик" произлиза от елински. За пръв път се смята, че е използвано от древния лекар Хипократ във формата "ναρκωσις" (narcozis - наркоза) за обозначаване на вещества с паралитично действие. Днес понятието обхваща голям брой вещества и агенти, обединени от едно: въздействат върху нервната система. Действието им може да е блокиращо или парализиращо - като например болкоуспокояващите; може да е стимулиращо, обострящо сетивата, като на кофеина, а и могат да предизвикват илюзии и халюцинации [1], [2], [3], [4], [5], [6].

Потискащи нервната система са обикновено наркотиците - аналгетици, болкоуспокояващи медикаменти - широко употребяваният в медицината морфин, опиум, сънотворни и други. Изострящи нервната система агенти са често употребявани поради митът за известната им безопасност и краткосрочните ползи. Такива са кофеин, кокаин, амфетамини, никотин и други, водещи до временно изостряне на сетивата. Халюциногените пък вещества, въздействащи централно на нервната система и предизвикващи халюцинации, миражи. В това число се включват широко разпространени наркотици, като LSD, Mescaline и др [1], [2], [3], [4], [5], [6].

.

Проблемът с наркотиците не би бил така сложен, ако те не създаваха зависимост. Наистина, не всички видове правят потребителя зависим, други пък бавно работят в тази насока. Това е характерно обаче точно най - силните и опасни вещества.

2. Изложение

Наркотици и зависи Зависимостта бива два вида – психическа и физическа. За да е налице зависимост, трябва да има осъзнато търсене, желание за наркотика. Именно за това има ли зависимост, тя винаги е психическа. Наркотикът заема място в желанията на наркомана, стремежът става неконтролируем, дори "заразеният" е склонен да пречупи всякакви бариери и да направи много компромиси, които иначе не би направил, за да се сдобие с обекта на желанието си. Тази зависимост е със сложен механизъм, трудно податлива на лечение. Вероятно има връзка с еуфорията и щастието, които наркотикът предизвиква и индивидуалният начин, по който всеки приемащ преживява това състояние.

Физическата зависимост обикновено настъпва по-късно или не присъства. При нея тялото на наркомана е до такава степен привикнало с наркотика, че приема за неестествена липсата му. Организмът проявява симптоми на неблагоразположение, болест, пристъпи при отсъствието на наркотика; лишението може дори да застраши живота на наркомана. В този случай говорим за пристъпи на абстиненция. Психическата зависимост усилва пристъпа, добавя към него фактори като паника, агресия, които много усложняват заболяването [1], [2], [3], [4], [5], [6].

Допълнителен проблем е, че с времето организмът започва да се "нагажда" по-бързо към дозата. Често организмът на ползващите упойващи вещества бързо привиква и се стига до състояние което води до бързо увеличаване на дозите.

Налице е една порочна спирала. От психическа зависимост наркоманът започва да се стреми към по-пълно удовлетворение и увеличава дозата. Създава се и физическа зависимост, с която организмът се бори, като си изработва толерантност към наркотика. Това обаче е в разрез с психичната зависимост и търсенето на удовлетворение от страна на наркомана и той отново увеличава дозата. И така докато наркотикът застраши живота му(свръхдоза) или докато по един или друг начин цялата процедура не премине в състояние на контрол, който за съжаление най-често е външно наложен контрол против който поразеният се съпротивлява, а не самоконтрол на наркомана.

Приемът на свръхдози наркотици е причина за смъртта на около 8 500 души всяка година, като 2100 лица умират от ХИВ/СПИН, свързан с употребата на наркотици, а 3000 лица се заразяват с ХИВ поради тяхната употреба [1], [2], [3], [4], [5], [6].

Няма общовалидна причина за пристрастяването към наркотиците. И все пак към дрогата обикновено се посяга поради:

- Любопитство. Човек, особено когато е млад, иска сам да опита онова, за което е чел и чувал. А наркотиците не престават да бъдат на мода;
- Желание за принадлежност към определена група. Дрогата става нещо като пропуск за някои тийнейджърски общества;
- Стремеж към независимост. Какво ли не прави понякога юношата, за да покаже, че е пораснал и че не му "пука" какво ще кажат възрастните?!
- Страст за нови удоволствия. Тук рисковете само усилват тръпката;
- Очакване за по-добри постижения. Това в най-голяма степен се отнася за стимулантите и халюцигените, набедени, че откриват "непознати творчески хоризонти"
- Потребност от отпускане и пълен покой. Този мотив е особено характерен за опиатите, сънотворните и транквилизаторите;
- Опит за бягство от угнетяващата реалност. Младия човек по принцип е критично настроен към заобикалящия го свят, още повече в периоди на криза. Бягството от действителността понякога е спасение от невъзможността за приспособяване или от липсата на самочувствие

Наркомания и престъпност

Наркоманията и престъпността имат немалко пресечни точки. Взаимното влияние между двата социални порока е силно изразено в три направления:

- Престъпления, извършвани от наркомани под непосредственото въздействие на дрогата или в състояние на силен глад за нея (посегателства срещу личността, вандализъм, нарушения на обществения ред) [1], [2], [3], [4], [5], [6];

- Престъпления с цел придобиване на наркотици или на средства за тяхното закупуване (кражби, грабежи, измами, проституция);

- Престъпления, свързани с производство, трафик и разпространение на наркотици.

Последния вид закононарушения са особено опасни, защото се осъществяват от могъща организирана престъпност, която е без аналог в човешката история. Противодействието срещу тези престъпления е възможно само при широко международно сътрудничество. Международния контрол се базира на три основни документа на ООН, ратифицирани и от нашата страна:

- Единна конвенция за упойващите вещества от 1961г.

- Конвенцията на ООН за психотропните субстанции от 1971 г.

- Конвенция за борба с незаконния трафик на упойващи и психотропни вещества от 1988г.

Резултати от анализа на ситуацията според стратегия 2009-2013.

- около 560-570 000 български граждани от 15 до 64 години поне веднъж в живота си са употребили някакво наркотично вещество;

- най-масово използвания наркотик е марихуаната;

- употребата на марихуана сред учениците е нараснала от 27,1 на 30,3%.;

- Хероинът пък е все още най-силно свързания с проблемна употреба наркотик, но с нарастваща тенденция към спадане за сметка на стимулантите. Нараства употребата на синтетичните стимуланти - амфетамини и вещества от типа на екстази. При употребата на кокаин също се наблюдава тенденция на увеличение. ;

- запазва се тревожната тенденция да се откриват нови ХИВ - позитивни сред употребяващите интравенозно наркотици.

- - наблюдава се тенденция на намаляване броя на смъртните случаи, свързани с употреба на наркотици - 15 смъртни случая през 2003 г., 74 смъртни случая през 2008 г. 25 случая през 2011 г.;

Българското законодателство ограничава използването на наркотици посредством Закон за контрол върху наркотичните вещества и прекурсорите. Свободната употреба, внос и износ на тези вещества са забранени, допустима е употребата им за медицински цели. Това се контролира от редица органи - специализирани национални и общински центрове, Министерство на здравеопазването, МВР и други [1], [2], [3], [4], [5], [6].

Целта на този закон е да уреди обществените отношения, свързани с контрола върху наркотичните вещества и прекурсорите и в съответствие с изискванията на международните договори, по които Република България е страна и на регламентите на Европейския съюз.

Законът се прилага:

1. за всички растения и вещества, класифицирани като упойващи и психотропни вещества, и препаратите, в които те се съдържат;

2. за всички вещества, използвани при производството на упойващи и психотропни вещества, класифицирани като прекурсори.

С наредба, приета от Министерския съвет, се определя редът за класифициране на растенията и веществата като наркотични, като наименованията на наркотичните вещества се съдържат в списъци, както следва [1], [2], [3], [4], [5], [6]:

1. Списък I - Растения и вещества с висока степен на риск за общественото здраве поради вредния ефект от злоупотребата с тях, забранени за приложение в хуманната и ветеринарната медицина;

2. Списък II - Вещества с висока степен на риск, намиращи приложение в хуманната и ветеринарната медицина;

3. Списък III - Рискови вещества.

Създава се Национален съвет по наркотичните вещества към Министерския съвет като орган за провеждане на националната политика срещу злоупотребата с наркотични вещества, както и за борба с наркотрафика.

Националният съвет по наркотичните вещества осъществява своята дейност съгласно правилник, приет от Министерския съвет.

Председател на съвета е министърът на здравеопазването, а заместник-председатели са главният секретар на Министерството на вътрешните работи, заместник-председател на Държавна агенция "Национална сигурност", заместник-министър на правосъдието.

1. определя и координира националната политика в областта на наркотичните вещества и прекурсорите, като изготвя и предлага на МС да приеме национална стратегия за борба срещу злоупотребата с наркотични вещества и срещу незаконния трафик с наркотични вещества и прекурсори за срок 5 години;

2. предлага на МС да приеме национални програми за борба срещу злоупотребата с наркотични вещества и срещу незаконния трафик с наркотични вещества;

3. предлага на министъра на финансите проектобюджет за провеждане на националната политика в тази област;

4. предлага на МС проекти на нормативни актове, свързани с наркотичните вещества и прекурсорите;

5. дава мнение по проектите за сключване или за присъединяване към международни договори;

6. дава становища за участието на Република България в международни програми, насочени срещу разпространението, злоупотребата и незаконния трафик с наркотични вещества и контролира изпълнението им;

7. определя и утвърждава националните координатори по наркотиците и националните координатори по международни програми и проекти в областта на наркотичните вещества;

8. събира, съхранява, анализира и разпространява информация от министерства и други ведомства, от съветите по наркотични вещества към съответните общини и от юридическите лица с нестопанска цел, която е необходима за определянето, осъществяването и координирането на националната политика в областта на наркотичните вещества.

3. Заключение

Министърът на здравеопазването осъществява контрол върху производството, преработването, вноса, износа, транзита, търговията, съхраняването, отчетността, пренасянето, превозването, употребата и рекламата на растенията и наркотичните вещества и препаратите от списъците, както и върху лечението на лица, зависими от наркотични вещества [1], [2], [3], [4], [5], [6].

Министърът на здравеопазването осъществява контрол по изпълнението на задълженията, произтичащи от международните договори, по които Република България е страна.

Министърът на образованието, младежта и науката и министърът на здравеопазването осъществяват контрол върху превенцията на употребата на наркотични вещества.

Министърът на здравеопазването и министърът на труда и социалната политика осъществяват контрол върху психосоциалната рехабилитация на лица, зависими от наркотични вещества [1], [2], [3], [4], [5], [6].

При осъществяване на контрола министърът на здравеопазването се подпомага от длъжностни лица от Националния център по наркомании към Министерството на здравеопазването.

Контролът на територията на страната върху лечението на лица, зависими от наркотични вещества, се осъществява от служители на регионалните здравни инспекции с висше медицинско образование.

ЛИТЕРАТУРА:

[1] Банчева, А. Превенция на употребата на наркотични вещества в България. Социална медицина, (2), 14-16, 2016 г.

[2] Колева, Н., Хаджиделева, Д., & Гавраилова, Д. Влиянието на алкохола и наркотичните вещества върху сексуалното поведение на учениците. Management & Education/Upravlenie i Obrazovanie, 2016, 12.

[3] по Наркотични, Н. С. 2. Вещества (Vol. 66). Годишен доклад по проблемите, свързани с наркотиците и наркоманиите в България 2006, 7-9, 63.

[4] Колев, В. В. Анализиране параметрите на образа на потребителя на незаконни наркотици. Научни трудове на Русенски Университет «Ангел Кънчев».–2011.

[5] Стоянов, М. Правна характеристика на понятието" наркотично вещество" според българското законодателство.

[6] [онлайн]. [прегледан 23.09.2018]. http:// https://bg.wikipedia.org.

Име на автора: Айсен Б. Басри
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.
Име на съавтора: Джансу Е. Мустафова
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.
Име на съавтора: Елица Б. Василева
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.

MATTEX 2018, Volume 2, part 1
CONFERENCE PROCEEDING, v. 2, pp. 315 - 319

SECTION Student (Information, Technical and Economical Problems of Security Systems)

ASPECTS OF MIGRATION PROCESSES IN THE REPUBLIC OF BULGARIA

BLAGOVEST P. YOSIFOV, SIMEON S. KRASTEV, MARIN G. GANCHEV

ABSTRACT: *In today's globalized world people are constantly moving. Migration destroys the traditional differences between cultures, ethnic groups and languages and contributes to diversity, cultural and economic wealth. Many people perceive migration as a challenge or even a threat. It is a challenge for human rights mechanisms that are struggling to ensure the full enjoyment of human rights by all, including migrants, because the human rights of migrants are often violated.*

KEYWORDS:. *Migration, the forms of migration, movement of people.*

АСПЕКТИ НА МИГРАЦИОННИТЕ ПРОЦЕСИ В РЕПУБЛИКА БЪЛГАРИЯ

БЛАГОВЕСТ П. ЙОСИФОВ, СИМЕОН С. КРЪСТЕВ, МАРИН Г. ГАНЧЕВ

АБСТРАКТ: *В днешния глобализиран свят хората се движат постоянно. Миграцията разрушава традиционните разлики между културите, етническите групи и езиците и допринася за разнообразието, културното и икономическо богатство. Много хора възприемат миграцията като предизвикателство или дори като заплаха. Тя е предизвикателство за механизмите на правата на човека, които се борят да гарантират пълноценното упражняване на правата на човека от всички, включително мигрантите, защото човешките права на мигрантите често се нарушават.*

1. Въведение

„Според археолозите, почти всички хора на Земята са мигранти, тъй като човечеството е произлязло от Африка преди около 200,000 години, а след това се е разпространило в целия свят – в Европа, Азия, Австралия и двете Америки… Днес има около 200 милиона мигранти по света, а проблемите и възможностите, свързани с миграцията, ожесточено се обсъждат от политиците и обикновените хора по целия свят… Можем да наречем XXI век „ерата на мигрантите“. [1]

В днешния глобализиран свят хората се движат постоянно. Миграцията разрушава традиционните разлики между културите, етническите групи и езиците и допринася за разнообразието, културното и икономическо богатство. Много хора възприемат миграцията като предизвикателство или дори като заплаха. Тя е предизвикателство за механизмите на правата на човека, които се борят да гарантират пълноценното упражняване на правата на човека от всички, включително мигрантите, защото човешките права на мигрантите често се нарушават.

Миграцията е процес на движение през международна граница или в самата държава и обхваща всички видове движение на хората, независимо от причините за това. Потрудно е да се даде определение за израза „мигрант“. Според Европейския комитет по миграция „изразът „мигранти“ се използва …, в зависимост от контекста, за емигранти, завръщащи се мигранти, имигранти, бежанци, разселени хора и хора с имигрантски произход, и/ или членове на етнически малцинства, които са създадени чрез имиграция“[2].

Международната организация за миграция (IOM) определя мигранта като израз, който „се отнася за всички случаи, при които решението да се мигрира се взима свободно от съответния човек по „лично убеждение“ и без намесата на външен принудителен фактор.“[3]

Горепосочените две определения отразяват конвенционалното разграничение между доброволните и принудителните мигранти. В случай на доброволна миграция, хората напускат своя дом по свой собствен избор, главно заради т.нар. „теглещи фактори“, например по-добри възможности за кариера, въпреки че възможностите, от които могат да избират, понякога са много ограничени. Принудителната миграция повечето пъти е резултат от т. нар. „бутащи фактори“, например преследване, война или глад, когато хората бягат от нарушаването на техните човешки права. Винаги съществува, обаче, комбинация от теглещи и бутащи фактори. Много мигранти напускат държавата си поради икономически причини и за да избегнат злоупотребите с права на човека. Счита се, че дори и икономическите мигранти са принудителни мигранти, когато искат да избягат от ситуации, при които техните икономически права са нарушени.

За Върховния комисар на ООН за бежанците (UNHCR) бежанците и търсещите център за бежанци представляват отделна група хора, защото са напуснали домовете си в резултат на сериозни заплахи за живота и свободата си. UNHCR предупреждава за рисковете от размиване на границата, която разделя бежанците от другите групи мигранти, които са се преместили от своята държава в друга поради икономически или социални причини, за да подобрят живота си, докато бежанците са принудени да избягат, за да спасят живота си и да запазят своята свобода.[4]

2. Изложение

В настоящата статия изразът „мигрант“ се използва в широкия смисъл и включва всички хора, които са напуснали домовете си за по-дълъг период от време. Въпреки това, когато е необходимо, е направено и разграничение. Думата „миграция“ също се използва със значение на международна миграция, освен ако не е отбелязано друго.

Формите на миграция могат да бъдат разграничени според различни фактори, например мотивите, правния статут на засегнатите или продължителността. Някои най-общо използвани категории мигранти са:

- **Мигранти** за временна заетост (наречени още гостуващи работници)
- **Мигранти с големи умения и бизнес мигранти:** професионалисти, които се местят в рамките на международните пазари на транснационалните корпорации и международни организации.
- **Нередовни (или без документи, незаконни) мигранти:** хора, които влизат в дадена държава без необходимите документи и разрешителни
- **Принудителни мигранти:** бежанци, търсещи център за бежанци, или хора, които са принудени да се преместят в резултат на външни фактори, например въоръжени конфликти или екологични бедствия
- **Членове на семейства:** които се присъединяват към техни близки роднини, които вече са мигрирали
- **Завърнали се мигранти:** хора, които се завръщат в техните държави на произход след като са прекарали период в друга държава.

Бежанците, търсещите център за бежанци и вътрешно разселените лица са защитени от националното законодателство. UNHCR определя тези три групи по следния начин.

Бежанец „е някой, който не може или не желае да се върне в своята държава на произход, поради основателен страх от преследване заради раса, религия, националност, членство в определена социална група или политически възглед.“[5]

Търсещите убежище са „хората, които търсят международна защита и за чиито искания за издаване на официален статут на бежанци все още не е взето решение.“[6]

Вътрешно разселени лица (ВРЛ) са хората, „които са били принудени или задължени да избягат или да напуснат домовете си или мястото си на обичайно пребиваване главно в резултат на или за да избегнат ефектите от въоръжен конфликт, ситуации на масово насилие, нарушения на правата на човека или природни или предизвикани от човека бедствия, и които не са преминали международно призната държавна граница.“[7]

Съществува още една група, чиито членове срещат подобни проблеми и нарушения на човешките права, въпреки че може изобщо да не са променили местожителството си: хората без гражданство. Това са хора, които не се считат за граждани на нито една държава; следователно, те не могат да се възползват от правата, които важат само за гражданите. Съществуват различни причини, поради които някой може да стане човек без гражданство, включително разпадане на държави като например Съветския съюз или Югославия, или създаване на нови държави в резултат на деколонизация. Според прогнозите, по света има около 12 милиона души без гражданство. UNHCR получи мандат от Генералната асамблея на ООН да предотврати и намали бездържавността по света и да защитава правата на хората без граждани.

Дискусиите за миграцията обикновено започват от гледна точка на първия свят, концентрирайки се върху потоците между развиващите се и развитите държави. Все пак по-голяма част от мигрантите се движат в своите собствени държави. Броят на вътрешните мигранти е около четири пъти по-голям от този на международните мигранти. В допълнение, дори и ако акцентираме върху хората, които се преминават през международните граници, повечето от това движение се осъществява между държави с еднаква степен на развитие. Приблизително 60% се движат или между развиващи се, или между развити страни, и само 37% от международните мигранти преминават от развиващи се към развити страни, а 3% от развити към развиващи се държави. Що се отнася до бежанците, дисбалансът е все по-явен, тъй като развиващите се държави приемат четири пети от бежанците по света. По този начин товарът за оказване на помощ на търсещите център за бежанци и бежанците по целия свят се поема от някои от най-бедните държави в света. [8]

Общият брой международни мигранти се е повишил от около 150 милиона през 2000 година до 214 милиона души през 2010 г., като 57% от тях са в държави с високи доходи.

Въпреки че броят на мигрантите като процент от световното население е останал стабилен през периода 2000-2010 година, паричните средства, които мигрантите изпращат у дома си, драстично са се увеличили. Официалните и неофициалните парични преводи към развиващите се държави са почти три пъти повече от размера на официалната помощ за развитие. Делът на бежанците сред мигрантите е спаднал от 8.8% през 2000 г. на 7.6% през 2010 г. Съществуват данни, че около 36 милиона души са се преместили в резултат на екологични бедствия през 2008 г. През 2010 г. 43.7 милиона души по света са били принудително разселени в резултат на конфликти и преследвания, като това е най-високият брой за повече от 15 години. Той включва 15.4 милиона бежанци, 27.5 милиона ВРЛ и повече от 837,500 търсещи център за бежанци.

През 2010 г. 44% от бежанците и 31% от търсещите център за бежанци са били деца под 18 годишна възраст. През същата година са подадени 15,500 молби за център за бежанци от непридружени или разделени деца.

Промените в социалната и икономическата обстановка в страната доведоха до проявлението на нови фактори и условия, формиращи миграционното поведение на населението.

Резултатите от проведеното резпрезентативно социологическо изследване за вътрешната и външната миграция на населението показват, че семейните причини са в основата на миграцията за по-голямата част от мигриращите - близо 50%. [11] Изследването е реализирано върху извадка от 25 хил. души и обхваща населението на възраст 15 - 60 години. По тази група причини 57% са се заселили в градовете, 35% - в селата, и 8% - в столицата. Тук основно преселванията са свързани със сключване на брак (30% от всички причини) и придружаване на родители, деца (13%).

Втората по обхват група причини за миграцията е свързана с осигуряването на трудовата заетост. Близо една четвърт (24%) от българите са напуснали своите населени места, за да си намерят работа, а 13% - за да си осигурят работа съобразно притежаваната от тях професионална квалификация. От всички, които са мигрирали с цел осигуряване на работа, 74% са отишли в градовете, 12% - в селата, и 13% - в столицата. За да постигнат съответствие между своята квалификация и трудовата си заетост, по-високо е предпочитанието на мигрантите към градовете и столицата. От тях 77% са се преселили в градовете, 18% - в столицата, и само 5% са намерили подходяща работа в селата.

Общо осигуряването на трудовата заетост е посочвано като мотив за миграция при 43% от преселванията в градовете, 17% - в селата, и 40% - в столицата.

За да си осигурят по-добри условия на живот са мигрирали 22% от населението в този възрастов интервал. От мигриралите по тази причина 68% са се насочили към градовете, 17% - към селата, и 15% - към столицата.

По-добрите условия за живот са били една от причините за 23% от преселванията в градовете, за 17% - в селата и за 23% - в столицата.

Най-общо причините, които пораждат миграциите в България, могат да се разгледат в две групи – причини, които обуславят вътрешната миграция на населението на страната, и причини, които влияят на външната миграция. Причините за вътрешните миграции могат да бъдат: намиране на „постоянна работа“ и „временна работа“, „сключване на брак“, „образование“, „с (при) родители“ и др.

За целия период от 1985 г. до 2016 г. населението на България е намаляло с 1.85 млн души. Повече от половината от това число се дължи на отрицателния естествен прираст (над 52%), докато 48% - на нетната миграция, според анализаторите от "Отворено общество". Въпреки тенденцията на постепенно намаляване на населението на България данните сочат, че делът на нетна миграция в спада на населението намалява до 39% за периода между 1992 г. и 2001 г. до под 10% за периода от 2011 г. насам. Въпреки това все още повече хора напускат страната, отколкото се завръщат.

3. Заключение

Миграцията е феномен, присъстващ в световен мащаб. Добре управлявана, от нея могат да бъдат извлечени ползи както за националния трудов пазар и за икономическия растеж на ЕС, така за благоденствието на самите мигранти и страните им по произход. Непрекъснатата и всеобхватна европейска миграционна политика, основана на солидарност, е основна цел за Европейския съюз. Миграционната политика има за основна задача да установи балансиран подход както към законната, така и към незаконната имиграция. Що се касае до законната миграция, ЕС има компетентността да определя условията за влизане и пребиваване на граждани на трети държави, които навлизат и пребиват законно в дадена държава членка. Държавите членки запазват правото си да определят процен-

та на приемани лица, идващи от трети държави до тяхната територия, за да търсят работа. Относно интеграцията ЕС може да подтикне държавите членки да вземат мерки, насърчаващи интеграцията на законно пребиваващите граждани от трети държави на тяхната територия и подпомагащи техните действия. Колкото до борбата срещу незаконната миграция, от ЕС се очаква да предотврати и намали незаконната имиграция, провеждайки ефективна политика за връщане на лицата при зачитане на основните им права. Правилното контролиране на миграционните потоци гарантирано ще доведе до справедливо третиране на граждани на трети държави, законно пребиваващи в държавите членки, засилване на мерките за 135 борба с незаконната имиграция и насърчаване на по-тясно сътрудничество с трети държави във всички области.

ЛИТЕРАТУРА:

[1] Борис Алтнер, журналист1, 1 Борис Алтнер. Ерата на мигрантите (на руски) http://www.rosbalt.ru/main/2006/06/28/258300.html

[2] Начална страница на Европейския комитет по миграция, http://www.coe.int/t/dg3/migration/European_committee_on_Migration/default_en.asp

[3] Речник по миграция, МОМ, http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/serial_publications/Glossary_eng.pdf

[4] Изказване на UNHCR пред Глобалния форум по миграция и развитие (Брюксел, 9-11 юли 2007), http://www.unhcr.org/468504762.pdf

[5] Конвенция и протокол за статута на бежанците, UNHCR, http://www.unhcr.org/3b66c2aa10.pdf

[6] Глобални тенденции 2009: Бежанци, търсещи център за бежанци, вътрешно разселени лица и лица без граждани, UNHCR, http://www.unhcr.org/4c11f0be9.html

[7] Водещи принципи на вътрешното разселване, ООН, http://www.unhcr.org/43ce1cff2.html

[8] Глобални тенденции[10] 10Източници: Факти и фигури, МОМ (http://www.iom.int/jahia/Jahia/about-migration/facts-and-figures/lang/en); Мониторинг на разселването в резултат на бедствия в контекста на климатичната промяна, OCHA, IDMC & Норвежки съвет за бежанците, 2009; (http://www.internal-displacement.org/8025708F004BE3B1/(28httpInfoFiles)29/12E8C7224C2A6A9EC125763900315AD4/$file/monitoring-disaster-displacement.pdf); UNHCR Глобални тенденции (http://www.unhcr.org/4dfa11499.html)

[9] Изследването е реализирано върху извадка от 25 хил. души и обхваща населението на възраст 15 - 60 години.

Име на автора: Благовест Пламенов Йосифов
Месторабота: Студент от I-ви курс, специалност „Системи за сигурност“, катедра „Управление на системите за сигурност“, Факултет по технически науки, Шуменски университет „Епископ Константин Преславски“
Име на съавтора: Симеон Стоянов Кръстев
Месторабота: Студент от I-ви курс, специалност „Системи за сигурност“, катедра „Управление на системите за сигурност“, Факултет по технически науки, Шуменски университет „Епископ Константин Преславски“
Име на съавтора: Марин Георгиев Ганчев
Месторабота: Студент от I-ви курс, специалност „Системи за сигурност“, катедра „Управление на системите за сигурност“, Факултет по технически науки, Шуменски университет „Епископ Константин Преславски“

MATTEX 2018, Volume 2, part 1 SECTION Studemt (Communication and Computer
CONFERENCE PROCEEDING, v. 2, pp. 320 - 326 Technologies)

3D VISUALIZATION OF PROGRAMS FOR PROGRAMMABLE LOGIC CONTROLLERS THROUGH SOFTWARE PRESETS

DANIEL R. DENEV, VIKTOR V. LILOV, MIHAELA A. KARADOCHEVA

ABSTRACT: *The subject of the study shows us how to create a program for programmable logical controllers and its visualization in 3D. For the creation of the program is used The TIA Portal software and for the visualization is used, a new generation software known as Factory I/O.*

KEYWORDS: *Factory I/O, PLC, TIA Portal.*

3D ВИЗУАЛИЗАЦИЯ НА ПРОГРАМИ ЗА ПРОГРАМИРУЕМИ ЛОГИЧЕСКИ КОНТРОЛЕРИ ЧРЕЗ СОФТУЕРНИ ПРИСТАВКИ

ДАНИЕЛ Р. ДЕНЕВ, ВИКТОР В. ЛИЛОВ, МИХАЕЛА А. КАРАДОЧЕВА

АБСТРАКТ: *Предметът на изследването ни показва начина за създаване на програма за програмируеми логически контролери и нейното визуализиране в 3D. За създаването на програмата се използва софтуера на TIA Portal, а за визуализацията софтуерна програма от ново поколение по известна като Factory I/O.*

1. Въведение

С развитието на индустрията, създаването на производствените агрегати става основен приоритет пред всяко предприятие. Въз основа на това в настоящия доклад се залага визуализация на резервоар за течности с отточващ и зареждащ механизъм.

Избора на разработка се обосновава с факта,че много предприятия започват да разчитат на химични препарати и течности. Аналогично с тяхното използване излизат на преден план въпросите: „Къде би било тяхното съхранение?” и „Как би било по-безопасно тяхното отточване и зареждане?”. Основната цел чрез визуализация е бъдещо подпомагане на фирмите (предприятия) с готово проектирано устройство за съхранение с механизъм за по безопасно ползване.Осъществяването на разработката ще стане с помощта на контролер от класа S7-1200 на Siemens, включително и на основната част от софтуера за програмиране на TIA. По отношение на визуализацията му се разполага с широк набор от програми за симулация.Основната за тази дейност е PLCSIM, която в настоящия доклад ще бъде оставена на заден план за сметка по иновативната FACTORY I/O.

2. Factory I/O

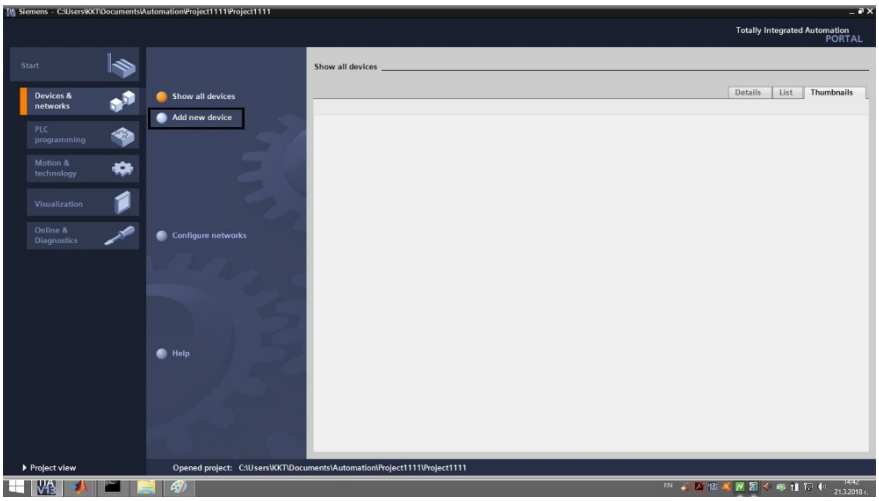
Factory I/O е 3D симулационна програма за тестване на програми проектирани на STEP7. Работи с голям клас от контролерите на Siemens.

Разполага с широка библиотека с палитри от индустриални части! Позволява на своите креативни потребители да създават не само едно 3D устройство, а цяло множество. След закупуването и лицензирането на пакета всеки потребител получава и няколко сцени, подходящи за навлизащите в програмата.

3. Създаване на програмата в TIA Portal

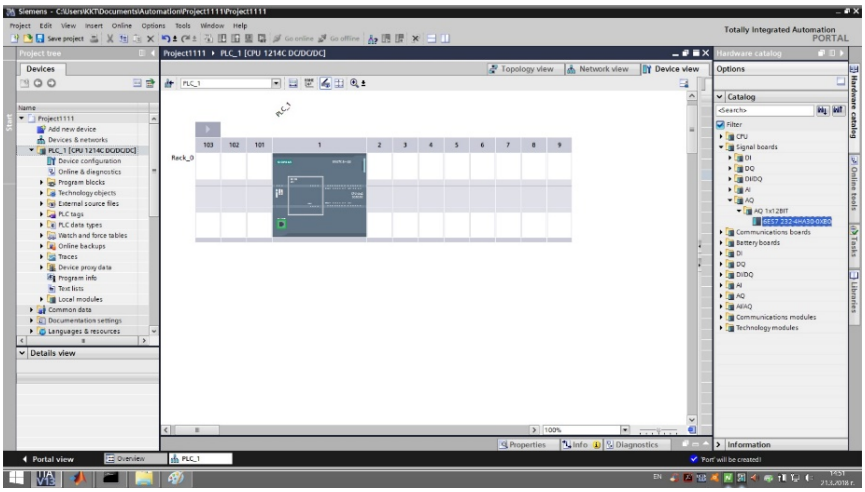
За начало на конструкцията на програмата се започва с стартирането на програмата TIA Portal v13.

От панела със задачите се избира Create new project за създаване на нов проект. Избира се име на проекта, директория къде да бъде записан и се натиска бутона Create. Проекта към този момент се създава и започват стъпките за неговата конфигурация чрез бутона Configure Device. Отваря се променен диалогов прозорец от който се избира Add new device, чрез която команда се добавя ново устройство. Това действие е показано на Фиг. 1.



Фиг. 1. Добавяне на ново устройство

За избора на устройство се разполага с широк каталог с процесори. В настоящия момент се избира Unspecified CPU 1200 във версия 4.1. Процесора се появява в работно пространство във вид на празна кутия. Същевременно така се появява и бутон Detect, който след щракване с мишката се използва за откриване на процесора. Поява се нов прозорец от който чрез функцията Start Search се открива по мрежата нужния контролер. Селектира се и се натиска бутона Detect. Програмата се свързва с контролера и извлича информация за него и неговите блокове. След осъществената връзка контролера се появява в работното поле във вида показан на Фиг. 2.



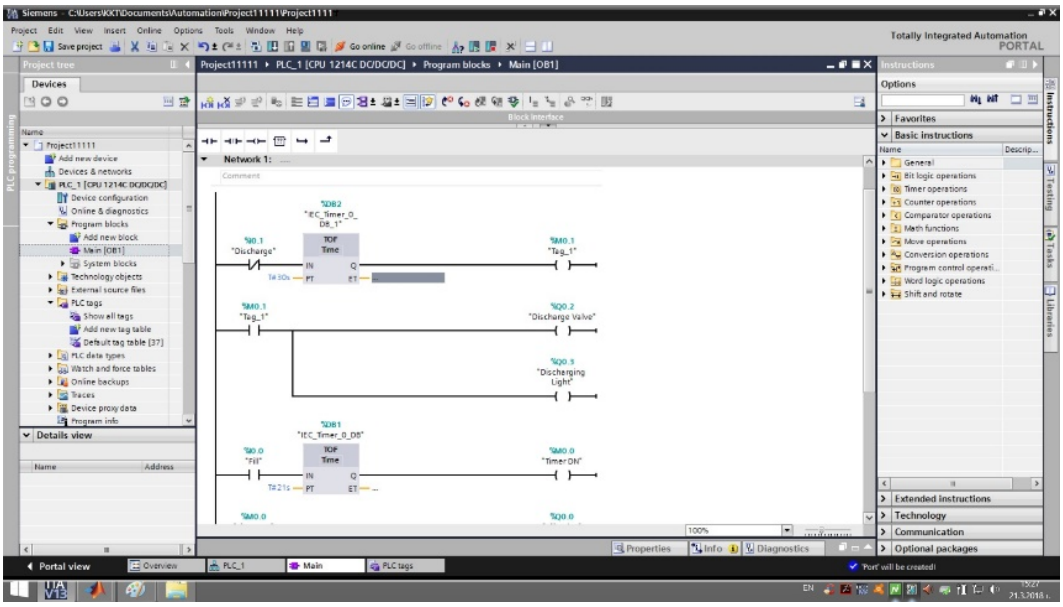
Фиг. 2. Процесор след извлечената информация

След като контролера е подготвен идва реда за построяване на електрическата и управляваща схема.Това става от навигатор на проекта. От него се избира процесора на контролера и от неговото падащо меню в подраздела Program blocks се селектира Main (OBI). По разбиране построяването на схемата се прави в Network 1. В зависимост от сложността на всяка схема може да се използва повече от един Network. Програмния език който се използва е стандартния по подразбиране от програмата LAD. За да поставя елемент в работното поле се селектира лентата и се щраква върху избрания елемент от категорията FAVORITE. В определен момент при изграждането се налага да се направи паралелно свързване на елемент. За тази цел използвам бутона Parallel. По специфичен елемент е изграждането на таймера, за него се използва функцията Create box. Тя се поставя върху схемата и за да я превърне в таймер е необходимо с десен бутон на мишката върху нея да се отворят нейните параметри. При тяхното отваряне се получава пълен достъп до елемента и неговото преобразуване. Избира се нужния таймер TOF и той се поставя на мястото на Create box автоматично.

Схемата е достъпна за изграждане и е съставена от две части. Първата част отговаря за отточващия механизъм. Съставена е от Normal close contact който играе ролята на бутон, таймер да отчита времето за отточване, assignment contact – играеш ролята на изход и Normal open contact който служи за управление на клапана за отточване на течността, както и за сигналната индикация на бутона. Втората част за зареждане е изградена аналогично.

След изграждането на схемата идва и момента за задаване на стойности и корекцията на таговете. Корекцията на таговете е важен елемент спомагащ ни за по-удобно свързване на схемата и по-добра визуализация на схемата. Тяхната корекция става от навигатор на проекта.От него се избира опцията PlC Tags, която отваря функцията Show all tags. От нея освен, че могат да се коригират наименованията на таговете, могат и да се променят всички стойности, ако е необходимо.

Всички входни данни се задават с стойност %I и дадена цифрова стойност, докато изходните се задават с %Q и цифрова стойност. След извършените действия схемата придобива вида показан на Фиг. 3.



Фиг. 3. Крайна схема

Достига се до момента за проверка на конструкцията и зададените стойности. Това става с помощта на функцията Compile.

За да се стигне до нея се влиза в навигатора на проекта, от него се щрака с десен бутон на мишката върху процесора на контролера (PLC_1) и се появяват опции, една от тях е Compile. Когато се маркира Compile се появяват много възможности, но са необходими Hardware (rebuild all) и след това Software(rebuild all blocks).Чрез първата опция се прави хардуерната проверка на контролера дали е идентично с хардуерното устройство на стема, а чрез втората се проверява софтуерната конструкция на схемата с нейните стойности, които са въведени. След компилиране и проверката покаже, че конструкцията е вярно направена, се пристъпва към операцията Download to device. Чрез нея вече готовата програма, която е конструирана, може да бъде качена на хардуерното устройството на стема показано на Фиг. 4.

Фиг. 4. Хардуерния стем с контролера

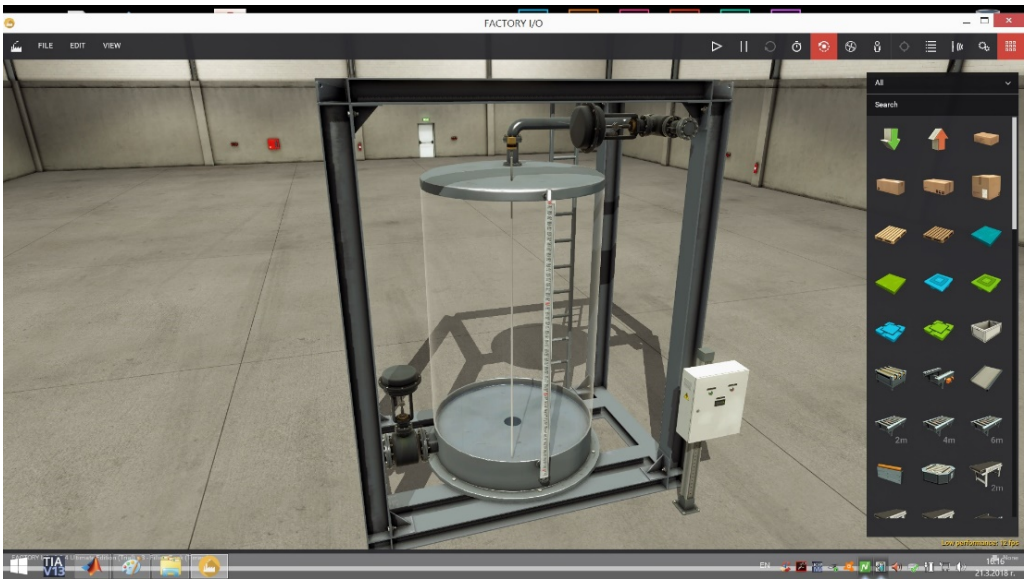
4. Визуализация

Преминавайки през всички стъпки на конструкцията идва и момента за визуализацията на устройството. Стартира се програмата Factory I/O и от нейното Меню се избира опцията NewProject, за да се създаде нов проект. Новото което се забелязва на пръв поглед е средата за визуализация. Тя не е както класическата дисплей за визуализиране, контрол и мониторинг, а е 3D форма на цех(склад, помещение). Тук макета, който се съставя ще бъде визуализиран в 3D вид, за да се покаже как би изглеждал той в реални условия.

За построяването на макета се щрака върху падащото меня All, което дава широк набор от библиотеки с елементи за конструкция. Избира се библиотека Stations(станции). В тази библиотека може да се открие желаният резервоар.По подразбиране в библиотеката, резервоара е свързан с своята платформа както и с клапите за отточване и зареждане. За да бъде поставен от библиотеката на работното поле е необходимо с щракане върху него да се провлачи до желаното място. Програмата позволява да се позиционира на всяко място в работното пространство без ограничения.След поставянето на резервоара идва и реда за поставяне на друг важен елемент, а именно управляващото го табло.Отново от менюто All, което дава избор на библиотеки, се избира библиотеката Operators (оператори). За да бъде поставено от библиотеката на работното поле е

необходимо да се щракне върху него и да се провлачи до желаното място, в близост до резервоара.

Следващата стъпка е визуализацията на бутоните върху таблото. Те отново се намират в библиотека Operators. Има нужда от два управляващи бутона, те ще са зелен за зареждане и червен за отточване.За да бъдат поставени от библиотеката на работното поле е необходимо да се щракне върху тях и да се провлачат до желаното място. Аналогично ще се сложат в максимална близост до таблото, а те чрез автоматична функция се сливат с него. След извършените действия визуализирания макет приема вида от Фиг. 5.



Фиг. 5. 3D визуализиран Резервоар

Преминавайки напред стигаме и до опроводяването. Щракайки върху падащото меню File и от там Driver се пристъпва към избора на контролера с който да свържем Factory I/O. Аналогично както в TIA така и тук се избира контролера да е от класа S7-1200. Появя се контролера в средата на екрана в вид който подлежи на опроводяване. От лявата страна са входовете, там се поставят Fill и Discharge (зареждане и отточване), както и Factory I/O (running), което служи за управлението на контролера. От дясната страна са изходите там се поставят FillLight, Fill Valve (зареждащ бутон, зареждащ клапан) както и Discharge Light, Discharge Valve(отточваща бутон, отточващ клапан).За да бъде поставена операция върху анимирания контролер е необходимо да се щракне върху желаната операция и да се провлачи до желаното място. Приключвайки с опроводяването идва и реда за задаване на IP в програмата за да може да се свърже Factory I/O с хардуерния контролер и от него да извлече предварително създадената електрическа схема.

5. Работа на резервоара

За стартиране на триизмерната среда се натиска бутона Play, който я активира. При натиска на бутона Fill (Зареждане), който се намира на таблото с зелен цвят, резервоара реагира, клапата се отваря и течността започва да го изпълва. При достигане на максималния му капацитет има датчик за сигнализиране, който казва на клапата да се затвори. Аналогично на същия принцип пристъпваме и към отточването. Натиска се бутона Discharge (Отточване), който се намира на таблото с червен цвят, резервоара реагира долната клапата се отваря и течността започва да се отточва. При достигане на

дъното има датчик, който сигнализира на клапата,че резервоара е празен и тя трябва да се затвори. Процеса на Зареждане е показан на фиг. 6, а процеса по Отточване е показан на фиг. 7.

Фиг. 6. Зареждане на Резервоара

Фиг. 7. Отточване на Резервоара

6. Заключение

Настоящия доклад е посветен на Програмируемите логически контролери. Основна цел на разработката е бъдещо подпомагане на фирмите(предприятия) с готово проектирано устройство за съхранение с механизъм за по-безопасно ползване. Реализацията на предложения от нас резервоар позволява да се съхраняват, разнообразни продукти и суровини във всички сектори на промишлеността като вода, нафта, бензин, химични препарати и други

ЛИТЕРАТУРА:

[1] Георгиева, И. Системи за автоматизация с програмируеми логически контролери, С. (2016).

[2] Лалев, Х., Цанков, Ц., Николов, И. IP управление на технологични обекти. Научна конференция с международно участие MATTEX 2010, Шумен (2010).

[3] SIMATIC S7. S7-1200 Programmable controller. System Manual (2012).

[4] Fetfov O. M. Nikolov L. G., Kulev N. Zh., Cellular Radio Channel Carrier Aggregation Motivation and Benefits Overview- „Machines, Technologies, Materials”, ISSN 1313-0226, YEAR VIII, ISSUE 5/2014.

[5] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[6] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[7] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

Имена на съавтора: Даниел Р. Денев
Месторабота: Магистър от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“
Имена на съавтора: Виктор В. Лилов
Месторабота: Студент от II-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“, специалност „Инженерна логистика“
Имена на автора: Михаела А. Карадочева
Месторабота: Студентка от III-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“, специалност „Комуникационни и информационни системи“

MATTEX 2018, Volume 2, part 1
CONFERENCE PROCEEDING, v. 2, pp. 327 - 330

SECTION Student (Information, Technical and Economical Problems of Security Systems)

ASPECTS OF THE USE OF WOMEN IN THE ACTIVITIES OF AN ISLAMIC STATE

EVGENIYA A. EVTIMOVA

ABSTRACT: *The presented report examines one of the most curious and poorly investigated aspects of the phenomenon "Islamic State"- the female participation. The material distinguishes facts from rumors and journalistic fictions; it seeks the answer to the question how this barbarian regime manages to attract women from all continents.*

KEYWORDS:. *Violence, sociality, terrorists, human misery, suicides.*

АСПЕКТИ НА ИЗПОЛЗВАНЕТО НА ЖЕНИ В ДЕЙНОСТТА НА ИСЛЯМСКА ДЪРЖАВА

ЕВГЕНИЯ А. ЕВТИМОВА

АБСТРАКТ: *От 2014г. терористичната организация "Ислямска държава в Ирак и Леванта" (ИДИЛ) стана най-дискутираната тема в международната политика. Тя привлече световното обществено мнение не само с невероятната си жестокост, но и с това, че се превърна в най-голямата заплаха за човечеството. ИДИЛ размести националните вътрешнополитически конфигурации в Сирия и Ирак и пренареди геополитическата архитектура в целия Близък изток.*

1. Въведение

От 2014г. терористичната организация "Ислямска държава в Ирак и Леванта" (ИДИЛ) стана най-дискутираната тема в международната политика. Тя привлече световното обществено мнение не само с невероятната си жестокост, но и с това, че се превърна в най-голямата заплаха за човечеството. ИДИЛ размести националните вътрешнополитически конфигурации в Сирия и Ирак и пренареди геополитическата архитектура в целия Близък изток [1], [2], [3], [4], [5], [6].

Всъщност ИДИЛ е човешко нещастие, което черпи силата си от обществено-политическия, социалния и военностратегическия хаос, в който изпадна арабския свят след т.нар. арабска пролет [1], [2], [3], [4], [5], [6].

Специална роля в армията на ИДИЛ играят представителките на нежния пол. През септември 2015 г. египетската НПО "Регионален център за стратегически изследвания" (РЦСИ) публикува интересно изследване за присъствието на жените в терористичната организация ИДИЛ. Според негови оценки в края на 2014 г. те формират около 10% от всички чужденци в терористичната организация. Това прави над 1500 души. Най-много жени от западните държави са с френски паспорт. Експертите ги оценяват на 100 и 150 души. В пропорционално съотношение те следват броя на отделните национални контингенти, напред с двете най-големи национални групи –иракската и сирийската. Поради тази причина най-голяма е общността на жените, дошли от Тунис и респективно от Саудитска Арабия. Значима е групата на представителките на слабия пол от Централна Азия, респективно от Западна Европа и САЩ. Обикновено възрастовите граници са между 18 и 21 години [1], [2], [3], [4], [5], [6].

2. Корупционни фактори, свързани с държавната администрация

Интересен факт е, че се наблюдава един процес на регионално групиране на тези жени. Особено ако те са сключили брак с боец от ИДИЛ с идентична националност. Получава се промяна на урбанизационния облик на някои селища в региона. Така например сирийският град Манбидж, на север от Халеб, е наречен от датския хуманитарен работник Ахмед Рашиди "малкия Лондон". Според последния по неговите улици може спокойно да се чуе английска реч. Според експерти в бъдеще тази нова емиграционно-цевилизационна фасада на отделните селища много трудно ще бъде променена.

По-важни са причините, които подтикват представителките на слабия пол да се присъединят към терористите. Авторите на анализа ги систематизират в пет водещи критерия, а именно [1], [2], [3], [4], [5], [6]:

1. Лични причини. Те очевидно са доминиращите при представителките на нежния пол. Особено силно важи това за сирийките и иракчанките. Обикновено те са от семейства, които са загубили някой свой член в битката срещу официалната власт. Става въпрос за съпрузи,братя, синове и други. Може да се направи аналогия с батальона на черните вдовици в ислямското движение на чеченските екстремисти. Това явление не е ново и за самия арабски свят. В ислямските бунтовнически формации, прегърнали идеологията на "Ал Кайда", в Ирак и в Египет, "отмъщението на съпругите" не е рядко явление през първите десет години на новия век.

Освен това самите жени може да са били обект на насилие, отвличане и всякакви форми на жестокост, на които сме свидетели през последните години в тези две арабски държави. Възможно е дори само домът им да е бил под обстрел. Жената е изпаднала в необичайна до този момент ситуация на изпитан ужас. Инстинктивно тя търси закрила в група, която според нея може да й донесе сигурност. Авторите на изследването твърдят, че присъединяването на жената към ИДИЛ в този случай е вид отмъщение срещу онзи, който й е причинил болка [1], [2], [3], [4], [5], [6].

2. Религиозни причини. Докладът на РЦСИ отстоява тезата, че политическата борба в Близкия изток отдавна се е превърнала в чисто религиозна. Множеството от жените не се интересуват от идеологията на ИДИЛ, а просто виждат в терористичната организация инструмент за защита на тяхната конфесионална група – сунитите. Битката срещу двата режима, иракския и сирийския, представлява за тези фанатички защита на праведната конфесия, ахл сунна уа джамаа (сунитите) срещу рауафид, шиитите. ИДИЛ се възприема като единствения инструмент за създаването на сунитска държава.

3. Идеологически причини. Част от жените възприемат призива на самообявилия се "халиф", главатар на терористите Абу Бакар ал Багдади, за преселването в "земите на исляма" като шириатско задължение. Така участието в джихада и живеенето на територията на "халифата" се превръща в част от догматиката, манипулативно стъкмена от мюфтиите на терористите [1], [2], [3], [4], [5], [6].

4. Социални причини. Те са приложими най-вече в случаите на жените, произхождащи от западните общества. Самите те са разделени на две групи. Първите са мюсюлманки по рождение, но преди всичко от трето или четвърто поколение имигранти. Въпреки притежанието на всички атрибути на интеграцията (родени на Запад, говорещи местния език без акцент, често образовани и социализирани съгласно местните цивилизационни критерии) западното общество не ги приема пълноценно. Те продължават да се чувстват отчуждени, което ги прави гневни. В ИДИЛ те си мислят, че намират онази социална среда, в която няма да има подобен тип дискриминация. Втората група е на жените, които идват от католически, еврейски или атеистично настроени семейства. Те са сключили брак с мюсюлманин и впоследствие приемат исляма. Често

съпругът изповядва ислямската религия в нейния радикален вариант, салафизма, което предопределя и ориентацията на самата жена. Съпругата следва своя мъж, когато той се присъединява към ИДИЛ в Ирак или Сирия [1], [2], [3], [4], [5], [6].

5. "Хуманитарни" причини. Редица жени, идващи от западните общества, са възпитани в ценностите на равенството, справедливостта, защитата на угнетения и правата на човека. Някои от тях възприемат сирийския народ като жертва на режима на Башар Асад. Паралелно с това ИДИЛ се възприема като истинския инструмент за отстояването на правата на жертвите. Присъединяването към терористичната организация е следствие от манипулативна интерпретация на необходимостта сирийският народ да бъде подпомогнат. Често жените участват в чисто хуманитарни дейности-разпределение на лекарства, храни, дрехи за ранени, грижат се за бедни, за нуждаещи се, за деца сираци и други, пострадали от битките в Сирия и Ирак. Те възприемат това като свое задължение, произтичащо от догматичния императив за участие в свещената война.

Жените вършат всякакъв вид работа. Те участват в битките, в тренировките за боравене с оръжие, в изучаването на основните прийоми на самоотбраната, в женските отделения на религиозната полиция, в медийната, пропагандаторска дейност (според експерти те са по-добри в привличането на младежи), вършат куриерски услуги, домакинската работа, поддържат семействата на муджахидините, възпитават децата, в това число и обучават следващото поколение муджахидини [1], [2], [3], [4], [5], [6].

Всъщност последното си остава най-важното за новите джихадистки. В книга, издадена от пропагандаторския център на ИДИЛ, се дават указания как майките трябва да отглеждат децата си с цел те да станат боеспособни муджахидини. Така например във въпросната брошура озаглавена "Ролята на сестрата в джихада", се казва, че майката трябва да възпитава детето си в такъв дух още когато бозае. Ако остави това за периода, когато детето се научи да ходи, ще е твърде късно. Джихадистката следва да обучава детето си в спорти игри, най-вече в стрелба с лък, тъй като това действие създавало способността у човека за "корекция". В снимковия инструктивен материал е дадено изображението на дете на около седем-осем години, което държи с едната си ръка отрязана глава, а други деца наоколо го гледат с възторг. Според експертите търсеният от екстремистите социално-педагогически ефект в душевността на детето е сходен, както при игра с кукли в нормалния цивилизован свят. Според наръчника за възпитание на екстремистите подобен тип игра трябва да се превърне в любима за подрастващото поколение, за да свиква на подобни гледки [1], [2], [3], [4], [5], [6].

Въпросното ръководство препоръчва обучението на децата да стане "забавление и удоволствие". В същото време пояснява, че това не означава практикуване на танци или слушане на музика. Нещо повече-на децата трябвало да се забрани да гледат телевизия, тъй като тя предизвиквала "лудост, хаос и сляпа агресивност" [1], [2], [3], [4], [5], [6].

Специален доклад на Мониторингова лаборатория на "Ал Азхар" от март 2016 г., озаглавен "ИДИЛ и създаването на ново по-опасно поколение", се отбелязва, че поради слабия приток на чуждестранни бойци терористичната организация поставя категорично акцент върху рекрутирането на жени и деца. Според експертите на авторитетния египетски богословски университет около 55% от бойците на ИДИЛ са вече жени. След последователните поражения на всички фронтове кадровиците на терористичната формация се виждат принудени да изпращат вече членовете на религиозната полиция. Не прави изключение и женското й отделение "ал кханса". Жените в ИДИЛ вече достатъчно добре са овладели бойните техники. Много скоро те ще бъдат готови да бъдат изпращани и за самоубийствени атентати. Това вече са сторили четири жени в Камерун, участващи в организация, която е част от глобалната мрежа на ИДИЛ. Според анализа жените отдавна

са приключили с етапа да бъдат съпруги на “чакания рицар” и майки на бъдещи джихадисти. Значителна част от тях боравят чудесно с оръжие и чакат голямото доверие да влязат в списъка на ал интихариин, самоубийците.

3. Заключение

ИДИЛ е световна заплаха, но тя не е еднакво опасна за различните държави. Отдалечеността от Близкия изток е сред основните фактори, която определя степента на заплахата. Ето защо освен задължителната координация на действията със съюзниците и партньорите, всяка национална държава трябва да има свой поглед върху произхода на ИДИЛ и нейната структура, да проникне в логиката на действието на организацията, да е наясно със случващото се със и във нея, да подреди известните емпирични данни, да приложи свои модели на анализ и синтез. Само по този начин определена държава може да е в състояние да формира гъвкав подход за противодействие, който освен универсалните за всички страни елементи да отчита нейните национални общностни. Например дори тя да не е източник на поток от джихадистки бойци към и от епицентъра на ИДИЛ в Сирия и Ирак, може да е коридор за терористи. Какъвто е случаят с България.

ЛИТЕРАТУРА:

[1] Чуков, Владимир. Даеш:(не) ислямска държава. Iztok-Zapad, 2016.

[2] [онлайн]. [прегледан 29.09.2018]. http://www.wikipedia.org.

[3] Чуков, В. (2014). „ИДИЛ между девиантния ислям и екстремизма “. Научни трудове на Русенския университет, 53(5.2), 9-17.

[4] Хаджиев, Б. (2018). Сходства и различия в онлайн стратегии на Ислямска държава и Ал Кайда. Ikonomiceski I Socialni Alternativi, (1).

[5] НАПОЛЕОНИ, Л. (2014). Ислямска държава и преначертаването на Близкия изток.

[6] Vasilev, V. R. Рекламните трикове на „Ислямска държава” в интернет. in хоризонти в развитието на човешките ресурси и знанието. Том 2. 12-14 ЮНИ 2015 (pp. 116-122). Бургаски свободен университет.

Име на автора: Евгения А. Евтимова
Месторабота: студентка от IV-ти курс в специалност „Системи за сигурност“, Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: evtimova_dg@abv.bg

TRAFFIC REPORTING AND THE ABILITY TO OPTIMIZE LAN

IVAN S. IVANOV, VIKTOR V. LILOV, DANIEL R. DENEV

ABSTRACT: *Viewed is the essence of what is local network, how to optimize and how to take account of traffic passing through it. They use techniques such as LAN Speed Test, Traffic LAN and capabilities of the operating systems Linux and Windows.*

KEYWORDS: *LAN, Linux, speed test, traffic LAN, Windows.*

ОТЧИТАНЕ НА ТРАФИК И СПОСОБНОСТИ ЗА ОПТИМИЗИРАНЕ НА ЛОКАЛНИ МРЕЖИ

ИВАН С. ИВАНОВ, ВИКТОР В. ЛИЛОВ, ДАНИЕЛ Р. ДЕНЕВ

АБСТРАКТ: *Разгледана е същината на това, какво е локална мрежа, как да се оптимизира и как да се отчете трафика преминаващ през нея. Използват се похвати като LAN Speed Test, Traffic LAN и способностите на операционните системи Linux и Windows.*

1. Увод

Локална (LAN) мрежа е вид малка компютърна мрежа, обслужваща компютри и други устройства (напр. мрежови принтери или скенери), свързани помежду си. За разлика от големите (международни) WAN мрежи, локалната мрежа се разполага обикновено в една сграда или една и съща стая. В днешно време все по разпространен е безжичният начин на свързване като WIFI или LI-FI, отколкото класическият метод с етернет кабел UTP или STP.

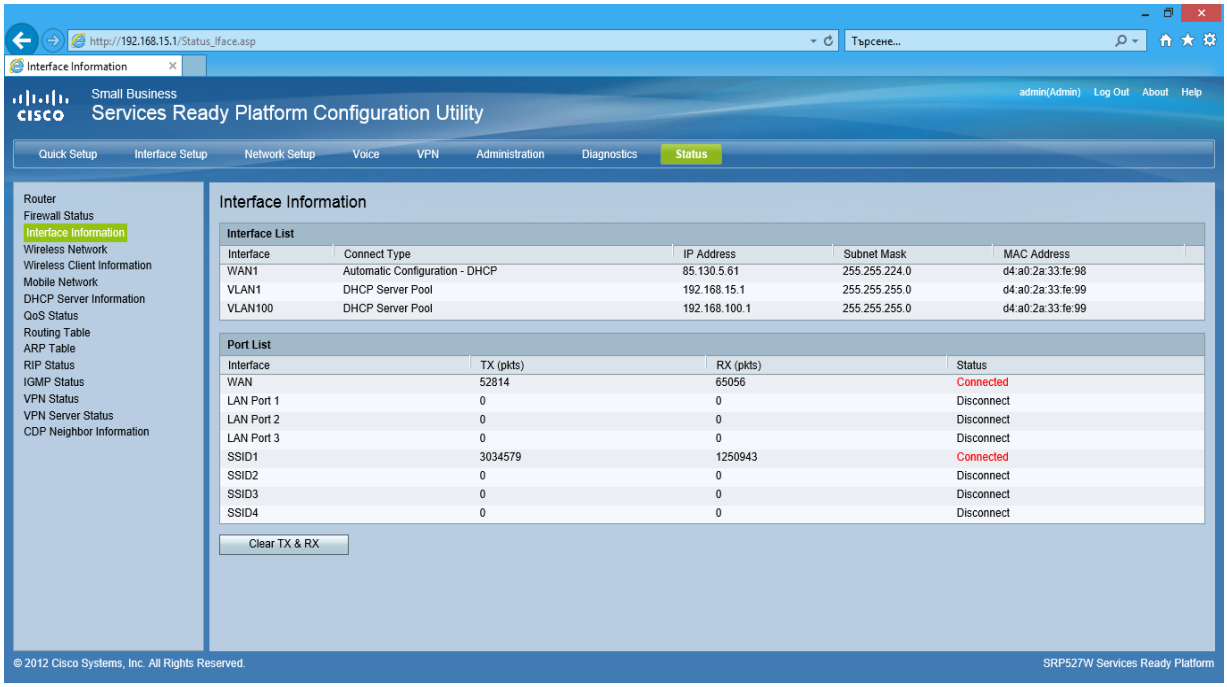
Най-често се използват равноправни локални мрежи от тип пръстен (ring) или от тип звезда (star). Като най-масов е вторият от горе споменатите поставяйки в центъра на мрежата комутатор (суич или рутер). Но по големите мрежи използват клиент-сървър топология, в чиято основа стои именно въпросния сървър, който може да бъде както нормален потребителски компютър (PC) така и специализиран такъв (Server) (рак масиви).

Основно използвани за следене на производителността на мрежата са програмите за автоматично събиране на статистика за мрежовата дейност, чрез които може да се анализира и оптимизира цялата LAN мрежа или конкретна локална машина. За по големи мрежи могат да бъдат закупени професионални такива като: PRTG - ALL-IN-ONE LAN SCANNER или Windows Performance Monitor който е част от Windows Server OS на Microsoft или аналогични инструменти вградени в Linux дистрибуции (Ubuntu server, RedHat Enterprise, SUSE Enterprise. Cent OS).

2. Изложение

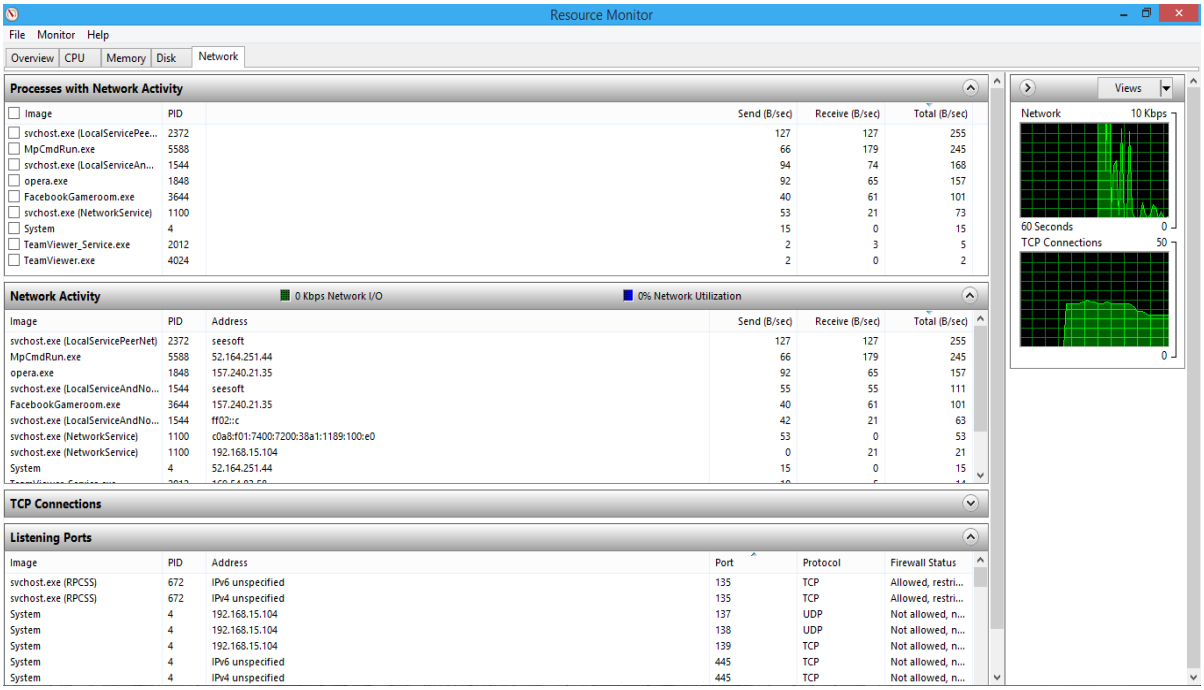
Хардуерното отчитане на трафика може да се осъществи през самите комутатори използвани за връзка. Те включват фърмуер за управление като чрез различно донастройване може да пази статистическите данни за преминаващите пакети.

Такива системи притежават комутаторите/маршрутизатори на Сиско (Cisco) (фиг. 1), TP-Link, D-Link, Asus и други.



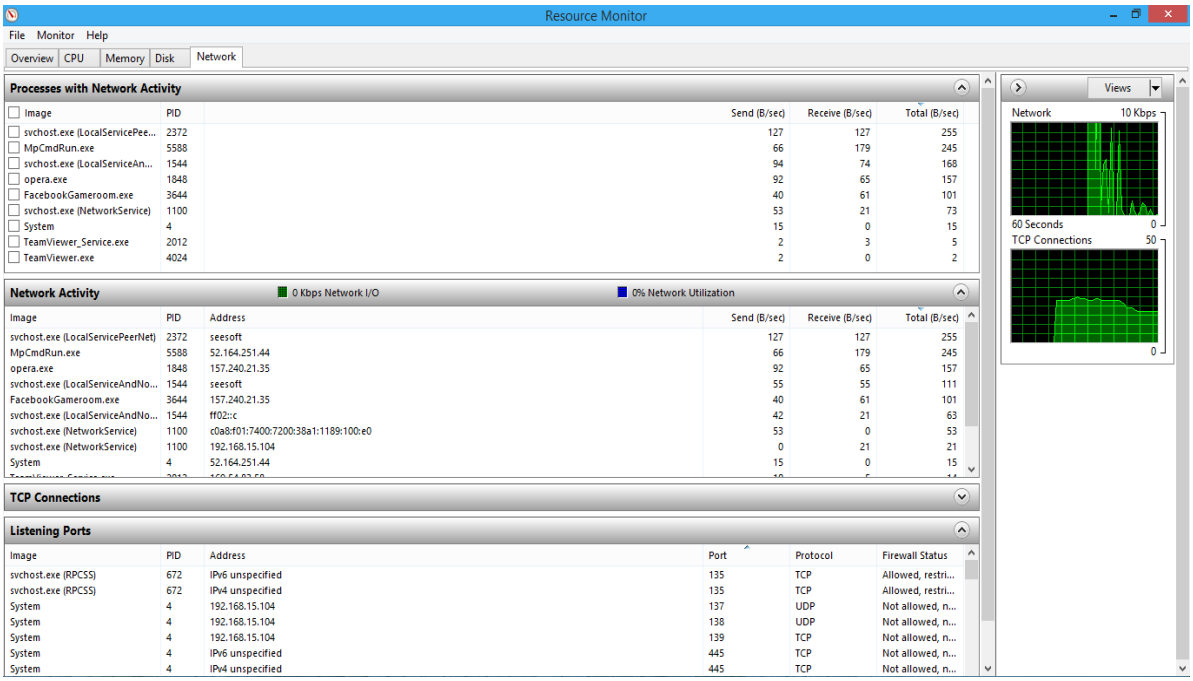
Фиг. 1.

Друг хардуерен метод е използването и преглеждането от драйверите на конкретни LAN карти инсталирани или интегрирани във възлите на мрежата (фиг 2.). За целта може да се изведат данните чрез вграденото в Windows приложение: Resource Monitor.



Фиг. 2.

При специализираното софтуерно следене на трафика под Linux дистрибуциите може да се ползват както графични програми, така и конзолни такива. Пример за графични програми са: cbm - Color Bandwidth Meter, Speedometera, а за конзолни: Iptraf, tcptrack (фиг.3).



Фиг. 3.

Оптимизирането на една локална мрежа може да се осъществи по най-разнообразни начини и методи (от физически до софтуерни). За вторите съществуват различни наръчници и ръководства за употреба, поясняващи конкретни настройки на апаратурата използвана за изграждането на възловите точки.

Нека да се спрем малко по-подробно на физическото оптимизиране.

Проблемите на бавната скорост на мрежата от механичен характер се дължат на фактори като: разстояния между клиентите, интерференция в използваните кабели или безжични сигнали от рутерите. Също така до проблеми води неподходящо оборудване за проектираната мрежа.

За да ускорим работата на мрежата е необходимо добре да си изясним каква е целта ѝ: дали да се свържат офис компютрите за общ достъп до физическите данни лежащи в паметта им или пък достъпването до мрежов принтер. Ако целта ни е бързо да съхраняваме и извличаме данни на отдалечено място най-добрият начин е използването на физически файлов сървър. Той може да бъде цял компютър без значение от класа му, но може и да бъде физическо устройство, представляващо малка кутия с няколко хардуерни диска разделени в томове и свързани в общ RAID масив и отдалечено управление, което може да се ползва от кой да е клиент свързан към наличната мрежа. За по сигурна връзка е препоръчително да се закачи към общата мрежа чрез UTP или STP кабел от категория 5 нагоре тоест 100 мегабита и нагоре.

Друг начин за оптимизиране е използването на различни физически сървъри за различните задачи и услуги. Това от своя страна води до разтоварване на специализираните машини и възможното по-голямо ресурсно отделяне за зададена услуга. При повреда в сървърът не се налага другите услуги да бъдат спирани.

Важна част на мрежата са начинът на свързване с клиентските LAN карти. Ако те са едва 10 или 100 мегабитови е препоръчително да се подменят с по-бързи такива, като гигабитовите от 1 гигабит до 10 гигабита са най-популярни.

Недостатък на кръговият тип мрежа, е че ако някоя от връзките откаже цялата мрежа пропада. Затова трябва добре да се подбере необходимата топология или да се промени вече съществуваща такава с цел стабилност и ускорение.

При по-големи мрежи кабелите, използвани от тип UTP/STP могат да се подменят от оптични такива (fiber-optic), чиято скорост е в пъти по висока както и дължината, при която могат да се използват. UTP кабелите са надеждни при дължина до 100 метра, след която трябва да се сложи или клиент, или устройство за ускорение трансивър и различни медия конвертори.

За подобряване на сигнала в безжична среда е хубаво да се знае плътността на стените, за да се прецени пенетрацията му. 2,4 *Ghz*-овия е по-ниско скоростен до 300 мегабита, но за сметка на това честотния му спектър позволява да се излъчва на по-голямо разстояние и през повече препятствия. Подходящ е за базов достъп като търсене на информация в бази данни и офис работа и свързаност с принтер. 5 *Ghz*-овото излъчване е с по-висока скорост на приемане и изпращане на пакети, но сигналът доста лесно се блокира от препятствия на пътя. Препоръчително е използването на повторители (Range Extenders) и точки за достъп (Access point). Чрез тях осезаемо може да се увеличи силата на разпространявания сигнал. Добре е да се провери каналът, на който се излъчва сигнала, за да се избегне сблъсък с други излъчени сигнали със същата честота. Избягването на интерференция чрез ръчното задаване на канал може да стане от самия рутер. Препоръчвани канали са 1, 6 и 11 за 2,4 *Ghz*. Съответно за 5 *Ghz*: 40, 80 и 160 *Mhz* канали. Този честотен диапазон се използва за гигабитови скорости. Подходящ е за онлайн игри, гледане на филми, стрийминг и високоскоростен файлов пренос.

Параметрите на самите физически сървъри също са от значение за скоростта на една мрежа. Колкото се може по мощни и бързи са, толкова по-лесно се достъпва до данните, които обработват. Да не забравяме, че един компютър е толкова бърз колкото е бърз най-бавния му компонент.

За да подобрим принтер сървърът се използват опашки. Това ни позволява да вършим всякаква друга работа докато чакаме разпечатването на нужните ни документи.

До подобряване на свързването и намаляване на загубите на пакети спомага използването на екранирани кабели. Това не позволява интерференция от външни източници като електромагнитни полета или натрупването на повече кабели на едно място.

3. Заключение

Можем да се обобщи, че съществуват най-разнообразни методи за следене на трафика (софтуерен и хардуерен). Двата са еднакво надеждни и точни. Изборът кой от двата да се приложи е до лични предпочитания и умения. А за една по-стабилна и бърза LAN мрежа при проектирането ѝ трябва да се изяснят целите, за които ще се използва, наличните средства отпуснати за целта. Трябва да се разгледа подробно архитектурното разположение на стените, през които ще се осъществява мрежата, да се определи каква ще бъде тя безжична или кабелна. Какви ще са устройствата, които ще са част от мрежата? Компютри, мобилни устройства, сървъри, принтери, телевизори, медийни конзоли и други. Да се избере подходяща топология за мрежата. Да се закупят надеждни кабели, комутатори, рутери и репийтъри. При вече налична мрежа е необходимо да се прегледа какво да се подмени, за да се оптимизира хардуерно или да се настрои ръчно софтуера за управление, постигайки по-високи скорости за пренос на данни и минимизиране на риска от интерференция.

ЛИТЕРАТУРА:

[1] Немет, Е. и др. Linux. Наръчник на администратора. СофтПрес, С. (2007).

[2] Цанков, Ц. Администриране на мрежи. Център за дистанционно обучение на Шуменски университет „Епископ Константин Преславски“ (2013).

[3] Цонев, И., С. Станев. Компютърни мрежи и комуникации, Университетско издателство „Епископ Константин Преславски“, Шумен (2008).

[4] Fetfov O. M. Nikolov L. G., Kulev N. Zh., Cellular Radio Channel Carrier Aggregation Motivation and Benefits Overview- „Machines, Technologies, Materials”, ISSN 1313-0226, YEAR VIII, ISSUE 5/2014.

[5] О. Фетфов, „Защита на информацията в груповите радиомрежи TETRA“, Годишник на Факултета по технически науки, Шуменски университет „Еп. К. Преславски“, 2015г.

[6] Zhelev, St., Comparative analysis of the probability in digital wireless communication systems. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 2, 2012, pp. 21-27.

[7] Желев, Ст., Приложение на рекурсивните систематични конволюционни кодове в ТУРБО кодери. Сборник научни трудове от национална конференция с международно участие “40 години Шуменски университет 1971 - 2011”, Шумен, Университетско издателство „Епископ Константин Преславски”, ISBN: 978-954-577-620-5, 2011, с. 122-128.

Имена на автора: Иван С. Иванов
Месторабота: Студент от III-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“, специалност „Комуникационни и информационни системи“
Имена на съавтора: Виктор В. Лилов
Месторабота: Студент от II-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“, специалност „Инженерна логистика“
Имена на съавтора: Даниел Р. Денев
Месторабота: Магистър от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Комуникационна и компютърна техника“

THE MANIFESTATION OF RELIGIOUS TERRORISM

MERAL. M. GALIB, HRISTINA I. KOSEVA

ABSTRACT: *Events in recent years have shown that terrorism is one of the greatest threats and challenges to humanity and the war against terrorism is a new kind of war. War waged by a new type of players with different methods and means of warfare. A war, in which civilians are involved and actually participate. Violence, threat of violence and the ability to carry out violence equals terrorism.*

KEYWORDS: *Religious terrorism, al-Qaeda, Shiites, sunnis.*

ПРОЯВЛЕНИЕ НА РЕЛИГИОЗНИЯ ТЕРОРИЗЪМ

МЕРАЛ М. ГАЛИБ, ХРИСТИНА Й. КОСЕВА

АБСТРАКТ: *През последните години събитията показват, че една от най-големите заплахи и едно от най-сериозните предизвикателства за човечеството е тероризмът, а борбата с него е нов вид война, която се води от нов вид участници с различни методи и средства за воюване. Това е борба, в която е въвлечено и участва цивилното население. Насилието, заплахата от него и способността за извършване на насилие, е равно на тероризъм.*

1. Въведение

През последните години събитията показват, че една от най-големите заплахи и едно от най-сериозните предизвикателства за човечеството е тероризмът, а борбата с него е нов вид война, която се води от нов вид участници с различни методи и средства за воюване. Това е борба, в която е въвлечено и участва цивилното население. Насилието, заплахата от него и способността за извършване на насилие, е равно на тероризъм.

Проблемите на съвременния тероризъм са резултат и на обвързаността му с религиозния фактор, присъствието на който намира израз в обособяването на различни наименования на тероризма като: „религиозен тероризъм“, „терор в името на Бога“ и т.н.. През последните години значителна част от тероризма се свързва с исляма, тъй като през последните години ролята на религията нараства и заема важно място в живота на човека. Ако се направи съпоставка ще се видят особеностите в следването на религиозните правила. От друга страна е налице стремежът на хората да обвързват идентичността си с религията. В условията на миграционни процеси, когато идентичността и принадлежността на дадена нация е поставен под въпрос, религията е факторът, който обвързва хората [1], [2], [3], [4], [5], [6], [7].

Поради възможността религията да се обвърже с важни аспекти на социалния живот понякога тя се използва за оправдание на насилие, на тероризъм. Отделни случаи, характеризиращи тази страна от взаимоотношението между религията и обществото, се наблюдават още в древността. През I век пр.н.е. редица действия на насилие извършва еврейската политическа групировка зелоти /защитници, покровители/. Нейните представители използват методите на терора за борба с римските завоеватели. Сектата на сикариите /някои изследователи смятат, че това е друго тяхно наименование/ действа в Палестина през 66-73 г. от н.е. Според историка Йосиф Флавий те използват

необикновена тактика – атакуват противника през деня, особено на празници, когато в Йерусалим има тълпи от хора [1], [2], [3], [4], [5], [6], [7].

2. Изложение

По-известна на Запад е сектата на асасините. Тя действа през периода X-XIII век на територията на днешния Иран и Сирия. Названието й е свързано с употребата на хашиш. За това свидетелстват легенди и разкази на съвременници. Привържениците се наричат „хашашини”. Но е малко вероятно при изпълнение на сложните задачи, които са им възлагани, членовете на сектата да са били в състояние на опиянение. По-скоро прозвището „хашашини” е израз на отрицателното отношение на други членове на обществото към сектата [1], [2], [3], [4], [5], [6], [7].

Най-известният им водач е имамът Хасан ибн Сабах. Привържениците на сектата са му предани и са готови да дадат живота си при изпълнение на задачата, която той им е възложил. Действията на избраниците са свързани с убийства на политически противници на водача. Убит е Конрад Монфератски, управител на Йерусалимското кралство, два пъти членове на сектата се опитват да убият египетския султан Саладин. Хасан ибн Сабах разбира, че разполага с малко хора, за да се сражава открито, но и че продължителните, добре обмислени компоненти на терора, осъществени от добре обучени и дисциплинирани воини, могат да донесат сериозен политически ефект. Асасините действат под прикритието на най-строга секретност, преобличайки се често като чужденци, в това число и християни. Те не ползват нито отрова, нито снаряди. Тяхното оръжие е кинжалът – не само поради неговата висока надеждност, но и защото в убийството виждат нещо ритуално. Сектантите приемат мъченичеството и смъртта в името на идеята и твърдо вярват в настъпването на нов ред. В историческа перспектива дейността на сектата представлява отчаяна, макар и обречена на крайно поражение, борба на религиозно малцинство за право на свой начин на живот и на свое вероизповедание. Известно време тактиката им носи успех. Но по-късно главната им крепост Аламут е превзета от монголците [1], [2], [3], [4], [5], [6], [7].

През Средновековието в името на религията се водят войни, хиляди хора са подложени на преследвания, действа инквизицията. Понякога религиозните норми стават държавни и това увеличава възможностите за извършване на различни форми на насилие.

Важна идейна предпоставка за насилие на религиозна основа е фундаментализмът. В стремежа си да се запази, да се утвърди всяка религия може да достигне до призиви за връщане към корените. Не е задължително това да доведе до екстремистки прояви, но съществуват някои предпоставки за подобно развитие. Понятието „фундаментализъм” се появява в християнската традиция – протестантството - в САЩ. Смята се, че това понятие не може да се използва в други религии. Но през последните години намира широко приложение, открива се и в други сфери на обществения живот.

Най-силно е влиянието на ислямския фундаментализъм. Той може да бъде открит в редица организации. Една от тях е „Мюсюлманско братство”, създадена през 1928 г. в Египет от ислямския духовник Хасан ал Бана. Мотото на организацията е: „Аллах е нашият идеал, Коранът е нашата конституция, Пророкът е нашият лидер, джихадът е нашият път и смъртта в името на Аллах е нашето вдъхновение” [1], [2], [3], [4], [5], [6], [7].

Мюсюлманите се разделят на сунити и шиити след смъртта на пророка Мохамед през 632 година. Той не посочва свой наследник, който да води мюсюлманската общност. Последват спорове за това кой да застане начело на младата и бързо разрастваща се религия. Някои смятат, че с консенсус трябва да изберат нов водач. Други вярват, че само наследници на пророка могат да бъдат халифи.

Така властта преминава в ръцете на Абу Бакр – близък сподвижник на пророка. Някои обаче смятат, че начело трябва да застане братовчедът на пророка и негов зет Али. Той все пак става халиф, след като двамата наследници на Абу Бакр са убити. По-късно обаче Али също е посечен в Куфа, на територията на днешен Ирак. Синовете на Али - Хасан и Хюсеин претендират, че те трябва да наследят титлата, но Хюсеин и голям брой негови роднини са избити в Кербала през 680 година. Отново от привърженици на другия лагер [1], [2], [3], [4], [5], [6], [7].

Мъченичеството на Хюсеин се превръща в централно събитие за тези, които вярват в правото на Али да наследи пророка. Така последователите им започват да се наричат шиити (от Шиат Али – последователи на Али). Сунитите от своя страна приемат първите трима халифи преди Али за легитимни и правоверни, т.е. следват традицията на пророка. Сунитските владетели предприемат завоевания, които разширяват халифата до Северна Африка и Европа. Последният халифат изчезва с разпадането на Османската империя след Първата световна война [1], [2], [3], [4], [5], [6], [7].

Сунитската и шиитската секти в исляма имат свои доктрини, вярвания и развити духовни школи. И при сунити, и при шиити има както светски настроени, така и фундаменталисти. Шиитите приемат Али и следващите водачи за имами. Те вярват в 12-те имама, последният от които е изчезнал през девети век в Ирак. Някои от шиитите очакват неговото завръщане като Махди, т.е. месия. Шиитите също така имат духовна йерархия.

Сунитите обаче приемат себе си за ортодоксалния и традиционен клон на исляма. Названието им идва от „суна“ - традиция. Те славят всички пророци, споменати в Корана, особено Мохамед. Всички следващи мюсюлмански водачи обаче не са признати от сунитите [1], [2], [3], [4], [5], [6], [7].

Сунитите признават властта на Бога и в материалния свят, което при някои включва дори и обществената и политическата сфера. Шиитите пък ценят мъченичеството и саможертвата.

Над 85% от всичките милиард и половина мюсюлмани по света са сунити. Те живеят в Арабския свят, както и в Турция, Пакистан, Индия, Бангладеш, Малайзия и Индонезия. Шиитите са мнозинство само в Иран, Ирак, Бахрейн и Азербайджан. Саудитското кралско семейство, което следва строгата и консервативна сунитска школа Уахабизъм, контролира светите места за сунитите – Мека и Медина. Светите места за шиитите са Кербала, Куфа и Наджаф в Ирак [1], [2], [3], [4], [5], [6], [7].

Саудитска Арабия и Иран, които са доминиращите сунитска и шиитска сила в Близкия Изток, често са на противоположни позиции в регионалните конфликти. В Йемен шиитските бунтовници от север Хути свалиха доминираното от сунити правителство. Това доведе до военна намеса на водената от Саудитска Арабия коалиция. В Сирия мнозинството са сунити, но шиитската секта алауити на президента Башар Асад доминира правителството. А в Ирак разногласията между воденото от шиити правителство и сунитските общности подпомогнаха настъплението на т.нар. „Ислямска държава“ [1], [2], [3], [4], [5], [6], [7].

Хасан ал Бана определя дейността на „Мюсюлмански братя” като „призив към традицията”, „път за следване на суната”. В идеен план изпитва влиянието на Мохамед Ибн Абд ал Вахаб, създател на едно от крайните направления в сунитския ислям – уахабизма. Също така въздействие оказва концепцията за „ислямския призив” на Ибн Таймия и принципите на религиозно-правната школа на Ахмед бен Ханбал. Значение имат и други идейни течения. Появата на това първо в арабския свят фундаменталистко движение от съвременен тип е обусловена от негативната реакция на египетското общество по отношение на внесените западни модели. Организацията разглежда

капитализма, комунизма „арабския социализъм” като връщане към „джахилията” /доислямското невежество/. Исторически първообраз на идеалното ислямско общество може да стане събирането на единомишленици от периода на пророка Мохамед и следващите четири „праведни халифи” /Абу Бакр, Омар бен Хатаб, Осман бен Афан и Али бен Аби Талиб – бел. авт./. [1], [2], [3], [4], [5], [6], [7]

Хасан ал Бана издига идеите на панислямизма. Обосновава необходимостта от съюз на ислямските държави под знамето на единна религия. Предлага създаването на халифат. Смята, че държавната власт трябва да се регулира от висш държавен орган, който би давал експертно заключение относно съответствието на провежданите от правителството мероприятия на нормите на исляма. Като такъв орган разглежда своята организация.

През 50-60-те год. на XX век главен идеолог на организацията е Саид Кутб. Той е „водещ мислител на движението – първият теоретик на каузата на ислямистите в арабския свят”. Посещава САЩ, за да изучава педагогика. Има отрицателно отношение към западния начин на живот. „Либералното общество ограничава владенията на Бог само на небето... и отрича или премахва суверенитета на Бог на земята”. Според Кутб управляващите кръгове в Египет игнорират принадлежността към мюсюлманския свят и това води до национална криза. Критикува управлението на Насър. Смята, че режимът му е „неверен”, че осъществяваните действия не са в съответствие със закона, спуснат от Бога. Движението се ориентира към вземане на политическата власт. По-нататъшно влияние на радикалните ислямистки организации, в т.ч. и на „Мюсюлманско братство”, се наблюдава при управлението на А. Садат. През 60-70-те години на XX век на основата на ислямския фундаментализъм възниква политическият ислям /ислямизмът/[1]. Трудно е да се разкрие същността на ислямизма. Сред изследователите не съществува единно мнение по въпроса. Според С. Евстатиев към ислямизма се отнасят всички движения и доктрини, които се стремят да приведат политиката в съответствие с предписанията на шариата[2]. Прави обаче впечатление, че в ислямизма по сложен начин се комбинират идеи, обвързани с традицията, и със съвременността. Но не може да се твърди, че фундаментализмът или ислямизмът автоматично предполагат тероризъм, че задължително пораждат тероризъм. Те са известни идейни предпоставки. Техни доктрини се подлагат на крайни, радикални интерпретации и така стават част от идеологията на терористични организации [1], [2], [3], [4], [5], [6], [7].

През 80-те години на XX век възниква „Ал Кайда”. Тя е организацията, която в края на XX и началото на XXI век в най-голяма степен се свързва с тероризма. Но се създават и други организации. Нейният лидер Осама бен Ладен, убит от американски командоси в Пакистан през 2011 г., оказва личностно въздействие върху своите привърженици и последователи. Той е от Саудитска Арабия и важна част от неговия живот е участието му във войната в Афганистан. Приет е от талибаните и живее там дълго време. Именно в тази страна през периода 1996-2001 г. „Ал Кайда” реализира своите утопични държавно-управленски модели и разгръща структурата си. Според организацията идеалната държава е сунитският халифат. Желаната цел е изграждане на ислямска държава, каквато е съществувала по времето на праведните халифи [1], [2], [3], [4], [5], [6], [7].

Спорен е въпросът за религиозната доктрина, която изповядва лидерът на „Ал Кайда”. Но е сигурно, че той е последовател на идеите на С. Кутб, възприемайки неговия яростен антиамериканизъм. Бен Ладен се опитва да превърне в първостепенно задължение на мюсюлманите „изтласкването на американците от Свещената земя”. Използва цитати от Ибн Таймия, който твърди, че когато мюсюлманите са поставени пред голяма опасност,

[1] Возженикав, А. В./ред./, Международный терроризм, М., 2005, с. 201 и сл.
[2] Евстатиев, С. Религия и политика в арабския свят, С., 2012, с. 267

трябва да преодолеят различията си. В свое послание от 1996 г. Бен Ладен загатва за вида терористична акция, която има намерение да осъществи на 11 септември 2001 г. Поставя акцент върху създаването на условия за атака на авангардни и много чувствителни точки на САЩ[3]. След убийството му организацията под ръководството на египтянина Айман ал Зауахири продължава да извършва терористични атаки [1], [2], [3], [4], [5], [6], [7].

Напоследък особено активна терористична дейност се наблюдава от страна на организацията „Ислямска държава в Ирак и Леванта" /с Леванта през Средновековието латинските народи са обозначавали крайбрежните територии в Източното Средиземноморие заедно със светите земи/. Тя е създадена през 2012 г. От 2014 г. носи названието „Ислямска държава". Възникването на тази организация е вдъхновено от йорданския терорист Абу Мусаб ал Заркауи. Твърди се, че именно той е наставникът на сегашния ръководител на ИДИЛ Абу Бакр ал Багдади. Благодарение не само на идеологията, но и на неизчерпаемия финансов ресурс, ИДИЛ привлича нови привърженици. Към нея се присъединяват и европейски граждани. Според някои данни поне 2000 души от 30-те хиляди бойци са с европейски паспорти – от Франция, Великобритания, Германия. ЦРУ има сведения, че организацията разполага с 2 млрд. долара. Основен източник на доходи са приходите от нелегална продажба на петрол. Сериозни са постъпленията и от откупите, които ИДИЛ получава за взетите заложници. Организацията има и спонсори от различни държави в Персийския залив [1], [2], [3], [4], [5], [6], [7].

Ал Багдади и роден през 1971 г. Името му е Ибрахим и принадлежи към племето Ал-бу Бадри, което твърди, че произлиза от корейшите – племето на пророка Мохамед. Завършва Ислямския университет в Багдад, където изучава богословие и арабска литература. Формирането на Ал Багдади като терористичен предводител започва с навлизането на американските и британските войски в Ирак през 2003 г. Падането на Саддам Хюсеин го сварва в родния град Самара, където проповядва в една от сунитските джамии. Окупацията на Ирак става причина да премине в нелегалност. Присъединява се към иракския клон на „Ал Кайда". Там се среща с Ал Заркауи. По-късно през 2005 г. попада в плен и е хвърлен в най-строго охранявания сектор в американска военна база. Още тогава се е знаело, че опасен джихадист, верен на идеите си. Въпреки това е освободен и оглавява т.нар. шериатски комисии на иракската „Ал Кайда". През 2010 г. организира много терористични актове в Ирак [1], [2], [3], [4], [5], [6], [7].

Според специалисти Ал Багдади превъзхожда с качествата си на шеф-терорист както предшественика си Ал Заркауи, така и самия Бен Ладен. И амбициите му са по-големи. Те не се изчерпват само с отмъщението. Включват и исторически реванш над враговете на религията му, сред които са не само християни или шиити, но и предатели едноверци. Това проличава от неговата проповед от катедрата на мосулската джамия, където на 29 юни т.г. прокламира халифата и се обяви за наследник на Пророка. „Ислямска държава" е отрицание на целия регионален държавен ред. От публикуваната карта на халифата се вижда, че и големи части от Европа, включително Балканите, предстоят да бъдат завладени от неговите последователи. Духовни авторитети от редица арабски страни заклеймяват „Ислямска държава", обявявайки я за терористична. Но много джихадистки формации декларират подкрепа за халифата[4]. Фактически това се изисква и от самата организация. Говорителят на ИД заявява: „Уточняваме за всички мюсюлмани, че с обявяването на халифата те са задължени да положат клетва за вярност пред халиф Ибрахим и да го подкрепят. Нелегитимни стават всички емирства, групи, държави и

[3] Вж. Чуков, В. Ислямският фундаментализъм, С., 2004, с. 214-218
[4] Вестник „Преса", 23.09.2014, с.22-23

организации от момента, в който халифатът се разшири и неговите войски пристигнат на техните територии" [1], [2], [3], [4], [5], [6], [7].

В първото си послание след като групировката се преименува в „Ислямска държава", Ал Багдади отправя специално послание към учени, съдии, лекари и хора с военен и административен опит да дойдат в халифата, защото „мюсюлманите много се нуждаят от тях". „Мюсюлмани, стичайте се в своята държава. Да, това е вашата държава"[5].

Жертвите на организацията са многобройни. Убити са 1000 души в 10000 операции в Ирак през 2013 г. Извършват се заснети на видео и разпространявани в социалните мрежи екзекуции на журналисти, хуманитарни работници и други представители на западните страни. Според доклад на джихадистите те са заложили 4000 експлозива и са освободили „стотици" свои братя от затвора. Документът представя групировката като „организирана военна сила с ясна политическа стратегия – създаване на сунитски халифат".

Нигерийската ислямистка организация „Боко Харам", която поддържа връзки с „Ал Кайда, също обявява създаване на халифат. Завземането на територия свидетелства за промяна в тактиката на бързи набези и незабавно оттегляне. Организацията издига знамена над градовете, които завладява, и принуждава всички останали жители да следват нейното строго тълкуване на шериата или да бъдат убити[6].

Съществува мнение, че с ИД световният тероризъм навлиза в нов етап. Тази гледна точка изразяват и представители на организацията. С действията й започва „нова ера за международния джихад". Преди нея „Ал Кайда се е превърнала в терористичен интернационал, но като организация е слабо централизирана. „Ал Кайда по-скоро прилича на франчайз – на етикет, който различни организации в Йемен, Леванта и Северна Африка си закачаха, за да покажат вярност на идеите за борба със Запада, макар и да не бяха пряко подчинени на Осама бен Ладен [1], [2], [3], [4], [5], [6], [7]. Сега за първи път има държава на джихадистка база, която заличава старите граници в Близкия изток и е ориентирана към неконтролируема експанзия. ИД обявява всяка територия в света, в която живеят мюсюлмани, за потенциално своя и подлежаща на освобождаване. Друга разлика е, че ИД достига нови върхове в употребата на насилие срещу мюсюлмани и друговерци. Халифатът екзекутира пленени кюрди, а също така журналисти[7].

На пръв поглед изглежда, че съществува известно съперничество, конкуренция между „Ал Кайда" и „Ислямска държава". Новата организация привлича повече привърженици и намалява влиянието на предишната най-голяма терористична сила. Някои от по-младите последователи на ИД смятат Зауахири за „твърде стар и недостатъчно предприемчив". Но други признават, че сегашният лидер на „Ал Кайда" се опасява от събирането на много джихадистки бойци на едно място. Според него това би улеснило Запада в борбата срещу организацията. Бойците на Багдади обаче възразяват, че новият водач има куп скрити изненади за неприятелите си. „Той разполага с капацитет, който пази в тайна до настъпване на подходящия момент" – смятат негови привърженици. Багдади не се съобразява с някои препоръки на Зауахири и разширява операциите си в цяла Северна и Източна Сирия[8].

Въпреки различията между лидерите и организациите терористите от двете сили в крайна сметка започват да се подкрепят. Една от причините са действията на международната коалиция. Затова и две от разклоненията на „Ал Кайда" - в Северна Африка и на Арабския полуостров, отправят общ призив към джихадистите в Ирак и

[5] Вестник „Политика", 4-10.07.2014 г., с. 19
[6] Вестник „Политика", 12-18.09.2014 г., с. 14
[7] Митев, В. Новата война с тероризма, сп. „Тема", бр. 35, 2014, с. 60-61
[8] Вестник „Политика", 4-10.07.2014, с. 18-19

Сирия да се обединят срещу международната коалиция, създадена за противодействие на ИДИЛ. „Муджахидините трябва да спрат да се избиват помежду си и да се обединят срещу кампанията на Америка и нейната дяволска коалиция, която дебне всички ни" – заявяват терористите [1], [2], [3], [4], [5], [6], [7].

При тероризма, свързан с исляма, най-често на интерпретации се подлага понятието „джихад". В много случаи значението му се свежда до война с неверниците. Но това е неточно, едностранчиво представяне. В исляма става дума за „голям джихад" и за „малък джихад". „Големият джихад" е духовната борба на индивида със самия себе си. Пророкът е казал: „Големият джихад е борбата с това, което е в душите ни". „Малкият джихад" е употребата на сила за защита на семейството или общността от всякакви нападки. При това войната, съпротивата е позволена само ако съществува заплаха за живота, за вярата[9]. Изповядващите исляма не нападат първи, а само се защитават [1], [2], [3], [4], [5], [6], [7].

В ислямската традиция има мислители, които обосновават идеята за формиране на единна общност /умма/. Сред тях е Хасан ат-Тураби. Според него, „Когато мюсюлманите преодолеят своята привързаност към конкретна нация и религиозно направление, те ще осъзнаят принадлежността си към единната религия и умма, като следват примера на пророка Мухаммад в Медина за приобщаване на всички народи и верски общности, какъвто е бил в миналото „домът на исляма". Основни действащи принципи на тази умма ще бъдат свободата и шурата, способността на човечеството да разгръща своите способности в полза на процъфтяващата цивилизация"[10].

Според изследователи в момента няма мюсюлмански лидер, който да развива идеята за незабавно създаване на държавно образувание. Редица политици призовават мюсюлманите да положат усилия за интегриране в обществото, в което живеят, за да могат да влияят „отвътре". Но гледната точка на „халифатизма" /възстановяване на общата мюсюлманска държава/ се изразява от някои радикални формирования. Такава е „Партията на ислямското освобождение". Тя възниква през 1953 г. Седалището й е в Лондон. Според идеологията на организацията, ако в някоя отделна страна се избере халиф, мюсюлманите от целия свят трябва да го приемат и да му бъдат верни. Ако откажат, тогава ще бъдат смятани за врагове [1], [2], [3], [4], [5], [6], [7]. Но не всички сунити са за халифат. Много от тях са привърженици на идеята за самостоятелно управляващи се джаамати /ислямски общности/, а има и такива, които не поддържат идеята непременно да се установи ислямска държава. Отделни екстремистки лидери използват някои положения на ислямската доктрина, представят ги в едностранчив, изопачен вид и ги превръщат в основа на своите терористични организации. Също така не се интересуват и от степента на основателност на една или друга идея, от привлекателността й поне за част от обществото. По този начин може да се разбира обстоятелството, че халифатът, който ИД установява, не прави впечатление на една значителна част от населението. Говорителката на американския Държавен департамент Джен Псаки заявява: „Това не означава нищо за народите на Ирак и Сирия. ИДИЛ само се опитват да контролират населението чрез страха" [1], [2], [3], [4], [5], [6], [7].

Борбата с тероризма се води успешно с участието на международни сили. Това важи особено за необходимостта от противопоставяне на такава организация като „Ислямска държава". Със своите действия и намерения тя в крайна сметка се превръща в заплаха за целия свят. Поради това САЩ се ориентират към изграждане на коалиция, която да организира и проведе въздушни удари срещу позиции на организацията. Постигнати са известни успехи, но неизбежно се засяга и гражданско население. Полагат се и усилия и за

[9] Тодорова, Б. Иджтихад срещу джихад, С., 2008, с. 107-108

неутрализиране на ИД чрез изграждане на регионален съюз. В него засега се включват Йордания, Обединените арабски емирства [1], [2], [3], [4], [5], [6], [7], Саудитска Арабия, Бахрейн и Катар. Но трябва да се има предвид, че доскоро Саудитска Арабия финансово подкрепяше тероризма. Едва когато се постави въпросът за халифата, издигнаха се претенциите на Багдади в това се видя заплаха за кралската власт в страната и се предприе нова ориентация в политиката. Подобно е положението на Катар и на ОАЕ. Както подчертава изследователят Е. Ценков, всяка от тези страни „ще осребри участието си в свой интерес. Саудитска Арабия, Катар и ОАЕ ще се стремят да опровергаят обвиненията за причастност към каузата на джихадистите. Йордания ще оправдае репутацията си на най-близка до НАТО държава. А Бахрейн ще се легитимира като надежден съюзник срещу тероризма, след като смаза собствената си революция". Стои въпросът за начина, по който ще участва България. В същото време коалицията се разраства. Към нея се присъединяват и други западни държави, като Великобритания, Белгия, Дания. Своето включване обмисля и Австралия [1], [2], [3], [4], [5], [6], [7].

Религиозният тероризъм, независимо от това с коя конфесия е обвързан, се отличава с някои особености. Преди всичко това е неговата лексика, формулировките, които използва, за да определи целите си. Организациите, обвързани с религиозен тероризъм, водят „свещена война", борят се за „унищожаване на световното зло", за „ускоряване идването на месията", за „религиозно пречистване", за „сваляне на предателските светски режими", за „образуване на теократична държава /халифат/", за „господство на бялата раса" и т. н. Изследователката Джесика Стърн смята, че „повечето религиозни терористи преследват смесица от религиозни и материални цели, например придобиване на политическа власт с цел налагане определено интерпретиране на религиозни закони или позоваване на религиозни текстове като оправдание за придобиването на спорна територия". В същото време религиозните терористи са по-крайни в своите действия, в по-голяма степен са склонни да извършват жестокости. Основната причина за това е, че техните действия са божествено предопределени, задачите им са дадени от свръхестествена сила, която снема от тях отговорността за извършеното. „Вярват, че ги насочва по-висш авторитет. Виждат себе си като избрани, като миропомазани от Бог...По-самоуверени са и по-малко се съмняват в себе си, от повечето други" [1], [2], [3], [4], [5], [6], [7].

3. Заключение

Религиозният тероризъм е част от тероризма, негова разновидност. Съществува още от дълбока древност. Проявява се в различни форми през Средновековието, а и по-късно. В съвременните условия поради нарастващата роля на религията се разнообразяват неговите прояви. В момента с него са свързани терористичните атаки на най-опасната организация „Ислямска държава". Противопоставянето на религиозния тероризъм е сложен и продължителен процес. Изисква участие на представители от много страни [1], [2], [3], [4], [5], [6], [7].

ЛИТЕРАТУРА:

[1] Stoyanova, L. (2014). Тероризъм и религия.

[2] Стойков, С., Маринов, П., & Маринов, Р. (2015). Съвременната национална държава пред вълната на тероризма. Сборник, 249.

[3] Veshkov, S. (1977). Борбата с тероризма минава през неговото разбиране. In Европа през 21 век: Регионалната сигурност и необходимите реформи в Европейския съюз (pp. 346-353). Нов български университет.

[4] Казаков, К. (2017). Стратегията на тероризма. трансгранично сътрудничество и политики на развитие в българия и на балканите, 171.

[5] [онлайн]. [прегледан 29.09.2018]. http://clubz.bg/32704-kakvi_sa_razlikite_mejdu_suniti_i_shiiti

[6] [онлайн]. [прегледан 29.09.2018]. http://svobodazavseki.com/broi-49/455-savremenniyat-terorizam-kato-globalna-zaplaha-i-predizvikatelstvata-pred-religioznata-svoboda.html

[7] [онлайн]. [прегледан 29.09.2018]. http://worldrubric.com/%D0%BA%D0%B0%D0%BA-%D0%B8%D1%81%D0%BB%D1%8F%D0%BC%D1%81%D0%BA%D0%B0-%D0%B4%D1%8A%D1%80%D0%B6%D0%B0%D0%B2%D0%B0-%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B8-%D0%B9%D0%B5%D0%B7%D0%B8%D0%B4%D1%81%D0%BA%D0%B0/

Име на автора: Мерал М. Галиб
Месторабота: студентка от IV-ти курс в специалност „Системи за сигурност“, Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: meralmhmd@abv.bg
Име на съавтора: Христина Й. Косева
Месторабота: студентка от IV-ти курс в специалност „Системи за сигурност“, Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: hristinaii_@abv.bg

MATTEX 2018, Volume 2, part 1 SECTION Student (Information, Technical and
CONFERENCE PROCEEDING, v. 2, pp. 345 - 349 Economical Problems of Security Systems)

COMPARATIVE ANALYSIS OF MODERN TYPES OF TERRORIST ORGANIZATIONS

SIBEL H. FEVZIEVA, STILIANA G. STANCHEVA

ABSTRACT: *The terrorism is one of the most serious global problems in the modern world, which in the last few years has become a real nightmare in humanity. It is spread on all continents and equally affects people, regardless of their location*

KEYWORDS: *Corruption, public sector, security, terrorism.*

СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ВИДОВЕ ТЕРОРИСТИЧНИ ОРГАНИЗАЦИИ

СИБЕЛ Х. ФЕВЗИЕВА, СТИЛИАНА Г. СТАНЧЕВА

АБСТРАКТ: *Тероризмът е един от най сериозните глобални проблеми в съвременния свят, който в последните няколко години се превърна в истински кошмар в човечеството. Той е разпространен на всички континенти и в еднаква степен всява страх у хората независимо от местоположението им.*

1. Въведение

Тероризмът се характеризира трудно, като сложно и многопластово явление. Няма еднозначно определение за понятието „тероризъм”. Твърде много са опитите за дефиницията му у нас и по света. Определенията за тероризъм са многобройни. Някои от тях [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]:

• Системно използване на крайно насилие и заплаха от насилие за достигане на публични или политически цели. ;

• Противоправно използване или заплаха за използване на насилие против лица или обекти за достигане на политически, или социални цели. ;

• Систематично прилагане на насилие, за да се предизвика ужас и да се постигнат политически изменения.

През XX век спектърът от мотиви за използване на тероризма, като средство за политическа борба, се разширява. Ако дотогава на него се е гледало като на саможертва в името на някакви идеали, то за формиращите се крайно леви и крайно десни терористични формирования тероризъм се превръща в способ за самоутвърждаване.

Тероризмът е по същество театър, изиграван пред публика, действие предназначено да привлече вниманието на милиони, към нямаща нищо общо с тях ситуация посредством шок, пораждащ потрес и причиняващ нещо невъобразимо - без извинение или угризение [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2. Изложение

Терористична организация - организация, създадена с цел извършване на терористична дейност или признаваща възможността от използване на тероризъм в своята дейност, която осъществява актове на насилие, насочени към причиняване на смърт и телесни повреди [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

За съществуването на терористични организации и за ефективността на техните действия са необходими три условия [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]:

• средства (пари, оръжие, взривни устройства);

• възможност членовете на тези организации да придобиват военна и всякаква друга специална подготовка и знания;

• сигурни бази на територията на „приятелски държави“ (не само за подготовка, но и за осигуряване на надеждно укриване на извършили терористичен акт на територията на други държави) [2].

Цели и задачи на терористичните организации

Генералната цел на терористичните организации е преди всичко промяна на политическата система чрез създаване на смут, напрежение и страх у обществото.В зависимост от конкретните случаи, целта може да бъде създаване на теократична държава, управлявана от религиозен водач (напр. „Дал Калса“, „Дашмеш“, „Хизбула“, „Хамас“, „Ислямски джихад“ или „Аум Шинрикьо“ („Истината на Аум“), откъсване на цели региони от съществуваща страна и др. Друга цел е промяна на вътрешната или външната политика на конкретна държава. Напрежението и ужаса от проведен терористичен акт въздействат психологически както на управляващите от дадена страна, така и на страните – съседи. Поредна цел е отмъщение за историческа несправедливост. Повечето от терористичните организации, преследващи подобни цели, оправдават дейността си с етно-националистически или сепаратистки идеи. (напр. „Ирландска републиканска армия“ (ИРА), „Свобода на баската република“ (СБР) [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

Задачи на терористичните организации [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]**:**

- Създаване на недоверие в държавните институции от страна на населението на дадена държава – с извършване на множество терористични акции, чрез които да се докаже на обществото, че управляващите не са в състояние да се справят с терористичната дейност.

- Постигане на политическа, икономическа и социална нестабилност в дадена страна. Терористите се стремят да дестабилизират публичната власт и да наложат своя модел за управление в страната.

- Сплашване и/или отстраняване на определени (неудобни) лица (политици, общественици и др.), отделни части от населението или цялото население.

- Получаване на достъп до средствата за масово осведомяване за пропагандиране на идеите си сред населението.

- Набавяне на финансови средства, чрез които поддържат дейността си. Това става чрез обири или отвличания на лица с цел получаване на откуп, производство и разпространение на наркотици. Основният способ за финансиране на терористичните организации е чрез самофинансиране. По това те наподобяват организираните престъпни групировки [2].

Видове терористични организации

• Лявоориентиран тероризъм;

• Дясноориентиран тероризъм;

• Етноцентристки (сепаратистки) терористични организации;

• Конфесионално-политически терористични организации.

Според територията, която обхващат:

• Вътрешни терористични организации;
• Международни терористични организации.
Според обекта, който се засяга :
• Въздушен тероризъм;
• Воден тероризъм;
• Сухопътен тероризъм.
Според средствата, които се използват:
Тероризмът може да бъде диференциран като насилствена дейност, осъществявана чрез използването на оръжия за масово поразяване (ОМП) и на конвенционални оръжия. ОМП носят изключително висок степен на риск за цялото общество. При използването на конвенционално оръжие най-често се прибягва до взривни устройства с динамит или други вещества, или до обстрел с огнестрелно оръжие [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

Съвременен тероризъм

Съвременният тероризъм е проява на сблъсък, на конфликт между мощни икономически интереси, често прикривани с религиозна и етническа окраска. Той се разглежда като транснационално явление, което налага необходимостта от възприемането на еднообразен, унифициран подход за неговото дефиниране, като триединство [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]:

- Целта, преследвана от терористите, винаги е политическа. ;
- Средствата, използвани от терористите (насилие или заплаха с насилие), са според конкретните цели на всеки отделен терористичен акт. ;
- Обектите на терористични актове са хора, превозни средства и/или сгради, при което разрушенията са огромни, а човешките жертви – многобройни. [2]

Списък с терористични атаки на 21-ви век (някои от тях):

2001

При атентатите, извършени на 11 септември терористи от арабски произход вземат контрол над 4 самолета. 2 от тях се блъскат в кулите близнаци на Световния търговски център в Ню Йорк и напълно го разрушават, а друг се разбива в Пентагона в Арлингтън, Вирджиния. Убити са общо 2749 души [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2002

23 октомври – Чеченски терористи окупират театъра на улица „Дубровка” в Москва и вземат за заложници над 850 души. След тридневни преговори Руски специални части щурмуват сградата. Загиват 129 заложници, по-голямата част, от които се задушават от употребения ОМОН неизвестен упойващ газ [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2004

11 март – Бомбени атентати в Мадрид : Серия от 10 взрива избухват в 4 влака в Мадрид, Испания. Загиват 192 души, а близо 2050 са ранени. 30 чужденци от 13 националности са сред жертвите на атентатите в Мадрид, включително и 4ма български граждани. Отговорност за атентата приема Ал-Кайда. По-късно става ясно, че планът на терористите е бил 4те влака да се взривят в момента, в който се засекат на централната гара в Мадрид, за да може силата на взрива да унищожи сградата на гарата и да причини хиляди жертви [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

1 септември – Чеченски терористи вземат за заложници повече от 1200 деца, родители и учители в сградата на училището в град Беслан, Севрна Осетия. На 3я ден от кризата избухва престрелка между въоръжените родители на децата и терористите. Специалните сили по принуда се намесват. Чеченците взривяват покрива на училището. Загиват 334 души, от които 186 деца. Шамил Басаев поема отговорност за атентата [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2005

7 юли – Бомбени атентати в Лондон, при които при координирани взривове на атентатори-самоубийци в лондонското метро и един автобус на градския транспорт загиват 52 невинни граждани и са ранени около 700 души [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2006

18 септември – Терорист-камикадзе се взривява на многолюден пазар в град Тал Афар, северозападен Ирак, недалеч от границата със Сирия. Загиват 21 души, а повече от 20 са ранени [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2012

18 юли – Атентат на летището в Бургас срещу израелски туристи. Загиват 5 човека и около 35 са ранени [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2016

Януари – 11 германски туристи бяха убити при атентат в центъра на Истанбул, Турция. Те станаха жертва на атентатор-самоубиец от терористичната организация „ИДИЛ”. Инцидентът имаше катастрофален ефект върху туристическия сезон в Турция.

Март – Атентат потопи белгийската столица Брюксел в кръв. Загинаха 34 души, а 198 бяха ранени, след като трима терористи атакуваха летище „Завентем” и метростанцията „Малбек” [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

Юни – 2 експлозии на камикадзета на летище „Ататюрк” в Истанбул. 40 жертви и 147 ранени. Разтърсващите събития не спряха и през юли. „ИДИЛ” отново напомни за себе си, този път припознавайки атентатора в Ница. Камион, управляван от тунизиеца Мохамед Булел, прегази стотици хора на крайбрежната алея на френския туристически град. Загинаха 84 души, а над 300 бяха ранени.

Декември – Квартал „Бешикташ”, Истанбул. Атентатор се самовзривява до стадиона. Целта е автобус, пълен с полицаи. Следва 2ри взрив. Загиват 38 души и 150 са ранени [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

2017

Нова година - Истанбул. Нападател, предрешен като Дядо Коледа откри безразборна стрелба в модна дискотека на Босфора. Загиват 39 души и 69 са ранени.

Април – Санкт Петербург. Експлозия избухна в метрото. Взривът става във вагон между двете съседни метростанции „Сеная площад” и „Технологичен институт” в центъра на града. Открито е второ взривно устройство. Загиват 11 души и 47 са ранените.

Май – Манчестър. Взрив на концерта на американската певица Ариана Гранде в най-голямата покрита зала в Европа - „Манчестър арена”. Загиват 22 души и над 50 са ранените [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

3. Заключение

Борбата с тероризма трудно може да се осъществи с военни средства и бази в нарочените за рискови региони, но базите и военното присъствие могат да осигуряват

други интереси на господстващите в света държави. Всички изработени до тук конвенции за борба с тероризма са резултат от 4 десетилетия усилия и работа на международната общност. Европейската политика за борба с тероризма е утвърдила засилване сътрудничеството между полицейските и съдебните органи, като за целта се приложат всички утвърдени международни конвенции за борба с тероризма – ООН, ОИСР, НАТО и др. Да се засили сигурността и най-важната стъпка да се координират международните действия [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11].

ЛИТЕРАТУРА:

[1] Караганев, Р. (2008). Първи стъпки в кодифицирането на тероризма и международното му преследване. Исторически преглед, 64(5-6), 203-210.

[2] Чуков, В. (2014). „ИДИЛ между девиантния ислям и екстремизма “. Научни трудове на Русенския университет, 53(5.2), 9-17.

[3] Cheshmedzhieva-Stoycheva, D. (2013). Bulgaria: A new stage for international terrorism. Dynamics, Interdisciplinarity, Diversity, 16-28.

[4] Stoyanova, L. (2014). Тероризъм и религия.

[5] Doykov, N. Анализ на френската система за противодействие на тероризма. Мрежа за ранна тревога. In Европа през 21 век: Регионалната сигурност и необходимите реформи в Европейския съюз (pp. 516-522). Нов български университет.

[6] Василев, В. РЕГИОНАЛНОТО СЪТРУДНИЧЕСТВО–ФАКТОР В БОРБАТА С МОРСКИЯ ТЕРОРИЗЪМ В КРИТИЧНИТЕ ТОЧКИ ЗА КОРАБОПЛАВАНЕТО.

[7] Veshkov, S. (1977). Борбата с тероризма минава през неговото разбиране. In Европа през 21 век: Регионалната сигурност и необходимите реформи в Европейския съюз (pp. 346-353). Нов български университет.

[8] Miriyana, P. (2017). SOCIAL MEDIA AND NETWORKS-THE NEW TOOL FOR TERRORISTIC ORGANIZATIONS. Научни трудове на Съюза на учените–Пловдив. Серия А: Обществени науки, изкуство и култура, 4.

[9] Bakalov, Y. Съвременният тероризъм-негативен фактор в европейската среда за сигурност. In Европа през 21 век: Регионалната сигурност и необходимите реформи в Европейския съюз (pp. 310-318). Нов български университет.

[10] [онлайн]. [прегледан 19.09.2018]. Уикипедия, www.wikipedia.org

[11] [онлайн]. [прегледан 19.09.2018]. www.e-dnrs.org

Име на автора: Стилиана Генкова Станчева
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.

Име на съавтора: Сибел Хюсеинова Февзиева
Месторабота: Студентка от I-ви курс в Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“, специалност „Системи за сигурност“.

CORRUPTION IN THE FIELD OF PUBLIC ADMINISTRATION

VLADISLAVA A. RUSEVA, RUMYANA V. VASILEVA

ABSTRACT: *In recent years, corruption has become a global threat not only to the economic development of individual countries and their international ties but also to the global economy and politics as a whole. Even after Bulgaria's accession to the EU corruption in the sphere of state administration still remains a crime without punishment. Despite good economic growth and some success in anti-corruption reforms, the country faces two major deficits in countering corruption: political will and administrative capacity.*

KEYWORDS: *Corruption, crime, threat, state administration, consequences, society.*

КОРУПЦИЯ В СФЕРАТА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

ВЛАДИСЛАВА А. РУСЕВА, РУМЯНА В. ВАСИЛЕВА

АБСТРАКТ: *През последните години корупцията се превърна в глобална заплаха не само за икономическото развитие на отделните страни и техните международни връзки, но и за глобалната икономика и политиката като цяло. Дори и след присъединяването на България към ЕС корупцията в сферата на държавната администрация продължава да бъде престъпление без наказание. Въпреки добрия икономически растеж и известен успех в антикорупционните реформи, страната е изправена пред два големи дефицита в противодействието на корупцията: политическа воля и административен капацитет.*

1. Въведение

Понятието „корупция“ според едно от възприетите определения е злоупотребата с икономическа, политическа, административна и съдебна власт, която води до лично или групово облагодетелстване за сметка на правото и законните интереси на личността, на конкретна общност или на цялото общество.

Терминът „корупция” означава развала, поквара, подкупничество [2]. Като юридически термин „корупцията” означава антиобществено явление, характеризиращо се с морална поквара на личността или социалната група и с противозаконно използване на служебно или друго положение чрез които се получава противозаконна облага.

Трябва да се прави разграничение между държавна и публична администрация. Държавната администрация е част от публичната администрация, но не се покрива изцяло с нея. Западните автори употребяват понятието „публична администрация“ в смисъл и на държавна, и на местна администрация. Под държавна администрация в България се разбира административните структури и дейности на държавата. Държавната администрация се развива в дейността на държавните органи и се осъществява от държавни служители. В повечето случаи, когато се говори за публична администрация, се изследва и използва като основен пример държавната администрация.

Следва да се изясни значението на основните понятия, които ще бъдат обект на изследване в настоящия доклад.

Понятието „публична администрация“ може да се дефинира от две гледни точки: от гледна точка на властта и от гледна точка на гражданското общество.

Публичната администрация от гледна точка на властта се дефинира като комплекс от административни процеси, административни структури и лица, действащи в официални длъжности, подпомагащи и осигуряващи изпълнението на законите и други нормативни актове, както и действията на органите на властта.

Дефиниция на публичната администрация от гледна точка на гражданското общество е инструмент за реализация на обществения интерес, в т.ч. финансиране на обществените дейности, административното обслужване на населението, защита на териториалната цялост на държавата, вътрешен ред и сигурност, борба с престъпността, социална защита и др.

2. Изложение

През последните години Системата за мониторинг на корупцията на Центъра за изследване на демокрацията показва, че административната корупция в България не намалява. Същото се отнася и за една още по-всеобхватна форма на корупция – завладяването на държавата. Тези две прояви са тясно свързани, тъй като представляват различни аспекти на едно и също явление – корупционно поведение. Масовата административна корупция в страната е показателна не само за нарушения и злоупотреби от страна на държавните служители при взаимодействието им с бизнеса и гражданите. Ситуацията се усложнява от високите нива на политическа корупция – т.е. многобройните корупционни отношения и зависимости, в които са въвлечени висши държавни служители и политици на управленско ниво. Обикновено корупционните отношения на различните равнища на институциите в държавното управление са като цяло сходни и се обуславят от структурни за българското общество фактори [12].

През последното десетилетие по-голяма публичност придобиват особен тип комплексни корупционни сделки и зависимости, обикновено наричани завладяване на държавата. Това се отнася до практиката на много влиятелни (включително бизнес) фигури да си осигурят преференциално отношение от държавата чрез сложни корупционни сделки и други нарушения на закона. Те постигат това чрез въздействие върху функционирането и политиката на държавните институции с цел удовлетворяване на техните частни интереси за сметка на общественото благо [4].

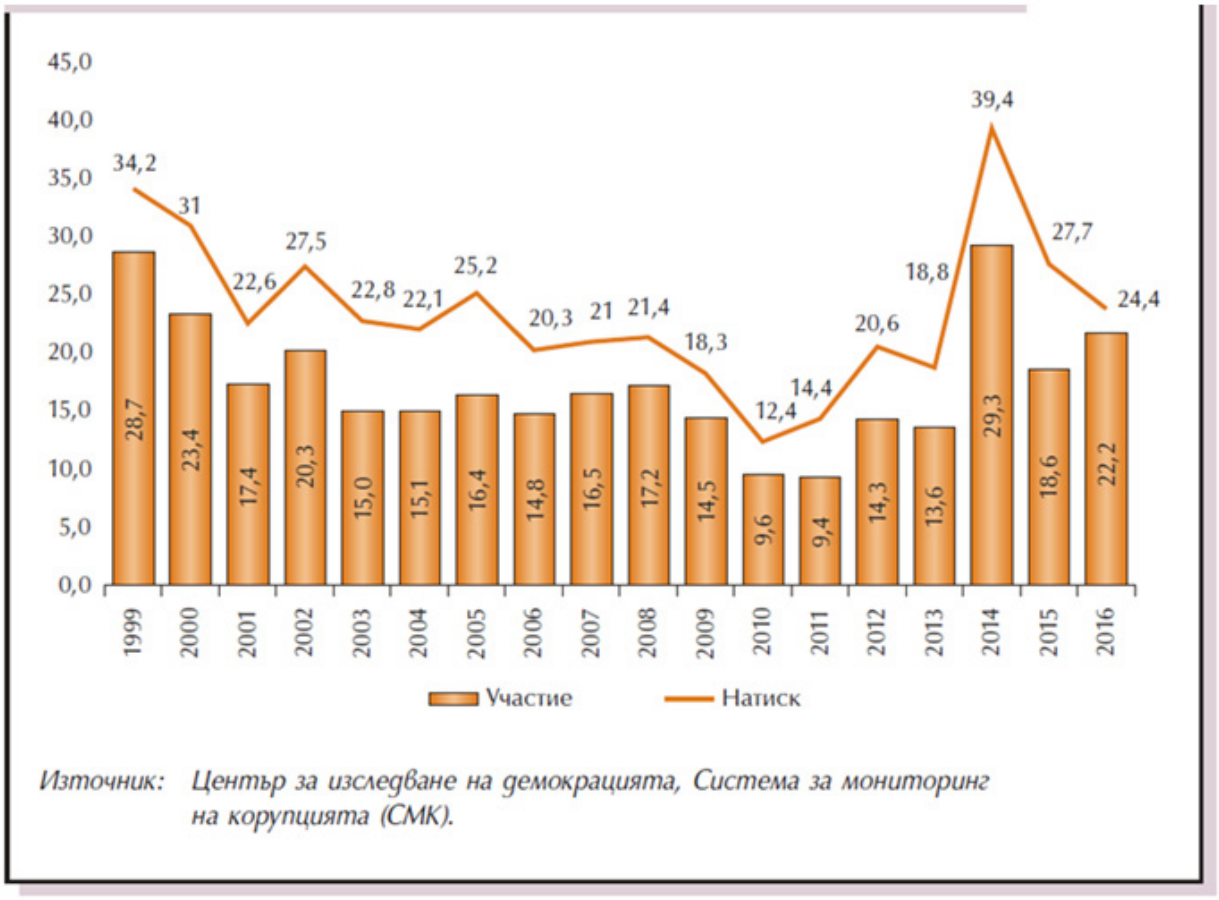
Оценката за нивото на корупцията и за развитието на антикорупционните стратегии и политики зависи до голяма степен от начина, по който се дефинират и интерпретират измеренията и формите на корупционно поведение. Общите заключения за състоянието на корупцията в страната в периода 2015 – 2016 г. не са оптимистични.

Корупция в държавната администрация

Административната корупция се увеличава постепенно след 2011 г. и в момента бележи високи нива. Като цяло, след 1999 г. (без да се отчитат незначителните колебания) могат да бъдат откроени два специфични периода, свързани с политическия цикъл:

1) 1999 – 2011 г., когато се регистрира неравномерен процес на общо намаляване на административната корупция (през 1999 г. около 29 % от населението съобщава за участие в корупционни сделки, докато през 2011 г. стойността на този индикатор спада до 9,4 %);

2) след 2011 г., когато се наблюдава процес на постепенно нарастване на административната корупция – 22,2 % за 2016 г., което съответства на участието на около 1,3 млн. граждани в корупционни сделки.



Фигура 1. Участие в корупция 1999-2016 (даване на подкупи и изпитан корупционен натиск, % от населението над 18 г.) [4]

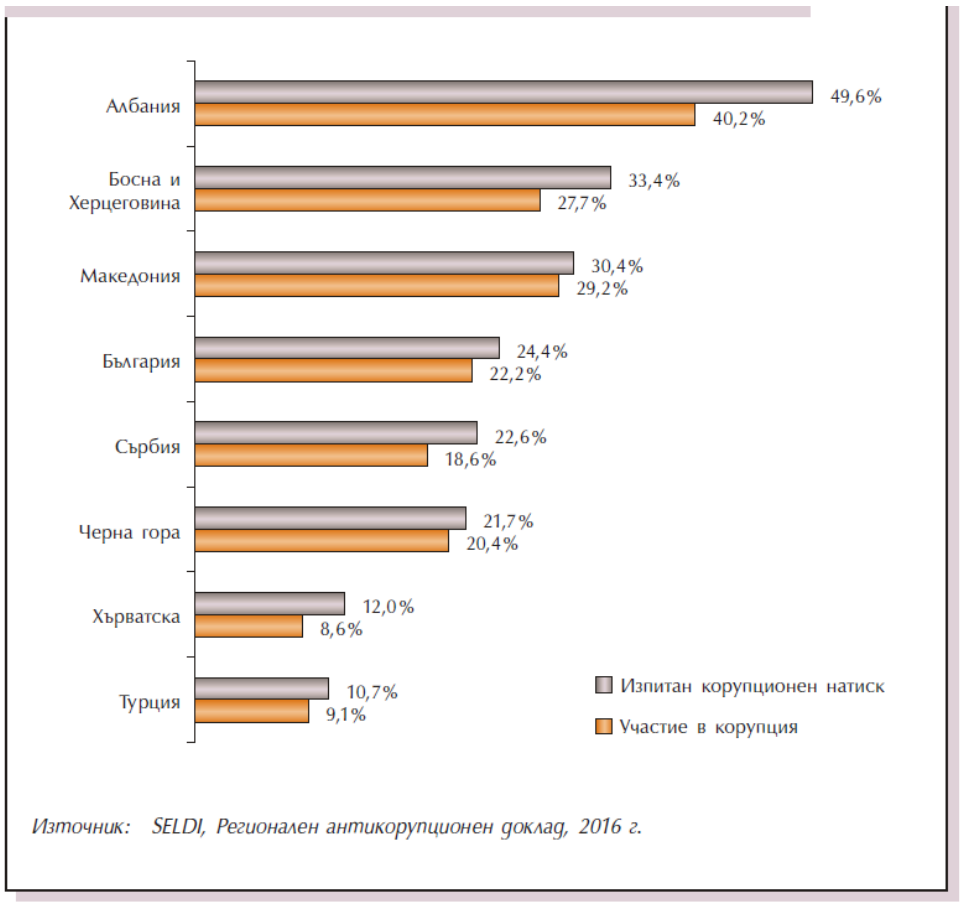
Данните за 2016 г. (Фигура 1) показват, че нивото на корупция в администрацията е било съизмеримо с това през 2000 г.

Зависимостта на равнището на корупция от политическата ситуация се вижда ясно в периода 2013 – 2014 г., когато е регистрирано най-високото наблюдавано ниво на корупция в администрацията – 29,3 % от населението над 18 г. възраст съобщава, че е участвало в корупционни сделки най-малко веднъж през предходната година.

До 2013 г. динамиката на корупцията следва изборния цикъл – намалява след встъпването в длъжност на всяко следващо правителство и се връща към по-високо ниво в края на неговия мандат. Рязкото увеличаване на корупционния натиск през 2013 г. се обяснява с високите нива на политическа нестабилност, които водят до два кръга от предсрочни парламентарни избори и масови улични протести. Данните за 2016 г. показват, че въпреки някои по-строги мерки за административен контрол, административната корупция нараства. В периода 2011 – 2016 г. равнището на административната корупция се удвоява.

От една страна, България е в неблагоприятно положение в сравнение с нейните съседи в Югоизточна Европа (Фиг. 2). За сравнение, стойностите на индикаторите за административна корупция за 2015 г. са 8,6 % за Хърватска, 9,1 % за Турция, 18,6 % за Сърбия и 40,2 % за Албания. В периода 2000 – 2002 г., когато е осъществена първата диагностика на разпространението на корупцията в Югоизточна Европа с помощта на Системата за мониторинг на корупцията, резултатите за България, макар и

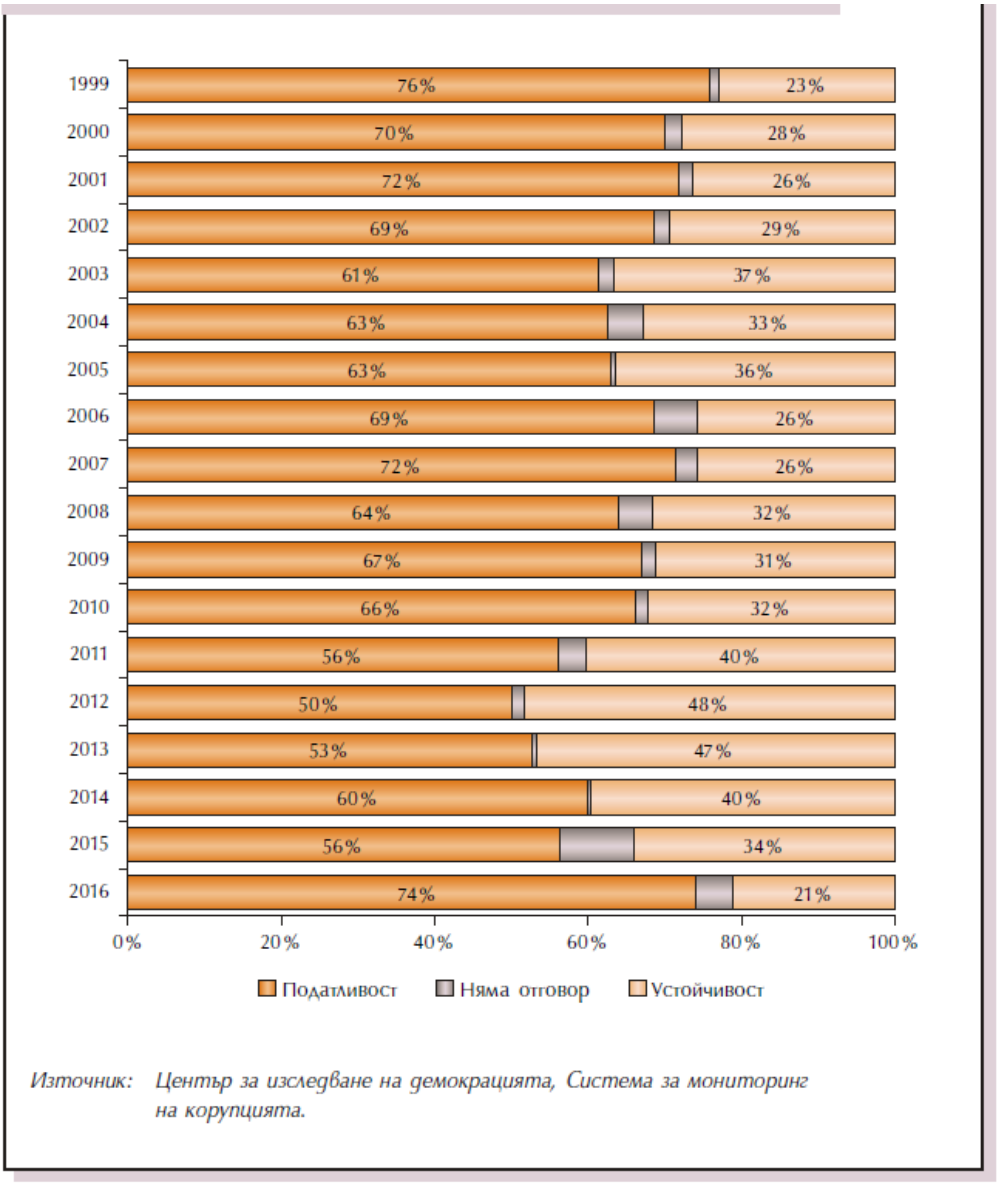
неблагоприятни, отреждат на страната относително най-добра позиция в региона по отношение разпространението на административната корупция.



Фигура 2. Участие в корупцията в Югоизточна Европа (даване на подкупи и изпитан корупционен натиск, % от населението над 18 г.) [9]

От друга страна, позицията на страната спрямо други държави – членки на ЕС е много неблагоприятна. Данните за оказван корупционен натиск (предложение на държавен служител за сключване на корупционна сделка) в България за периода 1999 – 2015 г. варира в диапазон 25-35 % от възрастното население, докато средната стойност за ЕС е 4 %, а тази за Дания е 1 % от населението на възраст 18 и повече години [10].

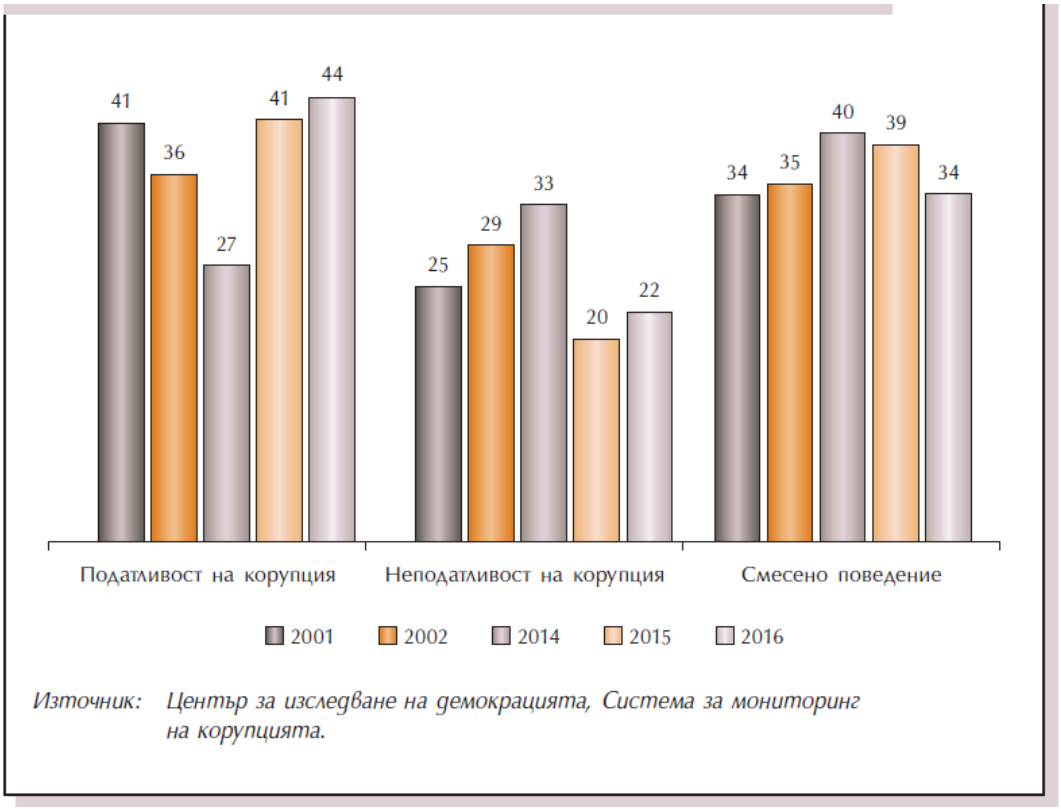
Данните на Центъра за изследване на демокрацията за периода след 1999 г. показват, че случаите на оказван натиск, водещ до корупционни сделки, варират през годините в диапазона 30-50 % в зависимост от устойчивостта на гражданите на корупционен натиск (Фиг. 3). Повечето корупционни сделки (по сведения на гражданите) са инициирани от държавните служители. Устойчивостта на корупционен натиск варира през годините, но до 2011 г. се наблюдава тенденция към бавно подобрение (повече граждани отказват да участват в корупционни сделки). Оттогава тенденцията се влошава и през 2015 г. устойчивостта на корупционен натиск, оказван от държавните служители, спада до нива, сравними с 1999 г.



Фигура 3. Податливост и устойчивост на корупционен натиск [4]

Тенденциите при разпространението на корупцията в бизнес сектора също са обезпокоителни. През 2015 г. около 18 % от бизнес организациите съобщават, че им е оказван корупционен натиск от страна на държавни служители. Тази стойност е значително по-висока от средната за ЕС (4 %), което показва, че е налице сериозен проблем [10].

Широкото разпространение на корупцията я превръща в обичайна характеристика на социалната среда. През 2016 г. само около 22 % от гражданите на възраст над 18 г. напълно отхвърлят възможността да участват в корупционни сделки. Други 34 % от възрастното население се колебаят и биха взели решение в зависимост от ситуацията, а около 44 % биха дали или приели подкуп (Фиг. 4).



Фигура 4. Податливост на корупция [4]

В обобщение, състоянието на корупцията в България в периода 2015 – 2016 г. може да се характеризира по следния начин:

• Критично високи нива на административна корупция.

• Институциите, които в най-малка степен са изправени пред проблеми с корупцията, са тези, които не управляват значителни обществени средства.

• Корупционните сделки са често срещани на всички нива в много обществени институции и се извършват със знанието и/или мълчаливото съгласие на висши ръководители.

В тази връзка, корупцията не е въпрос на няколко „гнили ябълки", а по-скоро системен проблем на държавната администрация. Широкото разпространение на корупцията е свидетелство, че основни обществени институции са „завладени" от частни интереси и/или много държавни институции са приватизирани от техни ръководни служители, които използват своята служебна позиция за реализиране на допълнителни доходи/корупционни ренти. Това оставя обществения интерес незащитен, публичните ресурси се изразходват неефективно или в полза на частни интереси, а общественият сектор се превръща в двойна тежест за данъкоплатците – както чрез данъците, така и чрез корупционните ренти, които те изплащат.

Корупцията в България е широко разпространена, придобила е системен характер и функционира като допълнителен данък за достъп до публични услуги [9]. Той се възприема като нещо обичайно както от гражданите, така и от държавните служители. Ендемичният характер на корупционните сделки достига такова ниво, че правителството не е в състояние да контролира ефективно своята администрация, а вместо това прокарва политики, които водят до намаляване служебната натовареност, увеличаване на заплатите, намаляване на отчетността, прозрачността и отговорността на служителите [3]. Опитите за

реформиране на администрацията срещат отпор от онези, които твърдят, че публичните институции са затрупани с работа при твърде ниско заплащане на служителите в тях.

Радикалните реформи в администрацията са блокирани, а когато се направят стъпки в тази насока, те обикновено се свеждат до намаляване броя на незаетите длъжности. Липсата на нужния капацитет или воля за реформи имат редица измерения:

• Противодействие на отчетността и прозрачността. Най-често опитите за по-голяма прозрачност и отговорност на администрацията се блокират. Много често различните административни служби блокират достъпа до информация за собствените си дейности, като по този начин крият преднамерените нарушения на закона, некомпетентните действия на служителите или други считани за недопустими от обществеността действия на публичните институции. Затова първата стъпка за преодоляване на създалото се положение е да се разреши достъпа на обществеността до електронните публични регистри, включително и до редовно обновяваните регистри и до разширеното търсене на данни в тях [8].

• Ограничаване на отговорността. Администрацията на практика е неуязвима за действията си, като щетите и преразходите се поемат от данъкоплатците. Това се отнася както за изпълнителната власт, така и за съдебната система. Честа практика е случаите на публично оповестени системни нарушения на правилата, като например тези с продаването от производителите на електричество от възобновяеми източници на енергия, произведена през нощните часове, с което си осигуряват по-високи цени, да остават без последствия.

• Толериране на злоупотреби с власт. Администрацията в повечето случаи проявява толерантност спрямо нарушенията на правилата от страна на висши служители или изпълнителски кадри. В това отношение злоупотребата с дискреционна власт винаги остава скрита и несанкционирана. Когато се разкрият съответни нарушения, в повечето случаи отговорните за това служители не получават наказания [5].

• Ниските заплати като невалиден аргумент. В редица публични изявления ръководителите на държавни институции твърдят, че техните служители имат ниски заплати и следователно „твърде строгото взиране в техните допълнителни приходи” е социално неприемливо. Най-често понятието „ниско заплащане” не се основава на сравнение с размера на възнагражденията на служителите в други институции в страната, а с тези в по-развитите страни – членки на ЕС.

Провалът на наблюдението на имуществото. Провеждането на една от най-важните антикорупционни мерки – декларирането на приходите и личното имущество – на практика бе провалено, тъй като досега няма нито един случай на наказание за нарушаване на това задължително изискване. Обикновено декларациите за имуществено състояние се подават в срок, но поради липсата на достатъчни институционални ресурси и управленска воля, на практика те не се проверяват за несъответствия, а случаите на нарушения не са разследвани. Много са случаите на държавни служители, за които е публично известно, че живеят охолно и чиито доходи не са проверявани от контролните и правоприлагащите органи.

• Държавни служители в ролята на „членове” на организирани престъпни групи. В някои публични институции служители се държат като членове на организирана престъпна група, чиято цел е събиране на корупционна „рента”. Такъв е примерът с арестуваните след дълъг период на видеонаблюдение членове на група служители в изпълнителната агенция „Автомобилна администрация”. Подобна е ситуацията, възникнала в Държавната агенция за метрологичен и технически надзор, където бе установено, че 600 бензиностанции са били извадени нарочно от списъка на Агенцията и

така са били изключени от контрола, осъществяван с нейното техническо оборудване. Тези корупционни практики са тясно свързани с широкомащабната намеса от страна на политици на изборни длъжности в работата на държавните структури. Веднага след идването си на власт, например, всяко поредно правителство започва дейността си със „завладяване" на ключови контролни и правоприлагащи институции, чрез назначаване на политически лоялни дейци на ръководни длъжности. Особено важно се счита завладяването на Министерството на вътрешните работи, Агенция „Митници" и други подобни институции. Показателно е, че често политическите дебати са изпъстрени с обвинения, че дадена партия „завзема държавните институции", за да „консумира власт". Обстоятелството, че тези обвинения се считат за клишета, показва, че различните форми на политическата корупция, патронаж и завладяване на държавата са се превърнали в нормални практики на политическата класа [6].

3. Заключение

Корупцията е комплексно социално-икономическо, административно, политическо и наказателноправно явление. Тя е налице тогава, когато се удовлетворяват лични интереси за сметка и във вреда на обществени. Като обществено отношение корупцията е форма на нерегламентирана социална размяна, в която и двете страни преследват определен интерес.

С течение на годините всичките управленски нива в България са завладявани от частни интереси, което доведе до ниска ефективност и намаляване размера на публичните ресурси на изпълнителната власт. Дейността на повечето правоприлагащи и контролни институции е блокирана или затруднена от една страна от опитите за извоюване на нелегитимни привилегии, а от друга страна от частни интереси, които на практика контролират политиките на държавните институции.

Корупцията в България е социално явление, което на този етап не може да бъде ликвидирана, единствено бихме могли да работим в посока нейното ограничаване в обществото, чрез създаване на механизми за противодействие.

Съществена причина за разпространение на корупцията в държавния апарат е липсата на модерно законодателство. В тази връзка не са уредени правно значими сфери от дейността на администрацията.

Борбата срещу корупцията е дълг не само на държавата, но и на цялото общество.

ЛИТЕРАТУРА:

[1] Антикорупционни политики срещу завладяването на държавата. Център за изследване на демокрацията. София. 2014. http://www.csd.bg/.

[2] Български тълковен речник. С., 1995г., с.386.

[3] Диманова Д., "Кризата като социално явление и фактор, влияещ върху състоянието на националната сигурност". Годишник ШУ "Епископ Константин Преславски". Шумен. 2014, Vol. IV E, ISSN 1311-834X.

[4] Доклад за оценка на корупцията 2016: Завладяване на държавата. Противодействие на административната и политическата корупция. София. 2016. http://www.csd.bg/

[5] Мониторинг на антикорупцията в Европа: Оценка на антикорупционните политики и измерване на корупцията. Център за изследване на демокрацията. София. 2015. http://www.csd.bg/

[6] Христов, Х., Исаев, Г. „корупцията в правоохранителните органи – заплаха за вътрешната сигурност на държавата", Научно-практическа конференция на тема „Право и сигурност", на Центърът по юридически науки на Бургаския свободен университет 29-30 септември 2017 г. Бургас.

[7] Христов, Хр., Граждански контрол на сектора за сигурност, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, 2015, p. 161.

[8] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018, pp. 386-391.

[9] SELDI, Ргионален антикорупционен доклад, 2016 г.

[10] TNS Opinion & Social. (2014). Corruption. Special Eurobarometer 397. Brussels: Directorate- General for Home Affairs, European Commission, p. 81.

[11] TNS Political & Social (2015). Flash Eurobarometer 428: Businesses' attitudes towards corruption in the EU.

[12] Досев, Н., „Корупция и национална сигурност“, ИКТ БАН, Юбилеен международен конгрес „40 год. България космическа държава”, Сборник с трудове на конгреса, Варна 2012 г.

Име на автор: Владислава Антонова Русева
Месторабота: студентка от III-ти курс в специалност „Системи за сигурност“, Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: vruseva01@abv.bg
Име на съавтора: преп. докторант Румяна Веселинова Василева
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: r.vasileva@shu.bg

MATTEX 2018, Volume 2, part 1 SECTION Student (Information, Technical and
CONFERENCE PROCEEDING, v. 2, pp. 359 - 369 Economical Problems of Security Systems)

CORRUPTION - SOCIAL PHENOMENON IN BULGARIA

VLADISLAVA A. RUSEVA, RUMYANA V. VASILEVA

ABSTRACT: *The proliferation of corruption is part of the effort to build public institutions of democracy and to promote the role of civil society. The first step in effectively counteracting corruption is the analysis of the various forms, mechanisms and consequences of corrupt practices as well as the successful attempt to overcome them.*

KEYWORDS: *Corruption, countermeasures, forms, mechanisms, consequences, society.*

КОРУПЦИЯТА - ОБЩЕСТВЕН ФЕНОМЕН В БЪЛГАРИЯ

ВЛАДИСЛАВА А. РУСЕВА, РУМЯНА В. ВАСИЛЕВА

АБСТРАКТ: *През последните години корупцията се превърна в глобална заплаха не само за икономическото развитие на отделните страни и техните международни връзки, но и за глобалната икономика и политиката като цяло. Дори и след присъединяването на България към ЕС корупцията в сферата на държавната администрация продължава да бъде престъпление без наказание. Въпреки добрия икономически растеж и известен успех в антикорупционните реформи, страната е изправена пред два големи дефицита в противодействието на корупцията: политическа воля и административен капацитет.*

1. Въведение

Корупцията се превърна в един от най-дебатираните проблеми, пред които са изправени всички общества. Корупцията и необходимостта от противодействие на нейните прояви все повече се тълкуват като ключови критерии за утвърждаването на демократичните институции и за въвеждането на съвременните стандарти на прозрачност и демократичен контрол в управлението на обществото. Поради голямото разнообразие на корупционни практики дори самото дефиниране на този феномен е обект на различни, понякога разминаващи се интерпретации. Трудности и неясноти съществуват и при определяне на обхвата, приоритетите и действащите лица [8].

Като комплексно явление, корупцията представлява отрицание на честната конкуренция в стопанската сфера, демотивира предприемачеството, стимулира сенчестата икономика и стопанската престъпност, влошава публичните услуги и утежнява социалното бреме за гражданите. По такъв начин корупцията допринася за увеличаването на пропастта между бедни и богати и се превръща в пряка заплаха за демократичните устои на обществото [4].

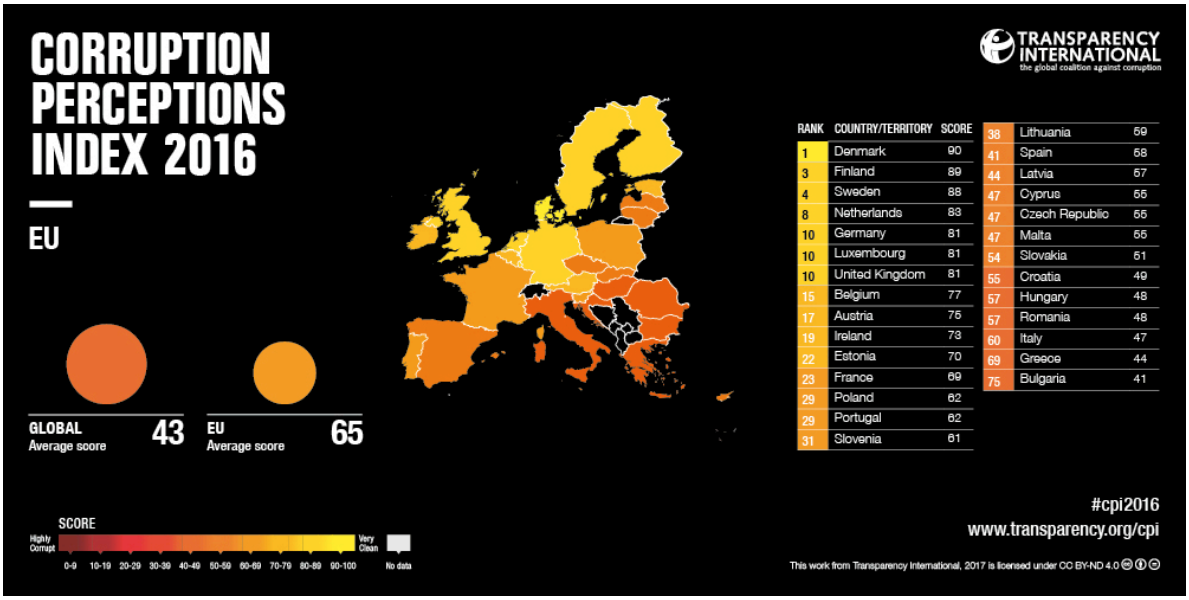
Настоящия доклад анализира същността на корупцията, разнообразните ѝ форми и типологията на корупционните практики.

2. Изложение

Корупцията е обществено явление, което е познато на човечеството от хилядолетия. В последните години то отново е обект на интензивно обсъждане в публичното пространство и се коментират многобройни случаи на корупция в различни обществени сфери. Независимо от това, макар да звучи парадоксално, все още липсва ясна и добре структурирана обществена представа за същността и характеристиките на това явление. В

общественото съзнание няма изградено и наложено общоприето разбиране за това що е корупция, а за нея често се мисли като за нещо, което се подразбира и няма нужда от специално уточняване. Проблемът се усложнява и от отсъствието на категорична правна дефиниция на понятието „корупция“, макар че то се използва като официален и законов термин. В него обаче се влага различно съдържание в различен институционален и правен контекст. Неяснотата се допълва от широката и нееднозначна употреба на понятието „корупция“ в областта на икономиката, политологията, етиката и особено в журналистическата практика. При тази ситуация е необходимо по-прецизно очертаване на възможните интерпретации (ежедневни, законови, международно-правни, аналитични) и внасяне на определено единство в разбирането на термина „корупция“.

Според Индекса за възприятие на корупцията през 2016 г. на „Прозрачност без граници“, България за поредна година остава най-корумпираната страна в Европейския съюз, а в световната класация отстъпва с 6 позиции и пада до 75-то място сред общо 176 страни (фиг.1).



Фигура 1. Индекс за възприятие на корупцията през 2016 г.

Анализът на резултатите през последните 19-те години, в които България е част от изследването, дава основание за критична оценка и показва, че борбата с корупцията е в застой.

Сравнителните данни за индекса на България за последните пет години показват липса на какъвто и да било напредък: страната остава далеч под критичната стойност от 50 пункта, което е показател за системно несправяне с това явление.

Сравнителните резултати от изследването за България подчертават острата необходимост от промяна в политиката за противодействие на корупцията, като в тази връзка трябва да бъде изоставен формалния подход в борбата с нея и да бъде проявен ясен ангажимент за дълбоки реформи в институциите, които играят основна роля в тази област [1].

Корупцията е многопластово социално, политическо и икономическо явление, негативен социален феномен, който датира от векове и съпътства упражняването на власт на различни нива от организирания политически и обществен живот на хората. Понятието „корупция“ произлиза от латинската дума „corruptio“, която означава „разваленост,

изхабеност, лошо състояние, лъжливост, подкупност“. През годините се разширява обхвата на понятието, неговите мащаби, сферите на разпространение и формите му, кръга корупционни престъпления и потенциалните извършители. То се употребява с различно, често пъти неясно съдържание. Няма универсална и общоприета дефиниция на това явление.

Европейска рамка

В Европейската правна рамка понятието „корупция” е дефинирано по два начина- пряко чрез регламентация на легална дефиниция и косвено чрез очертаване на рамката на корупционните престъпления и възможните извършители, т.е. чрез формулиране на определения на различни понятия, свързани с корупционни правонарушения или дефиниращи възможните субекти на такива правонарушения.

За първи път легална дефиниция се дава в Гражданската конвенция за корупцията на Съвета на Европа, приета на 04.11.1999 г.: „Искането, предлагането, даването или приемането, пряко или косвено, на подкуп или всяка друга неследваща се облага или обещаването на такава, което засяга надлежното изпълнение на някое задължение или поведението, което се изисква от приемащия подкупа, не полагащата се облага или обещаването на такава“.

В Наказателната Конвенция относно корупцията, приета на 27.01.1999 г. понятието се дефинира по косвен път, чрез регламентация на видовете корупционни престъпления /различните форми на подкуп и търговия с влияние/ и субектите на потенциалните корупционни действия. Макар и не така подробни легални дефиниции, свързани с корупцията се предлагат и в други международноправни актове като се дефинират понятията „активна” и „пасивна корупция”, „ измама”, “длъжностно лице”, „правителствен служител”, „юридическо лице”, „организирана престъпна група” „пасивна и активна търговия с влияние” и други.

Законодателна уредба на понятието в европейски държави

В законодателната рамка на европейските държави също е налице стремеж за очертаване на понятието, като различните страни имат различен подход и уреждат понятието в различни по ранг и характер нормативни актове. Обществената и юридическата дефиниция на корупцията е различна като някои от страните регламентират само понятието „корупция“ /Белгия/, други съдържат регламентация на понятията „корупционни престъпления“, „корупционно поведение“, „корупционни действия“ /Полша/. В голямата си част подходът в различните държави и в редица международно правни актове при изграждането на антикорупционно законодателство има комплексен характер. Наред с понятието „корупция” се влага не само наказателно правно съдържание и смисъл, но и се посочват някои от характеристиките на „корупционни действия” и „корупционно поведение”. Други очертават по косвен път понятието чрез посочване на връзката на корупционните деяния с други сфери на правно регулиране, определя се кръгът от възможни субекти на корупционно поведение, въвеждат се етични параметри (характеристики) на поведението, свързани с корупционното поведение.

Законодателна уредба на понятието в националната правна рамка на РБ

В българско законодателство липсва дефиниция на понятието „корупция“ или на понятията „корупционни престъпления“, „корупционно поведение“, “корупционни действия“.

Терминът „корупция“ се използва в наказателни, гражданско-правни и административни актове с различен обхват, субекти и съдържание.

Детайлна законова уредба се съдържа най-вече в наказателното правораздаване. Липсата на легална дефиниция води до „технизиране на понятието“ и промени в

съдържанието му. Наблюдава се ориентация към определяне на понятието чрез „комбиниран прочит“ на международните актове, съдържащи дефиниции за корупция или очертаващи обхват на корупционните престъпления.

Към настоящия момент наказателно-правната уредба в Република България урежда без претенции за изчерпателност разгърната номенклатура на корупционни престъпления, които са разпръснати като състави в особената част на наказателния кодекс в различни глави: престъпления против стопанството, престъпления по служба, престъпления против правосъдието, осуетяване на наказателното преследване, подкуп.

Гражданско-правни и административни актове също използват термина „корупция” като с това се обозначават различни по обхват, субекти и съдържание обществени явления /ЗОВС, ЗМВР, ЗДАНС, решения на Конституционния съд (напр. р. № 5 от 1993 (ДВ, бр. 30/1993 г.) и р. № 5 от 1995 г.(ДВ, бр. 62/1995 г.).

Научната доктрина твърди, че „всъщност точно тук се корени и основната трудност при дефинирането на корупцията”. Сочи се, че наказателния кодекс и други закони не могат да дефинират понятието, тъй като корупцията не е деяние, а сложно и комплексно многопластово явление, т.е. „това е невъзможно да бъде сторено чрез една норма в един закон, която да съдържа изчерпателна (крайна) дефиниция” [2].

Различни автори са единодушни, че наказателния кодекс не обхваща пълно всички форми на корупционно поведение, т.е. налице е празнота относно регламентацията на „по-незначителни деяния с оглед на тяхната обществена опасност, прояви, които остават задача на останалото законодателство [5].

Изразяват се становища, че „Явлението корупция е по-широко по обхвата си в сравнение със сега регламентираните в наказателния закон случаи. Като явление то обхваща и случаи, в които облагата, която се получава, няма материален характер, не е „имотна облага” по смисъла на наказателния кодекс. В контекста се излагат елементарни примери: „Могат да се определят като корумпирано поведение например случаите, в които е налице злоупотреба с власт или нарушаване на служебни задължения с цел лично облагодетелстване за сметка интересите на обществото; лицето се поставя в зависимост от получаването на определена облага при извършването на правомерно действие по служба; противозаконно се преразпределят ресурси в ущърб на обществения интерес, когато деецът цели лично (не само негово, но и на друго лице) облагодетелстване” [6].

Това води до извода, че липсата на законова уредба относно дефиниция на понятието „корупция“ и/или „корупционно поведение“, „корупционно действие“ затруднява квалифицирането на определени действия/поведения като корупционни. За да бъде наблюдавано, корупционното поведение следва да бъде конкретизирано и локализирано.

Едно от възприетите определения обозначава с понятието „корупция“: злоупотребата с икономическа, политическа, административна и съдебна власт, която води до лично или групово облагодетелстване за сметка на правото и законните интереси на личността, на конкретна общност или цялото общество.

В контекста на тази дефиниция реализацията на корупцията предполага наличието на четири необходими елемента:

служител (или група служители) в обществения сектор;

• дискреционна власт (възможност за вземане на самостоятелни решения по усмотрение);

• злоупотреба с публична власт от страна на служителя;

• извличане на лична или групова изгода.

Типология

Корупцията се проявява преди всичко в зоната на взаимодействие на публичния сектор с гражданите и частния бизнес. Най-често се разграничават два основни типа корупция, които се различават по своите мащаби, субектите на извършване, механизмите на реализация и др.

Голяма корупция. В голямата корупция влизат висши държавни служители, политици и бизнесмени, вземащи решения за разпределяне на значителни ресурси. Тя е с по-сложни и по-фини механизми на осъществяване. Обикновено се реализира чрез посредници. Посредниците между даващия и приемащия подкупа играят ключова роля. Тук размерите на злоупотребите и облагите са в много по-значими по размер, а границите между активната и пасивната страна се разминават. Обикновено има минимална прозрачност по линията на договаряне на взаимните изгоди.

Малка корупция. В малката (бюрократичната) корупция влизат служители от по-нисък ранг, които непосредствено контактуват с гражданите и с представителите на малкия и среден бизнес. Тя е по-масова и с всекидневен характер. Съответно за нея са типични по-малките по мащаб плащания, подаръци и услуги.

Ролите на основните действащи лица в осъществяването на корупционното действие особено в случаите на „малката корупция“ са следните:

служителят е активният и пряко заявява „цената“ за услугата която ще извърши след корупционния акт;

• служителят не афишира директно желанието си за лично облагодетелстване, но създава пречки от формален и неформален характер и намеква за корупционната алтернатива и принуждава ответната страна сама да стигне до нея;

• лицето, което желае да получи някакъв вид услуга, само предприема активни действия, като директно предлага на съот¬ветния служител определено корупционно „възнаграждение“.

Тези механизми на реализация се използват и в двата най-често срещани случая на корупция:

• при незаконното извличане на лична облага от служителя, задължен служебно да извърши определени дейности или административни услуги, тоест те са „в съответствие със закона” и се явяват както бе отбелязано своеобразен ускорител (“смазка“) за по-бързото, по-доброто или по-сигурното решаване на проблема на даващия подкупа;

• служителят извършва действия, осигуряващи на даващия подкупа облаги, на които той няма право (тоест в „нарушение на закона“).

Общото между двата случая е, че се купуват благоприятни решения и действия на държавния служител от заинтересовани лица, групи или организации, създавайки квази-пазар на административни и политически услуги.

В зависимост от субекта на корупционното отношение обикновено се разграничават активна и пасивна корупция.

В активна позиция е този който предлага подкупа или другата неследваща се облага. В пасивна позиция – този който приема. И двете страни са с еднаква отговорност.

Активна корупция имаме когато обещаваме, предлагаме или даваме пряко или косвено, на каквато и да е не следваща се облага на длъжностното лице, за да извърши или да не извърши действие по служба.

Пасивна корупция имаме при поискване или приемане, от което и да е длъжностно лице, пряко или косвено, на каквато и да е не следваща се облага за него или за някой друг, или на приемането на предложения или обещания за такива облаги, за да извърши или да не извърши действия по служба.

От гледна точка на начина на реализация на корупционния акт, се разграничават няколко най-разпространени механизми:

• Даване на подкуп на едно служебно лице, при което действието се извършва на „четири очи“. При този вариант доказуемостта на извършеното действие е максимално затруднена и това го прави предпочитан начин за осъществяване на корупционни действия.

• Даване на подкуп на няколко служебни лица, свързани професионално и/или изпълняващи съвместно определени функции. Среща се в случаите, в които, за да се осъществи корупционно действие, е нужно съучастието на група служители. В такива групи съществува особена „корупционна“ солидарност.

• Даване на подкуп чрез посредник. В случаите, в които между двамата участници в корупционното действие не съществуват вече установени отношения или в случаите, в които служебното лице има възможност да остане анонимно, се прибягва до услугите на трето лице, чрез което да се договорят условията и параметрите на корупционната сделка.

Според честотата на нейното прилагане корупцията бива системна и инцидентна.

Системна е когато съществуват бюрократични предпоставки за тяхната повторяемост при липса на контрол и прозрачност на дадената дейност както и при чиновнически монопол върху определена услуга.

Според начина на реализирането ѝ корупцията бива пряка и косвена.

При пряката имаме непосредствено облагодетелстване на получаващия подкупа и получаване на желаната услуга за даващия. Косвената осигурява главно предимства за близки, приятели или стратегически партньори.

Според мащабите на осъществяване корупцията бива национална и международна.

Националната корупция се осъществява в рамките на дадено общество и държава. Една от най-опасните форми тук е обвързването на представителите на държавните институции с интересите на организираната престъпност, поставящо под съмнение националната сигурност.

Международната корупция най-често се проявява под форма на дарения. Често тя е вградена в избраната политика и се отнася до:

• достъпа до поверителна информация;
• връзката с официални и неофициални пазари;
• слаб граничен и митнически контрол;
• наличието на офшорни зони и фирми;
• слаби и привидни данъчни убежища, привидни регулационни режими;
• реализиране на дейности със съмнителен произход.

Причини за поява на корупция

Корупция има, когато една организация или човек имат монополна власт над една стока или услуга, имат свободата на действие да решават кой ще я получи, колко този човек ще получи, като за това не носят отговорност.

Корупцията процъфтява, когато институциите са слаби, а действието на пазарните принципи в икономиката е ограничено. Тя се проявява там, където користният интерес намира благоприятни възможности и предпоставки за реализация. Най-простият модел, описващ факторите, влияещи върху размера на корупцията, е:

К (корупцията) = М (монополни права) + В (възможност за взимане на решение по усмотрение) - О (отговорност)

Мащабите на корупцията в дадена сфера са толкова по-големи, колкото по-голяма е монополната власт (контрол върху определени ресурси) и възможността за взимане на

решения по усмотрение от овластените лица и колкото по-ниска е степента на тяхната отговорност за взетите решения и извършените действия.

Корупцията обикновено е свързана с такива сфери на дейност, в които държавата има монополни права или съществува възможност за упражняване на изключителни правомощия върху определени ресурси (законодателство, изпълнителна власт на национално и местно равнище, поддържане на обществен ред, съдебна система, контрол върху естествени монополи и др.). Там, където има власт и възможност за свободно упражняване на произтичащите от нея влияния и правомощия, съществуват предпоставки за възникване на корупция. По силата на това обстоятелство корупционните практики намират най-силен разцвет в онези сфери на обществения живот, в които определен обществен ресурс се намира под контрола на един или няколко служители. Упражняващият власт в този контекст е ценен в качеството си на фактор, който може да задоволи някакъв частен интерес или да осигури доход [7].

Като обществено отношение корупцията се проявява във форма на нерегламентирана социална размяна. От икономическа гледна точка разпространението на корупцията се подчинява на класическите пазарни принципи. По-голямото търсене (изразено чрез броя на даващите подкуп и размера на предлаганите суми) и ограниченото предлагане (наличието на оперативна самостоятелност на служители в обществения сектор за вземане на решение) индуцират и по-голяма корупция.

„Корупционната цена“ (големината на подкупите) естествено се намира и в пряка връзка със стойността на очакваната изгода. Механизмите на корупционно поведение се различават и в зависимост от служебния статус на овластените лица, който по правило е тясно свързан с притежаваните от тях правомощия и власт. Принципът тук е: „колкото по-висок етаж от йерархията обитава един служител, толкова по-голям е мащабът на извършваната корупционна сделка“. Еквивалентът за исканата услуга може да бъде пари, материални ценности, услуги с особена стойност и др. В този смисъл корупционните действия могат да се разглеждат като специфични икономически взаимоотношения, от които в повечето случаи и двете страни имат интерес. Те са алтернативни на легалните пазарни механизми, ерозират нормалните икономически отношения и деформират критериите за ефективност на икономическите решения и действия.

Корупцията е нерегламентирана социална размяна на блага, която е незаконна, неморална и недопустима. Изхождайки от икономическите, социалните, политическите и законовите причини за нейното възникване, можем да изброим и някои от основните причини за появата на корупцията. По-долу изброените предпоставки, макар и формулирани общо, имат за цел на едно достъпно ниво да изведат причините за корупцията, изхождайки от основата на човешката същност и имайки впредвид начина на функциониране на едно демократично общество:

1. Причина за корупцията е човешкият егоизъм („Искам да имам повече блага”);

2. Причина за корупцията е човешката слабост (Морално-етичните и законовите забрани не са достатъчна бариера за получаване на нерегламентирани облаги);

3. Причина за корупцията е незнанието (Ниската професионална квалификация на икономическите и гражданските агенти създават предпоставки за корупция);

4. Причина за корупцията е лошото възпитание (Липсата на морални устои, както на ниво обществено самосъзнание, така и на по-ниски нива – групови, семейни, религиозни, медийни и др.);

5. Причина за корупцията е желанието за по-добър начин на живот (Желанието за едно по-добро материално и духовно задоволяване на потребностите на отделния индивид

не следва да се толерира от обществото, ако осъществяването на това желание е в разрез с моралните и законовите устои на това общество);

6. Причина за корупцията са ниските доходи (Една от най-трудно разрешимите дилеми в борбата с корупцията – как длъжностно лице, което получава няколко стотин лева, а управлява и/или контролира активи или икономически процеси за няколко стотин хиляди, понякога за милиони да не се подаде на корупционния натиск);

7. Причина за корупцията е нелоялната конкуренция (Икономически неизгодно за обществото е в процеса на конкуренция да спечели онзи икономически субект, чиито продукт е с по-ниско качество, но който има механизми за влияние върху решението за избора на продукт – обществените поръчки);

8. Причина за корупцията е политическата демагогия (Липсата на ефективен обществен и медиен контрол върху политиците за мониторинг на процеса „обещано-изпълнено”);

9. Причина за корупцията е неконтролируемата власт (Постулат, който не се оспорва от никой. В основата на демократичната правова държава е баланса и взаимното контролиране на отделните власти);

10. Причина за корупцията е бюрокрацията (Доколко всяка административна структура се състои от хора, централният въпрос тук е за намаляване и/или правилно „дозиране” на дискреционната власт, която се дава на отделните длъжностни лица);

11. Причина за корупцията е липсата на информация (Тук стои въпросът за тази информация, която длъжностните лица са задължени да предоставят на обществото в изпълнение на публичните си функции, а не за тази информация, която отделните лица са длъжни да знаят, за да участват пълноценно в стопанския оборот – достъпността на условията за участие в програмите на ЕС) [3];

12. Причина за корупцията е многото информация (Невъзможността на икономическите агенти да дефинират и да защитят своя собствен интерес поради незаинтересованост, непрофесионализъм, липса на ресурси и капацитет и др. – „По коя програма на ЕС да участвам?”);

13. Причина за корупцията е липсата на правила (Липсата на правила създава възможност дадено длъжностно лице да действа дискреционно (по свое усмотрение) в рамките на широк кръг от правомощия)

14. Причина за корупцията е недостига на времето. (Пример: трябва да се регистрира фирма за 5 дни вместо нормалния срок от 20-30 дни);

15. Причината за корупцията е ненамерения баланс между правото, морала и справедливостта („Трите кита“, на които се крепи този баланс и които следва да очертават неговите контури са политическата класа, свободните медии и гражданското общество в лицето на неправителствените организации).

Според изследователите на явлението корупция, условията които благоприятстват нейното разпространение са:

• концентрация на власт у хора, които не са пряко отговорни пред обществото, което е честа практика при недемократичните режими;
• липса на прозрачност при решенията на правителството;
• големи по размер обществени средства, използвани за даден проект;
• наличие на затворени клики и мрежи от „наши хора“;
• слабо правораздаване;
• ограничена свобода на словото или свобода на печата;
• нископлатени държавни служители;
• апатична, незаинтересована или наивна общественост.

Сфери на разпространение на корупцията

Корупцията може да бъде открита практически във всички сфери на обществения живот. Тя е комплексен феномен, обусловен от спецификата на социокултурната история на дадено общество, политическото и икономическото му развитие, бюрократическите традиции и управленските практики.

Проявите на корупционно поведение имат своя специфика в зависимост от конкретната област, в която се реализират. От тази гледна точка най-често се разграничават няколко основни сфери на проява на корупционни практики:

• корупция в сферата на държавната администрация (правителство, държавни ведомства, местни органи на властта и др.);

• политическа корупция (парламент, политически партии);

• корупция в съдебната система и правоохранителните институции (съд, прокуратура, следствени служби, полиция);

• корупция в сферата на обществените услуги (здравеопазване, образование, социално подпомагане и др.);

• корупция в частния сектор (транснационални компании, местни бизнес организации, медии и др.);

• корупция в третия сектор (граждански сдружения, неправителствени организации и др.).

Последици за обществото от наличието на корупция

Независимо от разнообразието на сферите на проявление, корупцията поражда едни и същи отрицателни последици за обществото. Нейното въздействие върху последното е винаги разяждащо и води до:

• извращава почтеността на индивида и подкопава управлението на държавата;

• разрушава културата и манталитета на всички нива;

• дестабилизира обществото;

• застрашава националната, регионална и глобална сигурност;

• опетнява понятието гражданин;

• деградира моралните устои забавя напредването на отделната личност в борбата за постигане на общо политическо и икономическо добруване;

• затруднява сключването на положителен обществен договор;

• противопоставя се на религиозни и морални принципи, които времето и историята са утвърдили като структурно определящи за обществото и държавата, както и във взаимоотношенията между хората.

Широкият обхват на дефиницията на същността, както и масовото ѝ разпространение в обществения живот подсказва, че противодействието срещу корупцията и на национално и на глобално ниво изисква координирани усилия, ангажиращи както държавата, така и гражданите от всички сектори на обществения живот.

Защо е трудно да се разкрият корупциите? Защото и двете страни имат причини да запазят своята тайна. От едната страна имаме страх от наказание и обществена дискредитация, а от другата страна има страх от отмъщение. Затова борбата с корупцията може да бъде само при наличие на стабилни правни основания и последователна воля и непримиримост за борба с нея, както и ако има ефективна правна защита и гаранции за физическата сигурност за лицето, което е изнудвано за подкуп и пожелало да сътрудничи на правно-наказателната система. Ефикасната борба изиска уточняване и на въпросът: Има ли косвени начини за корумпиране? Отговорът е положителен когато имаме получаване на неследващи се услуги. Такива имаме най-често в т.нар. състояние на

„конфликт на интереси”. Например често държавни все още предприятия, а и частни такива са длъжни да внасят пари във фондации, дори и когато нямат пари да внесат данъците си към държавния бюджет. Конфликт на интереси имаме и когато даден служител извършва паралелни дейности в обществения и в частния сектор. Същото се отнася и когато такава паралелна дейност извършва много близък негов родственик. Едно такова състояние винаги стимулира използването на общественото положение за частни интереси. От изясняване се нуждае и въпросът: Може ли корупцията да е едностранна, само ако имаме „оферта“ без тя да е оползотворена? Отговорът е положителен. Предлагането или искането на подкуп или друга корупционна сделка е също наказуемо по силата на закона, без да се е осъществило даването и приемането на предвидената облага.

3. Заключение

Налице е празнота в законодателството относно понятието „корупция”/, „корупционно поведение”/ „корупционно действие”, „органи за борба с корупцията, очертаване на персонален състав - кръг на възможни субекти. Това остава определени деяния и определени лица ненаказуеми. Липсват единни национални индикатори за корупция. Квалифицираните като корупционни престъпления състави са разпръснати в различни глави на наказателния кодекс.

Необходимо е приемането на нов антикорупционен закон/кодекс за борба срещу корупцията, дефиниращ понятието „корупция“ пряко или косвено, институционалната рамка и взаимодействието между различните органи, както и извършване на съответни промени в наказателния кодекс и специализираните закони.

Корупцията е разнообразно антиобществено и противозаконно явление, което заплашва с разпадане обществото и разяжда силата на държавата. Нейното осъществяване зависи от множество личностни и обществени слабости и несъвършенства. Като деяние корупцията е преди всичко морален акт – въпрос на мислене, нагласа и среда.

ЛИТЕРАТУРА:

[1] Асоциация „Прозрачност без граници”, Индекс за възприятие на корупцията за 2016г., http://transparency.bg/bg/transp_indexes/.

[2] Груев, Л., Велчев, Б., „Наказателно-правни аспекти в борбата срещу корупцията“. Коалиция 2000. С. 2000. http://www.csd.bg/artShow.php?id=13015.

[3] Марков, Ю., Христов, Х., „ПРОБЛЕМНИ ОБЛАСТИ В ПРЕВЕНЦИЯТА И БОРБАТА С ИЗМАМИТЕ ПО ПРОЕКТИ, СЪФИНАНСИРАНИ ОТ ЕС И НАЦИОНАЛНИЯ БЮДЖЕТ НА РЕПУБЛИКА БЪЛГАРИЯ – МАНИПУЛИРАНИ ОФЕРТИ В ТРЪЖНИ ПРОЦЕДУРИ”, Научно-практическа конференция на тема „Право и сигурност”, на Центърът по юридически науки на Бургаския свободен университет 29-30 септември 2017 г. Бургас.

[4] Национална Стратегия за превенция и противодействие на корупцията в Република България 2015-2020г. http://www.strategy.bg/StrategicDocuments/

[5] Таков, К., Гражданскоправни аспекти на корупцията. http://www.christiantakoff.com/wp-content/uploads/articles/25_Civil_Law_Consequences_Corruption_BG_Juridicheski_Svjat.pdf

[6] Терзиев, В., Ничев, Н., Банков, Ст., Наказателно - правни аспекти на корупцията и установени практики в България. http://www.csd.bg/

[7] Христов, Х., „Средства и способи за контрол“. Научна конференция с международно участие „Форум отбранителни технологии 2017”, на НВУ „В. Левски“ , Факултет „Артилерия, ПВО и КИС”, 20-21.04.2017 г. , на 3-5 октомври 2017 г. Шумен.Adati, T., Miyazawa, T., On paracontact Riemann manifolds. TRU Math. 13 (2) (1977), 27-39.

[8] Досев, Н., „Корупция и национална сигурност“, ИКТ БАН, Юбилеен международен конгрес „40 год. България космическа държава”, Сборник с трудове на конгреса, Варна 2012 г.

Име на автор: Владислава Антонова Русева
Месторабота: студентка от III-ти курс в специалност „Системи за сигурност“, Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: vruseva01@abv.bg
Име на съавтора: преп. и докторант Румяна Веселинова Василева
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
E-mail: r.vasileva@shu.bg

СЪДЪРЖАНИЕ

HUMANITARIAN ASPECTS OF PROTECTION OF INFORMATION
IVO V. VELIKOV 3

A VIEW ON THE PROCEDURES FOR IMPLEMENTATION OF SPECIAL INVESTIGATION MEANS IN THE FEDERAL REPUBLIC OF GERMANY
ILIN A. SAVOV 11

GENERAL ORGANIZATIONAL SECURITY THEORY
EVGENI P. MANEV 17

IMPLEMENTATION OF THE FOOTPRINTING AND RECONNAISSANCE CYBER ATTACKS AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS
PETAR KR. BOYANOV, HRISTO A. HRISTOV 23

IMPLEMENTATION OF INFORMATION SYSTEM CYBER ATTACKS AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS
PETAR KR. BOYANOV, HRISTO A. HRISTOV 34

IMPLEMENTATION OF SOCIAL ENGINEERING CYBER ATTACK AGAINST THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS
PETAR KR. BOYANOV 42

IMPLEMENTATION OF CYBER ATTACKS AGAINST WEB SERVERS AND WEB APPLICATIONS
PETAR KR. BOYANOV 52

IDENTIFICATION OF THE MAIN TYPES AND PHASES OF MODERN CYBER ATTACKS AND THEIR USE FOR IDENTIFYING WEAKNESSES IN COMPUTER NETWORKS AND SYSTEMS IN THE REGIONAL GOVERNANCE OF REGIONAL DIRECTORATES OF INTERIOR
PETAR KR. BOYANOV, VESELIN KR. RAYNOV 60

INTEGRATED MONITORING AND CONTROL SYSTEM
DIMITAR G. CHOBANOV 68

AN ALGORITHM FOR QUICK SEARCH OF IDENTIFIERS IN AN ACCESS CONTROL SYSTEM
DIMITAR G. CHOBANOV 74

THE EUROPEAN CIVILIZATION DISCOURSE AND THE SECURITY
DOBROMIR ZH. DOBREV 79

MODERN TRENDS AND ASPECTS OF THE INFORMATION SECURITY IN THE AUTOMATED INFORMATION SYSTEMS AND NETWORKS
NIKOLAY Y. DOSEV, VELIKO P. PETROV 85

ABOUT THE FINANCIAL PROVISION OF THE ACTIVITY OF A COMPANY COUNTER-INTELLIGENCE UNIT
IVAN I. KANTARDZHIEV, STANIMIR S. STANEV, HRISTO A. HRISTOV 96

TOOLS FOR DEFENSING THE SENSITIVE COMPANY INFORMATION FROM INSIDER THREATS
LUCHEZAR T. HRISTOV, STANIMIR S. STANEV, HRISTO A. HRISTOV 109

TENDENCES IN TRAINING POLICE OFFICERS ON SPECIAL POLICE TACTICS
DONCHO HR. TILEV 116

GDPBZN ACTIVITIES OF SAFETY AND PROTECTION
DONIKA V. DIMANOVA 122

INTERNATIONAL SECURITY STANDARDS
DONIKA V. DIMANOVA, ZDRAVKO YU. KUZMANOV 131

RISK MANAGEMENT IN INFORMATION SECURITY
DONIKA V. DIMANOVA, ZDRAVKO YU. KUZMANOV 139

CORRUPTION IN THE STATE ADMINISTRATION AND ECONOMIC CORRUPTION IN THE CONTEXT OF THE MEMBERSHIP OF BULGARIA IN THE EUROPEAN UNION
GALIN I. ISAEV 146

PLACE AND ROLE OF DIRECTORATE – GENERAL FOR SECURITY IN THE NATIONAL SECURITY
GEORGI HR. ZHEKOV 157

TENDENCES IN TRAINING POLICE OFFICERS ON SPECIAL POLICE TACTICS
IVELIN G. KATSEV, HRISTO A. DESEV 164

DATA FUSION IN SECURITY
KONSTANTIN K. KAZAKOV 170

ROLE AND PLACE OF SPECIAL SERVICES IN NATIONAL CRITICAL INFRASTRUCTURE PROTECTION SYSTEM - REPUBLIC OF ROMANIA
KONSTANTIN I. STOYANOV 175

THE AGGRESSION AS INTERNATIONAL CRIME
KREMENA B. RAYANOVA 183

GOVERNANCE, COMMAND AND MANAGEMENT OF THE ARMED FORCES IN PARTICIPING IN COUNTER-TERRORISM IN OPERATIONS IN THE COUNTRY
LYUBOMIR K. DUCHEV 188

NAZISM AND ISLAM
MILEN M. IVANOV 196

ORGANIZATIONAL THEORY AND SECURITY IN CRISIS MANAGEMENT
NEDELCHO R. NEDELCHEV 206

CONFLICTS IN THE ORGANIZATION AND THEIR MANAGEMENT
NELI G. BORISOVA 213

GOOD PRACTICES IN THE EDUCATION OF FEMALE MILITARY PERSONNEL IN THE EUROPEAN MILITARY ACADEMIES
NEVENA TSV. ATANASOVA – KRASTEVA 222

MANAGEMENT POLICIES IN KOZLODUY NPP
PETAR D. DJOROV 231

GEODESIAN CONTROL OF INFRASTRUCTURE OBJECTS KOZLODUY NPP
PETAR D. DJOROV 238

ESSENCE AND PECULIARITIES OF LOCAL SELF-GOVERNMENT
RUMYANA V. VASILEVA 247

REGIONAL PROJECTION ON CURRENCY WARS - THE THREAT FOR THE FINANCIAL SECURITY OF REPUBLIC OF BULGARIA
STANIMIR ST. STANEV 255

OUTLOOK AND OPPORTUNITIES FOR IMPROVEMENT OF PRIVATE SECURITY SERVICES IN BULGARIA
TATYANA M. IVANOVA 259

ISLAMIC RELIGIOUS FUNDAMENTALISM AND EXTREMISM
TIHOMIR I. SOLAKOV, HRISTO A. HRISTOV 272

NATIONAL AND CORPORATE SECURITY
TSVETELINA I. METODIEVA 285

GRADUATION OF ILLEGAL BEHAVIOR
VESELIN VELKOV 294

IDENTIFICATION AND MANAGEMENT OF OPERATIONAL RISKS IN COMMERCIAL BANKS
ZHANETA ST. GEORGIEVA-PANAYOTOVA 298

CORRUPTION IN THE PUBLIC SECTOR
ANASTASIA G. HRISTOVA, NURAY M. IDAETOVA 304

DISSEMINATION OF NARCOTIC SUBSTANCES IN THE PUBLIC AREA
AYSEN B. BASRI, DZHANSU E. MUSTAFOVA, ELITSA B. VASILEVA.....310

ASPECTS OF MIGRATION PROCESSES IN THE REPUBLIC OF BULGARIA
BLAGOVEST P. YOSIFOV, SIMEON S. KRASTEV, MARIN G. GANCHEV 315

3D VISUALIZATION OF PROGRAMS FOR PROGRAMMABLE LOGIC CONTROLLERS THROUGH SOFTWARE PRESETS
DANIEL R. DENEV, VIKTOR V. LILOV, MIHAELA A. KARADOCHEVA 320

ASPECTS OF THE USE OF WOMEN IN THE ACTIVITIES OF AN ISLAMIC STATE
EVGENIYA A. EVTIMOVA 327

TRAFFIC REPORTING AND THE ABILITY TO OPTIMIZE LAN
IVAN S. IVANOV, VIKTOR V. LILOV, DANIEL R. DENEV 331

THE MANIFESTATION OF RELIGIOUS TERRORISM
MERAL. M. GALIB, HRISTINA I. KOSEVA 336

COMPARATIVE ANALYSIS OF MODERN TYPES OF TERRORIST ORGANIZATIONS
SIBEL H. FEVZIEVA, STILIANA G. STANCHEVA.....345

CORRUPTION IN THE FIELD OF PUBLIC ADMINISTRATION
VLADISLAVA A. RUSEVA, RUMYANA V. VASILEVA 350

CORRUPTION - SOCIAL PHENOMENON IN BULGARIA
VLADISLAVA A. RUSEVA, RUMYANA V. VASILEVA.....359