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 2020

СБОРНИК НАУЧНИ ТРУДОВЕ

МАТТЕН 2020

CONFERENCE PROCEEDINGS

Том 2

Комуникационна и компютърна техника и технологии

Информационни, технически и икономически проблеми на системите за сигурност

Геодезия, картография и кадастър

Общо инженерство, технически системи и логистика

Volume 2

Communication and Computer Technologies

Information, Technical and Economical Problems of Security Systems

Geodesy, Cartography and Cadastre

General Engineering, Technical Systems and Logistics

Ш У М Е Н
2020

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 2020

СБОРНИК НАУЧНИ ТРУДОВЕ

МАТТЕН 2020

CONFERENCE PROCEEDINGS

Том 2

Комуникационна и компютърна техника и технологии

Информационни, технически и икономически проблеми на системите за сигурност

Геодезия, картография и кадастър

Общо инженерство, технически системи и логистика

Volume 2

Communication and Computer Technologies

Information, Technical and Economical Problems of Security Systems

Geodesy, Cartography and Cadastre

General Engineering, Technical Systems and Logistics

Ш У М Е Н
2020

Университетско издателство
"Епископ Константин Преславски"

Настоящият сборник съдържа научни доклади, изнесени на проведената през октомври 2020 година в Шуменския университет научна конференция с международно участие МАТТЕХ 2020 с резултатите от научните изследвания на преподаватели, докторанти, специалисти и студенти от Шуменския университет, други учебни заведения, фирми и организации.

Всички доклади, публикувани в сборника, са рецензирани.

This volume contains the reports presented on the Scientific Conference with international participation MATTEH 2020 held at Konstantin Preslavsky University of Shumen in October 2020. 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.

All papers published in this volume have been reviewed.

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

ISSN: 1314-3921

COMMUNICATIONS SECURITY (COMSEC)

IVO V. VELIKOV

Abstract: *Regulation 4300B.200 - Communications Security (COMSEC - Version 3) of the US Department of Homeland Security is a new and modern document that, with few exceptions, regulates policy in this area for virtually the entire US administration. The 2016 version intrigued me because of its topicality, because of its clean and maximally clear structure, as well as because of its obvious practicality, ubiquity and applicability. For the last two qualities we should rather look for practitioners in the IT sector, but it is a fact that the terminology and the latest regulations in our country are as close as possible and even in certain parts are directly borrowed from US regulations. As a hegemon in the field of technology and in NATO, the United States is able to impose its concepts and definitions, its procedures and mechanisms in the information community, its perceptions of communications security.*

Keywords: *Communications Security.*

КОМУНИКАЦИОННА СИГУРНОСТ

ИВО В. ВЕЛИКОВ

АБСТРАКТ: *Регламентът 4300B.200 - Communications Security (COMSEC - Version 3) на Министерството на вътрешната сигурност на САЩ е нов и модерен документ, който с малки изключения урежда политиката в тази сфера на практика за цялата държавна администрация на САЩ. Версията от 2016 г. ме заинтригува поради своята актуалност, поради изчистената си и максимално ясна структура, както и поради очевидната си практичност, повсевместност и приложимост. За последните две качества по-скоро трябва да потърсим практиците в ИТ – сектора, но е факт, че терминологията и най-новите разпоредби в нашата страна се доближават максимално и дори в определени части са директно заимствани от американската нормативна уредба. Като хегемон в областта на технологиите и в НАТО, САЩ е в състояние да налага и своите понятия и дефиниции, своите процедури и механизми сред информационната общност, своите схващания за сигурността на комуникациите..*

Keywords: *комуникационна сигурност.*

Въведение

Говорейки за Комсек, нека не бъркаме с понятия като COMPINT (вид техническо разузнаване, но Комсек определено не е противодействие на такова техническо разузнаване, дори коментари, че всъщност COMPINT е конкурентно (не компютърно, а Competitive Intelligence) или икономическо разузнаване не помагат да обвържем двете понятия). Комсек не е и COMPSEC (Computer Security), най-малкото не се свързва с понятие, а по-скоро компания, с централен офис в Нова Зеландия, предлагаща услуги на най-високо ниво в тази област. Друга подобна най-малко по име и достатъчно популярна - Computer Security Solutions, LLC Compsec, но също просто наименование на компания.

4300B.200 Communications Security (COMSEC), Version 3, February 4, 2016 е некласифициран материал, няма никакви ограничения в текстовете си по неговото използване.

Държа и предварително да се извиня на читателите, че въпреки огромното ми старание да изясняват появилите се нови понятия, които понякога дори имат фрагментарно отношение към настоящите текстове, често пъти е невъзможно, не защото не може да се

откриe подходяща информация, а повече защото тази информация е прекалено широка, обилна и просто ще претовари с нови специфични знания и без това достатъчно специфичната материя на тази Инструкция/Регламент/Документ. Също така трябва и да се извиня за някои неясноти, настъпили в следствие на моя превод, които въпреки усилията и опитите да съгласувам по смисъл всички текстове, най-вероятно не съм успял в най-висока степен.

Дори и в по-суров вариант ползата от този превод е огромна за всички ИТ специалисти, служители в мрежи за създаване, съхранение, разпределение и изпращане на информация, за публичния и частен сектор, поради несъмнената си практичност и подробност, която ясно показва модерното схващане за защита на информацията. Възприетият подход чрез този документ, подобно на наръчник, да се обясняват действията подробно и изчерпателно, на най-ниско ниво на ползвателите и потребители на Комсек оборудване, ключове и материали, е доказателство за особеното внимание на САЩ като държава към изграждането на тази политика.

Политиката за комуникационна сигурност (COMSEC) за Министерството на вътрешната сигурност (DHS) се предоставя от този документ и от документи на национално ниво. Когато разпоредбите на този документ противоречат на политиките на национално ниво, ще се прилагат политиките на национално ниво, освен в случаите, когато политиките в този документ са по-строги от националните.

Изложение

1.1 Определение

Комуникационната сигурност (COMSEC) се определя като мерките и контролите, предприети за отказ на информация на неоторизирани лица, получена от телекомуникациите, и за гарантиране на автентичността на такива далекосъобщения. COMSEC включва криптосигурност, сигурност на предаването, сигурност на емисиите и физическа сигурност на материалите на COMSEC.

1.2 Обща политика на COMSEC

Всеки номиниран служител носи пълната отговорност за контрола върху всички материали на COMSEC, съхранявани в акаунта на COMSEC дейността.

1.3 Система за контрол на материалите COMSEC (CMCS)

Материалният контрол на COMSEC в правителството на САЩ се основава на система от централизирано счетоводство и децентрализирана грижа и защита. Използват се компютърни приложения, за да се сведе до минимум ръчното счетоводство и да се осигурят навременни и точни данни, които са от съществено значение за непрекъснатия и ефективен контрол на материалите на COMSEC, поверени или произведени от американската индустрия за правителството.

2.0 ЦЕНТРАЛЕН ОФИС НА ЗАПИСИТЕ (COR - Central Office of Record)

Централният офис на записи (COR) отговаря за поддържането на записи на всички материали за комуникационна сигурност (COMSEC), получени или генерирани от акаунт на DHS COMSEC (вижте единствените две изключения в раздели 2.2 и 2.3 по-долу). В съответствие с Плана за изпълнение на консолидирането на DHS COR от 2012 г., бившите DHS COR и FEMA COR са обединени за създаването на единен COR. В цялата тази публикация DHS COR се нарича COR.

2.1 Отговорности на COR

COR е отговорен за ежедневното управление на COMSEC и отчетността на всички материали на COMSEC, получени в рамките на отдела. Конкретните отговорности включват:

• Създаване и закриване на акаунти на COMSEC

• Поддържане на записи на всички материали на COMSEC, издадени по сметките на COMSEC под негово познаване, и актуализиране на записи чрез провеждане на рутинни одити

• Мониторинг на получаването на транзитен COMSEC материал

• Създаване или одобряване на процедури за отчитане на получаване и предаване на материали на COMSEC

Създаване или одобряване на счетоводни процедури за сметки под негово познаване

• Гарантиране на спазването на изискванията за отчетност на материалите на COMSEC

• Създаване процедури за инвентаризация и одит за сметките на COMSEC

• Увереност, че одитите се провеждат в съответствие с параграф 98 от CNSSI 4005

• Предоставяне инструкции за разпореждане на заместени, излишни и остарели COMSEC материали

• Осигуряване освобождаване от отговорност на ръководителите на акаунти, когато е необходимо

• Удостоверяване назначенията на мениджърите на акаунти на COMSEC и заместник мениджърите на акаунти на COMSEC за всеки акаунт в COMSEC

• Предоставяне криптографски брифинги за достъп на мениджъра на акаунти на COMSEC

• Изпълнение на дейности за наблюдение на инциденти на COMSEC и поддържат запис на инциденти на COMSEC, както се изисква от CNSSI 4003

• Предоставяне обучение и ръководство на COMSEC на мениджърите на акаунти на COMSEC

ЗАБЕЛЕЖКА: COR не носи отговорност за обучението на мениджъри или потребители на COMSEC как да работят с оборудване

2.2 Брегова охрана на САЩ

Програмата COMSEC на бреговата охрана на САЩ продължава да работи съгласно Централният офис на записи (COR) на централния офис на ВМС на САЩ (U.S. Navy’s Central Office of Record) и нейните ръководни директиви. Като единствена военна агенция, пренастроена по DHS, бреговата охрана трябва да поддържа обширен защитен комуникационен интерфейс на DOD и оперативна съвместимост, който се поддържа от съществуваща инфраструктура на Министерството на ВМС (DON) COMSEC.

2.3 Сикрет сървис

Програмата COMSEC на Сикрет сървис на САЩ работи независимо от COR за целите на отчитането. Услугата поддържа собствен административен контрол и бюджет във връзка с COMSEC; COR предоставя само ограничена логистична поддръжка.

(б.а. – Очевидно горните две структури имат собствени правила и не са длъжни да се съобразяват с този документ на министреството на вътрешната сигурност. По друг начин се уреждат и отношенията в МО на САЩ.)

3.0 COMSEC УСЛУГИ

CNSSI № 4009 (Committee on National Security Systems (CNSS) Glossary) определя съоръжението на COMSEC да бъде „Оторизирано и одобрено пространство, използвано за генериране, съхранение, ремонт или използване на COMSEC Материал“.

(б.а. - Речник на комисията по национални системи за сигурност (CNSS) на CNSSI 4009

Тип: Ръководство

Тази инструкция се прилага за всички правителствени управления, агенции, бюра и служби на САЩ; поддържащи изпълнители и агенти; които събират, генерират процес, съхраняват, показват, предават или получават класифицирана или контролирана некласифицирана информация или които работят, използват или се свързват с системите за национална сигурност (NSS), както са дефинирани тук.

За повече информация - посетете уебсайта: https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009)

За целите на настоящата инструкция, съоръжение на COMSEC е:

• Пространство, в която използването на COMSEC материали е основното усилие, което се осъществява в тази област, например в телекомуникационен център.

ЗАБЕЛЕЖКА: Съоръжението на COMSEC може да бъде толкова малко, колкото контейнер или малка стаичка/шкаф (б.а. – поради характера на превода) за сигурност.

• Пространство, в която се произвежда, поддържа или ремонтира класифицирано оборудване на COMSEC (включително предварителен модел, класифицирано COMSEC оборудване).

ЗАБЕЛЕЖКА: Класифицираното оборудване на COMSEC включва и ключово оборудване, върнато за ремонт поради неизправност и невъзможност за нулиране на ключа или класифициран алгоритъм.

• Област, в която са налични незашифровани клавиатурни материали, която изисква сигурно съхранение на такъв ключов материал или устройства за електронно попълване на ключове (напр. Устройство за пренос на данни (DTD- Data Transfer Device), Защитена система DTD2000 (SDS- Secure DTD2000 System), Обикновен ключов товарач (SKL- Simple Key Loader) или Наистина прост Ключов товарач (RASKL- Really Simple Key Loader). Ако са налични само криптирани материали за въвеждане, пространството може да се счита за офисна зона и не е COMSEC.

Съоръжение на COMSEC не е:

• Район, в който се произвежда, поддържа или ремонтира Контролирани криптографски елементи (CCI - Controlled Cryptographic Items) или друго некласифицирано COMSEC оборудване.

ЗАБЕЛЕЖКА: Вграденото CCI оборудване, върнато за ремонт поради неизправност и невъзможност за нулиране на ключа, се класифицира на нивото на ключа или нивото на алгоритъма, както е изложено в оборудването в неговото текущо състояние, което от двете е по-високо и следователно не попада при това изключение за съоръжение COMSEC.

Защитена офисна зона - Защитена офисна зона е мястото, където е достъпно само оборудване COMSEC на ниво потребител за индивидуална употреба. Примерите за офис зона включват, но не се ограничават до зона със защитено терминално оборудване, продукти за Протокол за оперативна съвместимост на сигурни комуникации (SCIP- Secure Communications Interoperability Protocol) или продукти за сигурен глас през интернет (SVOIP - Secure Voice Over Internet Protocol) за индивидуални защитени гласови разговори;

пребиваване със Секретна мрежа за маршрутиране на интернет протокол (SIPRNET - Secret Internet Protocol Router Network) връзка, еднократно TACLANE (TACLANE - най-широко използваното семейство от висококачествени шифровачи тип 1 в света) или устройство за шифроване на протокол с висока сигурност (HAIPE - High Assurance Internet Protocol Encryptor); или набор от кабини в защитена офис среда, всяка кабина със собствено потребителско оборудване COMSEC. Материалите на COMSEC в такива офисни площи трябва да бъдат защитени минимум по начин, който осигурява защитата, която обикновено се предоставя на други високочувствителни / чувствителни материали и гарантира запазването на достъпа и целостта на счетоводството. Ако класифицираната информация е защитена от оборудването на COMSEC в офис зоната, зоната трябва да бъде разрешена за използване или съхранение на класифицирана информация съгласно указания от местната служба за сигурност.

3.1 Обозначение на затворена / ограничена зона

Съоръжение на COMSEC (с изключение на един, състоящ се само от контейнер за сигурност) трябва да бъде обозначено като затворена или ограничена зона. Това обозначение трябва да бъде ясно обозначено чрез знак, поставен от външната страна на вратата, водеща в пространството.

3.2 Списък за достъп

Оторизиран достъп на персонала до съоръжение COMSEC (с изключение на един случай - състоящ се само от защитен контейнер) трябва да бъде вписан в надлежно удостоверен списък за достъп, публикуван вътре в съоръжението на вратата или непосредствено до вратата. Удостоверяването се проверява от подписа на началника на отдел или филиал, служител по сигурността на съоръжението (например SSO), мениджър на акаунти на COMSEC или алтернативен мениджър на акаунти на COMSEC, както е подходящо за дейността. По преценка на упълномощаващото длъжностно лице списъкът за достъп може да прави разграничение между непридружени и придружаващи достъп до съоръжението на COMSEC и да изброява съответно разрешените лица. Лицата, които не са включени в списъка за достъп, могат да получат достъп до съоръжението COMSEC въз основа на валидна нужда да знаете и такъв достъп трябва да бъде записан в регистъра на посетителите (вж. Раздел 3.3 по-долу). Вижте приложение G Tab 5 за примерен списък за достъп.

3.3 Регистър на посетителите

Съоръжение на COMSEC (с изключение на един вид, състоящ се само от контейнер за сигурност) трябва да е поставило във входа регистър на посетителите, в който да се записват пристигането и заминаването на лица, чиито имена не фигурират в списъка за достъп. Регистърът на посетителите трябва да включва следната информация:

Дата и час на пристигане и заминаване;

Печатно име и подпис на посетителя;

Цел на посещение; и

Подпис на упълномощен физически приемник.

НЕ включвайте лична информация в регистъра на посетителите като SSN, дати и места на раждане и т.н.

3.4 Контролен списък за сигурност на активността (SF-701)

В съоръженията на COMSEC (включително тези, които се състоят единствено от контейнер за сигурност), които не са 24-часови съоръжения, лицето, обезопасяващо съоръжението в края на всеки работен ден, трябва да извърши проверки за сигурност и да документира тези проверки на SF-701. Този формуляр трябва да бъде осезаемо поставен от вътрешната страна на вратата на съоръжението. Формулярът трябва да бъде персонализиран за всяко съоръжение въз основа на неговите специфични изисквания, както следва:

• Елементи 1-5 са предварително отпечатани и се прилагат за повечето съоръжения, макар и с датирана терминология. Дейностите могат да се редактират по какъвто и да е начин, който те изберат, или да оставят, както е в разбирането за текущото приложение.

• Във формуляра са посочени допълнителни редове за специфични проблеми. В тези редове трябва да бъдат написани важни елементи за проверка. Примерите включват да се гарантира, че кафемашините са изключени, торбите за изгаряне са правилно закрепени и т.н.

• Факсимилета от формуляра на местно ниво са приемливи, при условие че те адресират основните проверки за сигурност и безопасност, които се прилагат за дейността.

Използването на SF-701 в 24-часови съоръжения не е задължително.

3.5 Проверка на контейнера за сигурност (SF-702)

Всички комбинирани брави в рамките на COMSEC съоръжението (включително бравата, която закрепва вратата към съоръжението COMSEC и тези, които осигуряват всички контейнери за сигурност), трябва да бъдат придружени от контролен лист за контейнери за сигурност (SF-702). В случаите, които включват електромеханично заключване в режим на двойно управление, за всяка комбинация трябва да се публикуват отделни форми SF-702. Този документ трябва да се използва за записване на минимална дата, час и инициали на лицето, което отваря и затваря ключалката всеки път, когато е достъпна. За брави в режим на двойно управление, когато блокировката е затворена, колоната „Проверено от“ на двата формуляра SF-702 трябва да бъде парафирана от втори индивид (НЕ индивидуалното затваряне на ключалката).

4.0 ДОСТЪП ДО МАТЕРИАЛ (ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ ЗА КОМСЕК)

Определена американска класифицирана криптографска информация, загубата на която може да причини сериозни или изключително сериозни щети на националната сигурност на САЩ, изисква специален контрол на достъпа. Съответно достъпът до класифицирана криптографска информация се предоставя само на физическо лице, което отговаря на следните критерии:

• е гражданин на САЩ

• Служител е на правителството на САЩ, е контрактор или служител на контрактор на правителството на САЩ или е назначен като представител на правителството на САЩ, включително консултанти на правителството на САЩ

• Притежава разрешение за сигурност, подходящо за класификацията на материалите на COMSEC, до които може да получи достъп

• притежава валидна необходимост да знае, както е определено необходимо за изпълнение на задължения за или от името на правителството на САЩ

• Получава инструктаж за сигурност, подходящ за материалите на COMSEC, до които се осъществява достъп

• Признава предоставянето на достъп чрез подписване на сертификат за криптографски достъп.

Проверката за сигурността на персонала с акаунт, притежаващ TOP SECRET ключови материали с надпис CRYPTO, трябва да се основава на окончателно проучване на самото физическо лице (SSBI - Single Scope Background Investigation).

Персоналът, на когото е предоставен разрешение TOP SECRET, може да получи достъп до материали на COMSEC, но само на ниво SECRET и по-ниско. Временно разрешение за SECRET не е валидно за достъп до всяка класифицирана информация на COMSEC.

Не е задължително дадено лице да има достъп до ключово оборудване COMSEC, ако е под придружител или ако физическа, техническа или процедурна мярка им пречи да получат знания или да променят информация, материали, ресурси или компоненти.

Когато ръководителите на отдели или агенции контролират лицата директно, може да се изисква достъп до информация за физическо лице, което да признае възможността да бъде подложено на полиграфско изследване за обхват на житейски път и нетипичен жизнен стандарт, за контраразузнавателно проучване, което се извършва в съответствие с директивите на отделите или агенциите и приложимото законодателство.

4.1 Достъп до контролирани криптографски елементи (CCI- Controlled Cryptographic Items)

Достъпът до CCI ще бъде ограничен до гражданите на САЩ, които имат нужда да знаят. Гражданите извън САЩ, включително имигрантите чужденци, могат да получат разрешение за достъп до CCI в съответствие с процедурите, установени в CNSSI 4001.

[Б.а. - Някои пояснения за него:

CNSSI 4001 - Самият документ е обозначен като „FOUO“, т.е. For Official Use Only (само за официално ползване)

Controlled Cryptographic Items (CCI)

Дата на създаване: 05/07/2013, File Size: 413341. Разпорежда дейностите и контрола със CCI. Чрез анекси се описват условията за външен (чуждестранен) достъп до CCI; критерии за подбор/процедури за транспортиране от фирми на CCI (индустриална сигурност и физическа сигурност –специални мерки по нашия ЗЗКИ); изброява изискванията към CCI; модифицирани изисквания за CCI, използвани за поддръжка на мрежови системи за сигурност; дефиниции на специални термини; и списък на документи на национално ниво, приложими към настоящата инструкция.

Документът е обазначен с FOUO. За достъп до защитено FOUO съдържание в библиотеката на CNSS, е необходимо клиентът да се логне чрез един от трите варианта

Federal/DoD Public Key Infrastructure (PKI),

Personal Identity Verification (PIV), или

Common Access Card (CAC), които по своето съдържание са client certificate (индивидуален сертификат за достъп), коректно инсталирани на използвания браузер и да кликне върху "CAC/PKI/PIV Login" бутон отгоре.

FOUO

For Official Use Only (FOUO) е обозначение върху документ, но не е класификация. Използва се от Министерството на отбраната и някои федерални агенции за обозначаване на материал или информация, които въпреки, че не са класифицирани, не са предназначени/пригодени за публично използване. Тази маркировка има връзка с некласифицираната, но чувствителна информация, която попада в категориите извън публична употреба съобразно the Freedom of Information Act. DoD Directive 5400.7 дефинира For Official Use Only информацията като " некласифицирана информация, която може да

бъде освободена от задължително публикуване според the Freedom of Information Act (FOIA)." Тази политика се създава на основата DoD Regulation 5400.7-R and 5200.1-R (регламенти на МО на САЩ)

Всяко държавно министерство или агенция определя каква информация трябва да бъде защитавана и как да се работи с такава информация.

Следната информация се отнася само до информацията на Министерството на отбраната FOUO. Когато лице се занимава с чувствителна, но некласифицирана информация от друг отдел или агенция, се консултира с инициатора относно подходящото боравене.

Разпространение на информация на FOUO

Информацията на FOUO може да бъде разпространявана в рамките на компонентите на DoD и между длъжностните лица на компонентите на DoD и изпълнителите на DoD при необходимост при извършване на официален бизнес/поръчка. Информацията за FOUO може също да бъде предоставена на длъжностни лица в други отдели и агенции на изпълнителната и съдебната власт при изпълнение на законова функция на правителството на САЩ.]

(б.а. – горните пояснение в средни скоби се налагат поради натрупването на множество абревиатури, понятия и терминология. Като цяло с поясненията показваме сложността на цялата система за защита на информацията в САЩ. Тя обаче е водеща система за НАТО и целия свят, поради което не трябва да остава неизяснена. Изключително любопитно е отношението към чувствителната, но некласифицирана информация, която предоставя допълнителни възможности на държавата да защитава ценната си информация от публичен достъп.)

Когато CCI оборудването е включено, лицата, зареждащи ключа или работещи по друг начин с оборудването, трябва да притежават достъп до ниво, поне равен на нивото на класификация на всеки ключ, съдържащ се в него. За визуален достъп не се изисква разрешение за сигурност, ако е придружен правилно от служител (т.е. само за наблюдаване на монитор).

4.2 Криптографски инструктаж за достъп и разглеждане на информация

Криптографските брифинги за достъп са необходими за лица, които имат постоянна нужда от достъп до TOP SECRET и SECRET ключ и автентификатори, които са обозначени CRYPTO, и за класифицирани криптографски носители, които въплъщават, описват или прилагат класифицирана криптографска логика, за да включват, но не се ограничават само до…, ръководства за пълна поддръжка, криптографски описания, чертежи на криптографска логика, спецификации, описващи криптографска логика, и криптографски компютърен софтуер. Следните лица също ще получат кратки брифинги за/преди криптографски достъп:

• Мениджъри на акаунти на COMSEC и алтернативни/зам.- мениджъри на акаунти на COMSEC, притежаващи класификация TOP SECRET и SECRET, маркирани с CRYPTO.

• Криптографски техници за поддръжка или инсталация.

• Персонал, който се нуждае от достъп до пространства, където се генерират или съхраняват криптографски ключови материали.

• Персонал, участващ в операции по въвеждане на ключ.

• Персонал, участващ в унищожаване на криптографски ключове, включително изтриване на ключ от електронни устройства за зареждане.

От лица, на които е предоставен достъп до класифицираната криптографска информация, описана по-горе, може да се изисква да признаят възможността да бъдат

подложени на полиграфско изследване за необичайна жизнена практика, в обхват на контраразузнаването, администрирано в съответствие с изискванията на МО или агенцията и приложимото законодателство.

Криптографски инструктаж за достъп не е необходим за лица, които работят (т.е. не използват или не поддържат) със системи, използващи криптографско оборудване. Брифингът за криптографски достъп се администрира за потребителите от мениджъра на акаунти на COMSEC или, в отсъствие на мениджъра, заместник мениджъра на акаунти на COMSEC. Брифингът за криптографски достъп се администрира към мениджъра на акаунти на COMSEC от COR (Централният офис на записи).

Лицата, които получават инструктаж за криптографски достъп, също изискват криптографски доклад за достъп. Дефинирането се извършва от мениджъра на акаунти на COMSEC или от зам. мениджър за потребители и от COR за акаунта на мениджъра на COMSEC. След приключване на разглеждане се попълва раздел II - Прекратяване на достъпа до класифицирана криптографска информация, SD формуляр 572. (б.а. - SD Form 572 "Cryptographic Access Certification and Termination". Това е законовата форма, създадена от МО на САЩ – 01.06.2000 г. и използвана в цялата страна. Към днешна дата отделът за издаване не предоставя отделни указания за подаване на формуляра.)

5.0 ФИЗИЧЕСКА СИГУРНОСТ НА МАТЕРИАЛА COMSEC (СЪХРАНЕНИЕ НА МАТЕРИАЛИТЕ COMSEC, ФИЗИЧЕСКА СИГУРНОСТ)

Материалът на COMSEC може да изисква различни нива на физическа сигурност при различни условия. TOP SECRET материал е най-чувствителният ключов материал за нашата страна, тъй като се използва за защита на най-чувствителната информация за националната сигурност на САЩ и загубата му от противник ще застраши сигурността на цялата информация, защитена от ключа. Поради тази причина, TOP SECRET ключовите материали трябва да имат специална защита на TPI контролите. Всяко нарушение на изискванията за TPI, посочени тук, се отчита като инцидент в съответствие с раздел 10.1, докладване на инциденти на COMSEC. В този раздел са изложени необходимите физически контроли, свързани с конкретните обстоятелства. Трябва да се спазват указанията, установени в CNSSI 4005, раздел VII.D (Съхранение на COMSEC Материал).

(*Б.а. – TPI - Two Person Integrity*)

5.1 Изисквания за съхранение

Съоръжение / организация няма да може да получава или генерира класифицирана информация на COMSEC, докато не бъде създадено подходящо хранилище. TPI съхранение на ключ TOP SECRET ще изисква акаунти на COMSEC и всички притежатели (потребители на получаване на ръка) да имат възможности за съхранение на TPI, както се изисква по-долу.

5.2 Класифицирано оборудване и информация на COMSEC

Класифицираното оборудване и информация на COMSEC, с изключение на ключовите материали с надпис CRYPTO, трябва да се съхраняват по начин, предписан в CNSSI 4005, подобно на класифицирания материал на същото ниво на класификация. Той също трябва да има сериен номер, за да поддържа непрекъсната отчетност.

5.3 КРИПТО маркиране на материали COMSEC

Съхраняващият се материал с маркировка CRYPTO ще се съхранява в одобрен от Обща администрация услуги (GSA – General Service Administation) контейнер за сигурност

клас V или клас VI, до който имат достъп само администраторът на акаунти на COMSEC и алтернативите. Когато ключът бъде издаден на потребителите, той също ще се съхранява в одобрен от GSA контейнер за сигурност от клас V или VI, до който имат достъп само правилно изчистените и инструкторите за криптографски достъп, и ключът трябва да се описва поне веднъж на ден, ако сейфът се отваря. Освен това, ако клавишният материал е маркиран строго секретно, ще бъдат приложени допълнителни контроли в съответствие с раздел 5.0, съхранение на COMSEC материали и изискванията по-долу.

(б.а. - GSA осигурява работни места чрез изграждане, управление и запазване на държавни сгради и чрез лизинг и управление на търговски недвижими имоти. Решенията за придобиване на GSA предлагат професионални услуги, оборудване, доставки и ИТ на частния сектор, на правителствените организации и военните формирования. GSA също така насърчава най-добрите практики за управление и ефективни правителствени операции чрез разработване на общодържавни политики. През 2019 г. GSA празнува своята 70-годишнина!)

• TOP SECRET ключови материали (включително ключ за криптиране на Top Secret transfer key (TrKEK)) трябва да се съхраняват под TPI контроли, използващи две различни комбинации, като никой не е разрешил достъп до двете комбинации. Материалите с ключов секретен ключ могат да се съхраняват:

o В контейнер за сигурност, одобрен от GSA, с двойни вградени комбинации от заключващи механизми на контролното чекмедже, или единична брава, отговаряща на Федералните спецификации FF-L-2740 на контролното чекмедже, при условие че се използва в режим на двойно комбиниране; или

o В специален контейнер (и) за контрол на достъпа (SACC), който се съхранява в одобрен от GSA контейнер за сигурност; или

o В контейнер за сигурност, одобрен от GSA, в рамките на свод, модулен свод или контролирана / затворена зона. Трябва да се установят процедури, за да се гарантира, че едно физическо лице, което има достъп до комбинацията от контейнери, не е оставено само в свода или контролираната / затворена зона.

• SECRET ключов материал може да се съхранява:

o По начин, одобрен за TOP SECRET ключови материали, обаче, TPI контролите не се изискват; или

o В контейнер за сигурност, одобрен от GSA.

• КОНФИДЕНЦИАЛНИТЕ ключови материали могат да се съхраняват:

o По какъвто и да е начин, одобрен за ключови материали за TOP SECRET или SECRET; или

o във файлов шкаф с интегриран в него механизъм за автоматично заключване и вграден променлив код с три позиции, тип набиране, с променлива комбинация за заключване; или

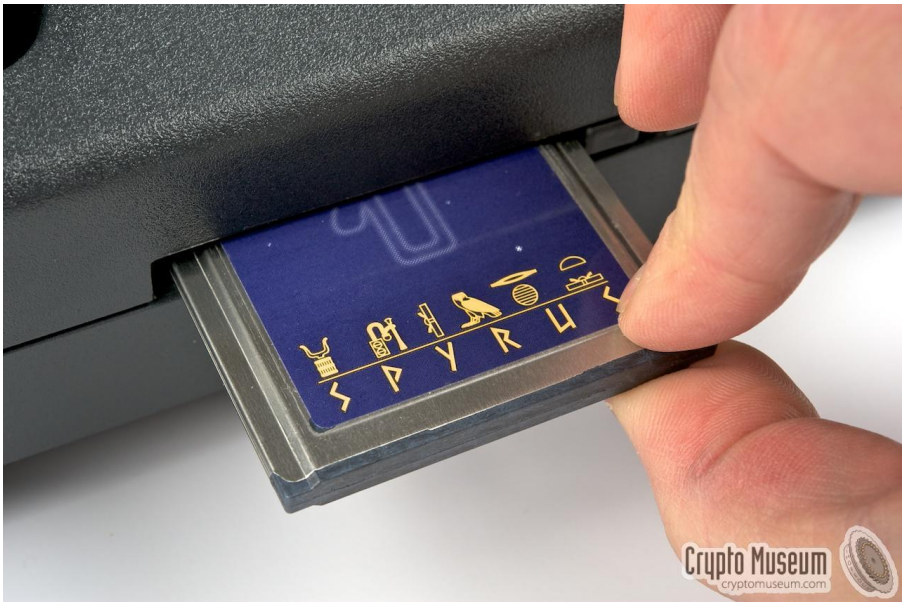
o В стоманен шкаф, снабден със стоманена щанга и код с три три позиции, тип набиране, или катинар със сменяема комбинация.

• НЕКЛАСИФИЦИРАНИ материали за въвеждане (за включване на свързани CIK (Central Index Key), KSV 21 и ключове за шифроване на ключове) могат да се съхраняват по начин, одобрен за TOP SECRET, SECRET или CONFIDENTIAL keying material или по най-сигурния начин, достъпен за потребителя.

ЗАБЕЛЕЖКА: Потребителите трябва да защитават свързана карта CIK или KSV 21, като я съхраняват в лично притежание или я съхраняват по начин, който ще сведе до минимум възможността за загуба, неразрешено използване, подмяна, подправяне или счупване. По принцип потребителят може да изпрати картата CIK или KSV 21 чрез

рентгенови апарати или други устройства за сигурност, които обикновено се използват на летищата без вредни въздействия на картата. KSV 21 „карта за попълване“, програмирана с оперативен ключ, трябва да се борави и съхранява по начин, съответстващ на класификацията на материала за въвеждане.

(б.а. - CIK номер е номер на централен индекс. CIK се използва като уникален идентификатор за документи с Комисията за сигурност и обмен на САЩ. Криптокартата KSV-21 Enhanced е одобрена от американската Агенция за национална сигурност PC карта, която осигурява функции за шифроване от тип 1 и съхранение на ключове за сигурни телефони и други устройства.) Виж изображение за картата[1]:



5.4 Процедури за работа с ключовете за COMSEC

Правилното боравене с ключовете за COMSEC изисква внимателно отношение към детайлите и трябва да се отчита в съответствие с DHS и националната политика от създаването до унищожаването им.

Съхраняваният материал трябва да се поставя в контейнери за сигурност, одобрени от Обща администрация услуги (GSA) за ниво на класификация на ключа. Достъпът до контейнера, съхраняващ бъдещите издания на класифициран ключов материал с надпис CRYPTO, обаче трябва да бъде ограничен до мениджъра на акаунти на COMSEC и алтернативните мениджъри на акаунти на COMSEC. Когато това ограничение не може да бъде приложено, тъй като други лица трябва да имат достъп до контейнера за текущи издания на ключов материал или друг съдържащ се в него материал, бъдещите издания на ключови материали трябва да се съхраняват отделно в заключена твърда кутия, която може да бъде отворена само от мениджъра на акаунти на COMSEC и алтернативен мениджър (и). Силовият модул трябва да се съхранява вътре в контейнера за сигурност.

5.5 Ключови списъци / ключови ленти (записи)

Списъците с оперативни ключове, опаковани в защитни технологии, не трябва да бъдат проверявани в системата до 72 часа преди датата на влизане в сила.

[1] http://www.cryptomuseum.alibaba.sk/crypto/usa/ste/img/301441/036/full.jpg

Ключовите ленти(записи), опаковани в пластмасови защитни кутии, не могат да бъдат изваждани за целите на инвентарни проверки или други. Мениджърът се уверява, че първият сегмент ще се появи в прозореца на защитната кутия. Сегментите не трябва да се изваждат от кутията, докато е необходимо.

При изваждане на този материал за получаване на ръка или при извличане на сегменти от материали, които НЕ са издадени при получаване от ръка, ръководителят на акаунта на COMSEC анотира във формуляра за запис, който му е на разположение - краткото заглавие, издание и регистрационен номер на материала. Всеки извлечен сегмент се проследява на този формуляр по номер на сегмент / копие, както е подходящо, и формулярът трябва да се съхранява заедно с материала до унищожаване.

Етикетите не могат да бъдат залепени върху кутии за ключове с материали или друга защитна технология. Ако е необходимо допълнително идентифициране, може да се използва специален молив с повече мазнини или флумастер, за да се маркира повърхността на кутията или кутията може да бъде поставена в пластмасова торбичка с цип и върху торбата може да се постави етикет. Перманентните маркери не могат да се използват при всякакъв вид защитна опаковка. Етикетите с баркод ще бъдат премахнати при получаването им.

5.6 Достъп до ключови материали, предназначени за шифроване на SCI (SCI – Sensitive Compartmented Information – чувствителна разделена/поделена информация)

Достъпът до ключови материали, използвани за криптиране на SCI, представлява достъп до самия SCI. Материалът за запазване се счита за SCI, когато е изваден от защитната му опаковка или защитната опаковка вече не е непокътната. Достъпът до незашифрован ключов материал, използван за защита на SCI, трябва да бъде ограничен, както следва:

• Съхраняващият материал, предназначен за криптиране на SCI, трябва да се издава и използва само от персонал, индоктриниран за SCI. (б.а. – преводът на термина „индоктриниран е буквален от английския, не намерихме по-добра и точна българска дума)

• Персоналът, който трябва да влезе в съоръжение на SCI (SCIFacility), за да изпълнява задълженията на COMSEC и по този начин да има достъп до (т.е. възможността да чуе или да гледа) SCI, трябва да бъде индоктриниран за SCI. Персоналът, който не е индоктриниран, може да влезе в SCIF, когато е одобрен от съответния орган, ако SCIF е обследван редовно и посетителят остава с придружител - индоктринирано лице, за да се предотврати неволно разкриване.

• Мениджърите на акаунти на COMSEC, одиторите и обучаващият персонал, който борави със защитен пакетиран ключов материал, предназначен за криптиране на SCI, не се изисква да бъдат индоктринирани за SCI. Въпреки това, този персонал трябва да притежава съответното разрешение в съответствие с класификацията на ключа. Персоналът, който извършва унищожаване на SCI материал, който изисква отстраняване на защитната опаковка, трябва да бъде индоктриниран за SCI.

5.7 Заключване на комбинации

Мениджърът на акаунти на COMSEC е отговорен за класифицираните COMSEC материали, съхранявани в защитни контейнери / трезори, които те контролират. Въпреки това, след като класифицираният COMSEC материал е издаден при получаване на ръка на потребителя, потребителят става отговорен за материала, а контейнерът, съхраняващ такъв материал, се счита за пряко контролиран от потребителя. (б.а. – у нас е абсолютно

аналогично по повод на всяка класифицирана информация – всяка каса се зачислява на определено лице и то отговаря за нея)

Комбинациите трябва да се съхраняват в контейнер в организацията на мениджъра на акаунти на COMSEC или в близост до DHS- или друго правителствено съоръжение, където те могат да бъдат достъпни в рамките на 24 часа.

Мениджърът на акаунти на COMSEC е отговорен за управлението на комбинациите от заключване и за обучението на потребителите въз основа на изброените по-долу разпоредби:

5.7.1 Избор на комбинации

Всяко ключалка трябва да има комбинация, съставена от произволно избрани числа. Тази комбинация умишлено не трябва да дублира комбинация, избрана за друго заключване в рамките на съоръжението, и няма да бъде съставена от последователни числа в систематична последователност, нито предвидима последователност (например дата на раждане, социалноосигурителни номера или телефонен номер).

5.7.2 Промяна на комбинации

Комбинацията от ключалки се променя само от надлежно проверено лице, което трябва във връзка със служебни задължения да знае информацията, защитена от ключалката. Освен това комбинациите с контейнери / трезори, използвани от диспечера на акаунти на COMSEC за съхранение на материали, се променят само от мениджъра на акаунти на COMSEC или алтернативния (заместник-) мениджър на акаунти на COMSEC. Притежателят на ръчно получена инструкция/предписание за промяна, персоналът попечител на COMSEC или служителят по сигурността (ако е приложимо) променят комбинации, използвани за защита на материали, издадени по изричното предписание. Комбинационните промени могат да се извършват под наблюдението на обучен ключар, но може да не бъде даван достъп на ключаря (ите).

5.7.3 Честота на комбинационните промени

Комбинациите за заключване се променят при следните събития:

• Когато първоначално се използва брава. (Предварително зададената комбинация от производителя не трябва да се използва.);

• Когато всяко лице, което има разрешение за достъп до комбинация, вече не се нуждае от такива знания (например чрез прехвърляне, прекратяване на работа или загуба на разрешение);

• Когато съществува възможността комбинацията да е била подложена на атака или компрометирана;

• Когато бравата се извади от употреба. Вградените брави трябва да бъдат настроени на стандартната комбинация 50-25-50. Катинарите трябва да бъдат настроени на стандартната комбинация 10-20-30;

• когато са извършени каквито и да е ремонтни дейности по комбинираното заключване; и

• Най-малко веднъж на две години или по-рано, както е продиктувано от горните събития.

5.7.4 Класификация на комбинациите

Комбинациите от брави трябва да бъдат класифицирани като най-високата класификация на информацията, защитавана от ключалките. За контейнер за сигурност това

е най-високата класификация на информацията, съхранявана в контейнера; за вратата на трезора е най-високата класификация на информацията, съхранявана в трезора.

5.7.5 Запис на комбинации

За осигуряване на готов достъп до обезопасен материал в извънредни ситуации, писмен запис на комбинации от брави се поддържа и съхранява в централизиран контейнер, разрешен за съхранение на материал при най-високата класификация на информацията, защитена от бравите. Всяка комбинация трябва да бъде записана на отделна карта за запис (например стандартен формуляр 700) и всяка карта след това да бъде поставена в отделен плик, правилно маркирана и запечатана. Лицето на плика трябва да бъде подпечатано с най-високата класификация на информацията, защитена от комбинацията и пояснено с идентификационния номер на контейнера, за който се прилага. Датата на промяна на комбинацията също ще бъде записана на плика. Когато дадена комбинация е променена, картата за запис трябва да бъде актуализирана и датата на промяната да бъде отбелязана върху плика за запис на комбинация. Пликовете за запис на комбинация трябва да бъдат закрепени в централен контейнер (вижте изискванията за защитена опаковка по-долу), който е одобрен за съхранение на нивото на информацията, защитена от ключалките (с изключение на защитно опакованите пликове за запис на комбинация за TOP SECRET контейнерите не изискват TPI контроли). Ако се поддържа писмен запис на централната комбинация от контейнери, той трябва да бъде опакован, както е описано по-горе, и закрепен в отделен контейнер, одобрен за съхранение на нивото на информацията, защитена от ключалките. В случаите, когато лица, различни от персонала на личния състав на COMSEC или служителя по сигурността (ако е приложимо), имат достъп до централната комбинация от контейнери, комбинацията трябва да бъде опакована защитно, както е описано в параграфа по-долу.

ЗАБЕЛЕЖКА: Записите на комбинации, използвани за защита на COMSEC материали, не могат да се поддържат в електронна форма (например в компютър или на компютърни носители). Освен това е специално забранено за физическите лица да записват и носят или съхраняват несигурно за лично удобство комбинацията до зони или контейнери, в които се съхранява материалът на COMSEC, да включват без надзор или непредвидени съоръжения. Обръщаме внимание на строгостта на разпоредбата, т.като при нас ключове за РАК-шкафове или пароли за достъп се съхраняват най-често в самите помещения и са записани на нерегламентирани карти, бележки, бележници в непосредствена близост до оборудването за което са предназначени и в което се прилагат.

5.7.6.1 Техники за защита на опаковките

Насоките за избор един метод (други методи могат да бъдат еднакво приемливи) за защитна опаковка са следните:

• Картите за запис на комбинации от заключване могат да бъдат опаковани защитно, като се покрива картата за запис (например SF-700 част 2A) отпред и отзад с алуминиево фолио. Поставете картата за запис на комбинация в част 2 или непрозрачен плик. Въведете на част 1 и лицето на плика информацията, посочена в параграф „Запис на комбинациите“ по-горе. Тези записи трябва да бъдат направени с мастило, за да се намали възможността за промяна.

• Поставете плика в найлонов плик, запечатан и запечатайте според инструкциите. Пластмасовите торби, се предлагат от Отдел на защитните технологии на NSA (б.а. – би трябвало да е Агенцията за национална сигурност), I23121, (301) 688-5861 или 688-6816.

5.7.6.2 Периодична проверка на комбинациите

Описаната в този раздел защитна опаковка осигурява допълнителна степен на защита, но не е устойчива при проникване. Следователно пакетът трябва да се проверява ежемесечно и да се води дневник за проверките с отбелязаната дата, номер на контейнера, обобщение на аномалиите (ако има такива; ако няма аномалии, така да е посочено) и инициали на лицето, извършващо проверката. Вижте раздел 4 от приложение Г (Tab 4 to Annex G) за образец на дневника. Тази проверка трябва да включва внимателно визуално изследване на надписите върху лицевата страна на плика, за да се гарантира, че те са автентични, и проверка на всички повърхности на опаковката, очертаващи възможно фалшифициране, включително четирите ръба на опаковката. Това може да разкрие действително опита за проникване през защитната опаковка.

5.8 Внедряване на интегритет с две лица (TPI - Two Person Integrity)

Операциите на TPI с TOP SECRET оперативен ключов материал (TOP SECRET CRYPTO) трябва да се извършват заедно с поне едно лице, което има окончателно разрешение TOP SECRET. Вторият индивид трябва да има поне междинен пропуск ТОП СЕКРЕТЕН с минимален краен секретен достъп. И двамата трябва да бъдат запознати с брифинга за криптографския достъп.

ЗАБЕЛЕЖКА: Докато сте в под опеката на Отдела на куриерите за отбраната (DCD - Defense Courier Division) или на Дипломатическата куриерска служба, не се изискват проверки за почтеност на две лица за ключови материали за TOP SECRET.

Получаване на ключов материал за TOP SECRET - Приемането на пакети от DCS не изисква TPI. Въпреки това, когато отваряте пакет и вътрешната обвивка показва, че е с ниво ТОП СЕКРЕТ, обработката трябва да спре, и TPI незабавно да се приложи, освен както е посочено по-долу:

Ключът TOP SECRET, получен от мениджъра на акаунти на COMSEC от Националния орган за дистрибуция на САЩ (NSA) или друг източник на дистрибуция на отдел или агенция и правилно съхраняван в одобрена от NSA опаковка за защитна технология, не изисква контрол на целостта на две лица (TPI) , при условие че е изпълнена програма за инспекция на защитните технологии съгласно параграф 52 от CNSSI 4005 и персоналът е подходящо обучен.

Преди затворената защитната опаковка, съдържаща ключ TOP SECRET, да бъде отворена в акаунта, и впоследствие да се получи достъп до ключът в него, TPI трябва да бъде изискван и строго приложен от мениджъра на акаунти на COMSEC. Освен това, всички незашифрован ключ TOP SECRET, издаден от акаунта, трябва да бъде под строг TPI контрол.

TOP SECRET COMSEC материалът трябва да се поддържа под TPI контроли. Когато такъв материал се получава на ръка, това става под TPI контроли и да се подписва от две лица.

ЗАБЕЛЕЖКА: Такъв TOP SECRET материал включва COMSEC оборудване, съдържащо ключ TOP SECRET, който може да бъде премахнат или извлечен от оборудването в некриптиран вид, и Top Secret TrKEK.

Когато ключът TOP TOP SECRET бъде изваден или унищожен, двама души трябва да получат ключа, както и посочените свидетелски лица за унищожаване също трябва да са поне двама.

TPI не се прилага в следните ситуации:

• ТОП СЕКРЕТНИ ПРОГРАМИ в производствените мощности.

• Криптологични местоположения (вижте CNSSI 4005, параграф 60.b).

• Тактически ситуации (виж CNSSI 4005, параграфи 60.d и 103.a).

• Seed Key, който се превръща в ключ TOP SECRET (Seed key е НЕКЛАСИФИЦИРАН).

(б.а. - Комитетът по системите за национална сигурност – CNSS - The Committee on National Security Systems, в съответствие с правомощията си по Директива за национална сигурност 42 (Референция a), издава настоящата инструкция - Instruction (CNSSI) No. 4005, Safeguarding Communications Security (COMSEC) F, с наименование „Защита на средствата и материалите за сигурност на комуникациите (COMSEC)“, за да предпише минималните национални изисквания за изграждане, одобрение и сигурност на съоръжения, при които основната цел е генериране, съхраняване, ремонт или използване на комуникационни материали за сигурност (COMSEC). Този CNSSI също така установява минималните национални изисквания за защита и контрол на COMSEC материали. Тези изисквания се прилагат за всички COMSEC материали, контролирани в рамките на системата за контрол на материалите COMSEC (CMCS), независимо къде се използват. Допълнен вариант от 22.08.2011 г. Този документ е НЕКЛАСИФИЦИРАН // ЗА ОФИЦИАЛНА УПОТРЕБА поради компилирането на иначе НЕКЛАСИФИЦИРАНА информация-UNCLASSIFIED//FOR OFFICIAL USE ONLY, на което обръщаме внимание – натрупването и обобщаването на чувствителна информация в него го прави защитен от публичен достъп. В Интернет може да се открие документът, но със заличени множество текстове, вкл. и в самото съдържание на инструкцията, т.е. не става ясно дори какво съдържа)

ЗАБЕЛЕЖКА: Други раздели на настоящата инструкция предоставят допълнителни ограничения за тези ограничения. Вж. CNSSI 4005, параграф 40 относно изискването за зони, които не са изолирани.

5.8.1 TPI хранилище

TPI съхранението изисква използване на две отделни комбинации за достъп, като никой не може да разреши достъп до двете комбинации. Поне една от комбинациите трябва да бъде от „вградена“ брава, като например сейф, одобрен от GSA или защитен контейнер. Съхраняването може да бъде в твърда кутия или допълнителен контейнер в контейнер за сигурност или контейнер за сигурност, одобрен от GSA, който има своята федерална спецификация FF-L-2740A, заключена в TPI, с двоен комбиниран режим. TOP SECRET ключовите материали трябва да се съхраняват в одобрен от GSA контейнер за сигурност.

ЗАБЕЛЕЖКА: ТОП СЕКРЕТНАТА ключова материя, която се съхранява в работната зона за периодична употреба през целия ден, може да се съхранява под една заключваща брава в зона, която не е изолирана. Познаването на комбинацията или достъпа до ключа, използван за закрепване на ключалката, трябва да бъде ограничен до дежурния надзорен орган.

5.8.2 Тактически ситуации

При нормални обстоятелства тактическите ситуации в контекста на TPI не се прилагат за нито един DHS COMSEC акаунт. За всеки отделен случай, ако възникне ситуация, която може да бъде повлияна от изискванията за TPI, свържете се с COR за ръководство.

5.9 Оборудване за CCI (Controlled Cryptographic items)

CCI оборудването никога не трябва да се съхранява в заключено състояние. Преди да поставите CCI оборудване на склад, всички ключови материали трябва да бъдат премахнати, а вътрешните регистри за съхранение на ключове да бъдат нулирани. Когато не се използва, оборудването на CCI трябва да бъде защитено срещу неразрешено

подправяне, отстраняване или кражба по време на съхранение (например, поставено в заключена стая или стая с подходяща алармена система).

5.9.1 Контроли за достъп на CCI

CCI оборудването по дефиниция е некласифицирано, но контролирано. Минималните контроли за оборудването на CCI се предписват при три различни условия; незаключено; заключено с некласифициран ключ; и заключено с класифициран ключ. Разпоредбите се прилагат за оборудване за CCI, инсталирано за оперативна употреба. Цялото оборудване за CCI трябва да бъде защитено по начин, който осигурява достатъчна защита, което да изключва кражба, саботаж, подправяне или неоторизиран достъп и поддържа отчетност за материала, независимо дали е инсталиран или не.

ЗАБЕЛЕЖКА: Няма изисквания за достъп, налаган за външен преглед на оборудването на COMSEC, когато няма възможност за неоторизиран достъп нито до ключа, до оборудването COMSEC, нито до входа и изхода на системата COMSEC.

5.9.2 Оборудване за CCI

Следва да бъдат установени процедури за осигуряване на физически контрол, достатъчен за предотвратяване на неразрешено придвижване на оборудването за CCI или неговите компоненти на CCI. Стаите, съдържащи незаключено оборудване за CCI, трябва да бъдат заключени в края на работния ден.

5.9.2.1 Инсталиран и заключен с некласифициран ключ

Мениджърът на акаунти на COMSEC е отговорен за предотвратяването на достъп от неоторизиран персонал чрез използване на адекватни физически контроли и / или чрез наблюдение на достъпа с упълномощен персонал.

5.9.2.2 Инсталиран и включен с класифициран ключ – С надзор

Оборудването за CCI трябва да бъде под непрекъснат контрол на персонала, който има разрешен достъп, поне равен на нивото на класификация на използвания ключов материал. Съоръженията, съдържащи TOP SECRET ключови материали, трябва да установят подходящи TPI контроли. TPI контролите винаги се прилагат за първоначалните операции по заключване и повторно набиране, които включват TOP SECRET ключ, обозначен CRYPTO.

5.9.2.3 Инсталиран и включен с класифициран ключ - Без надзор

Оборудването за CCI трябва да бъде в контролирана зона, както е описано в раздел 3.0, COMSEC съоръжения.

6.0 COMSEC АКАУНТИ

Акаунтите на COMSEC са създадени за подпомагане на дейности, които са длъжни да държат и / или произвеждат класифицирани материали на COMSEC, подлежащи на отговорност в рамките на CMCS.

6.1 Изискване за акаунт на COMSEC

Всеки компонент или офис на DHS, който изисква работа с материали на COMSEC, трябва да получава такъв материал чрез акаунт на COMSEC. Ако съществуващ акаунт на COMSEC не може да поддържа изискването, ще бъде създаден нов акаунт на COMSEC. Новите акаунти на COMSEC се създават чрез COR. Когато съществуващ акаунт на

COMSEC може адекватно да поддържа изискването за материали на COMSEC, материалът ще бъде предоставен на потребителя на базата на разписка на ръка от съществуващия акаунт.

6.2 Registration with USTRANSCOM J3/Defense Courier Division (DCD)

(*Б.а. - Тази процедура не разглеждаме, т.като препраща към сайт и алгоритъм от действия, но и няма принципно отношение към нашата идея за защита на информацията*.)

6.3 Създаване на акаунт на COMSEC

След получаване и приемане на искането за създаване на акаунт на COMSEC, COR ще препрати всички необходими документи, които трябва да бъдат попълнени от мениджъра на акаунти на COMSEC и заместник мениджъра. Отделът за сигурност ще провери валидността на разрешенията на назначените лица. Всички попълнени документи ще бъдат върнати в COR. След като акаунтът бъде официално установен, COR ще му предостави официално писмо за установяване на акаунт, което трябва да бъде задържано за постоянно във файловете на акаунта. Освен това, COR ще подпомогне/асистира новия акаунт при получаването на необходимите материали на COMSEC и първоначалната доставка на счетоводни форми на COMSEC.

6.3.1 Искане за създаване на COMSEC акаунт

Когато трябва да бъде създаден акаунт на COMSEC, службата, която го изисква, изпраща официално писмено искане, адресирано до COR. Искането трябва да съдържа следната информация:

• Обосновка в подкрепа на създаването на акаунт и списък на материали на COMSEC, които трябва да се съхраняват от акаунта.

• Ако се изисква записващ материал, се изисква валидиране от контролиращия орган (CA).

• Името на офиса и пълен адрес, където се намира акаунтът.

• Най-високо ниво на класификация за сигурност на материалите на COMSEC, което трябва да се съхранява в акаунта на COMSEC.

ЗАБЕЛЕЖКА: Ако трябва да се съхранява криптографски материал на SCI, включете това в заявката.

• Доказателство, че минималните стандарти за физическа сигурност, посочени в CNSSI 4005 за защита на COMSEC материали, могат да бъдат спазени.

• Имената, степените, социалноосигурителните номера (SSN) и удостоверенията за разрешение на лицата, които ще бъдат назначени като мениджър на акаунти на COMSEC и заместник мениджър.

• Условие, че мениджърът на акаунти на COMSEC и заместник мениджърът са граждани на САЩ и притежават окончателно разрешение на правителството на САЩ, равно или по-голямо от нивото на класификация на материала, който трябва да се държи от акаунта.

• Лицето, определено за мениджър на акаунти на COMSEC или алтернативен мениджър, трябва да е завършило успешно курса на DHS COMSEC Account Manager, преди новият акаунт да може да бъде активиран.

• Мениджърът на акаунти COMSEC трябва да получи инструментариум за криптографски достъп от COR и да подпише сертификат за криптографски достъп преди да поеме задълженията на COMSEC.

Времето за установяване на акаунт на COMSEC и потвърждаване на срещи е най-малко 45 дни.

6.3.2 Назначаване на мениджъри на акаунти на COMSEC

След определяне на необходимостта от акаунт на COMSEC, мениджърите на подходящи нива ще номинират експерт пред COR за мениджър на акаунти на COMSEC и поне един заместник за всеки акаунт на COMSEC под тяхна юрисдикция. След проверка на квалификацията, COR ще назначи този персонал. Персоналът, назначен като мениджър на акаунти на COMSEC или операторите на KMI (key management infrastructure) оперативен акаунт (Key management infrastructure Operating Account (KOA), трябва:

• Да бъдете гражданин на САЩ (или родом или натурализиран)

• Притежавате разрешение за сигурност, подходящо за материала, който ще се съхранява в акаунта. Мениджърите на акаунти на COMSEC, които имат достъп до ключови материали за TOP SECRET, трябва да имат разрешение за сигурност въз основа на окончателно предишно разследване, актуално в рамките на пет години.

(б.а. - Бизнес връзка с ключова инфраструктура за управление (KMI), която се установява 1) за управление на набора от потребителски устройства, които са под контрола на конкретна организация на KMI клиенти; и 2) да контролира разпространението на KMI продукти към тези устройства.

Източник (и): CNSSI 4009-2015)

о Само за служители от правителството на САЩ, междинните/вътрешните разрешения могат да бъдат одобрени; Въпреки това, за акаунти, притежаващи TOP SECRET COMSEC материали, междинните разрешения за TOP SECRET могат да бъдат одобрени само ако на физическото лице е предоставено окончателно SECRET разрешение.

о Разрешителните за изпълнители и извън федералното правителство трябва да съответстват на CNSSP № 14

• Да имате федерални правителствени степени най-малко GS-7 или държавен изпълнител на еквивалентно отговорно положение.

• Не сте имали история преди това да сте били освободени от задълженията на мениджъра на акаунти на COMSEC поради причини за небрежност, злоупотреба или неизпълнение на задълженията

• Имате максимална рентабилност (б.а. - достатъчно дълъг професионален път пред себе си) за установяване на приемственост и намаляване на възможността за честа подмяна. Лица с по-малко от шест (6) месеца, останали в настоящата им задача, не се назначават за мениджър на акаунти на COMSEC.

ЗАБЕЛЕЖКА: Нищо в тази инструкция не пречи на мениджъра на акаунти или алтернативен такъв на COMSEC да бъде COMSEC акаунт мениджър или заместник на няколко акаунта. Въпреки това, преди да бъде назначен във втория или следващите акаунти (и), длъжностното лице по назначаването трябва да удостовери на COR, че лицето ще има време да участва в ежедневните операции и да управлява правилно всички акаунти. (б.а. – у нас това не се позволява, поради редица причини, вкл. всички длъжностни лица в защитата на информацията, най-вече поради „необходимост да се знае“)

• Да бъдете упълномощени съгласно условията на договор на правителството на САЩ, ако сте част от изпълнител. Търговските предприемачи могат да назначат изпълнителен персонал, който да изпълнява функцията на мениджъри на акаунти на COMSEC, и заместници, когато са упълномощени да създават и експлоатират акаунт на COMSEC при условията на договор с правителството на САЩ. Изпълнителят трябва да отговаря на всички изисквания за обучение и сигурност на достъп, определени за

правителствените служители на САЩ и трябва да има окончателно разрешение за сигурност преди назначаването съгласно CNSSP № 14

• Да бъдете обучени.

o Всички нови мениджъри на акаунти на COMSEC трябва да присъстват на официално обучение на COMSEC, предоставено от COR преди назначаване или в рамките на две дати за свикване на клас.

o Всички връщащи се мениджъри на акаунти на COMSEC след прекъсване, превишаващо 18 месеца, трябва да посещават официално обучение на COMSEC преди назначаване или в рамките на две дати за свикване на клас за преназначаване.

o Необходимо е официално обучение за EKMS и KMI акаунти за задълженията и отговорностите на мениджъра на акаунти на COMSEC или KOA. В допълнение, такива лица трябва да бъдат официално обучени и сертифицирани в одобрено учебно заведение в експлоатация на използваната сертифицирана и акредитирана автоматизирана система (EKMS или KMI, ако е приложимо) преди започване на задължения.

Отделното лице може да има задачи за обезпечение и на други задължения, но когато се изискват функции на COMSEC и те не оказват неблагоприятно влияние върху изискванията на мисията, тези функции на COMSEC имат предимство пред другите техни задължения.

Номинационните писма и работни листове трябва да бъдат изпращани с помощта на шаблоните, достъпни на уебсайта на COR SharePoint, както е посочено в раздел 2 към приложение G. Освен това, за всяка предложена промяна на съществуващия персонал на акаунта на COMSEC, ново писмо за номинация за целия нов персонал, бъдещи и действащи служители, и работни листове за всеки нов персонал и всяка дължима за актуализация информация за разрешение, трябва да бъдат представени на COR. В случаите, които строго включват отстраняване без замяна на персонала на акаунта на COMSEC, в COR трябва да се изпрати само ново писмо за номинация за целия останал персонал (без работни листове, освен ако не се актуализира информацията за разрешение за всеки персонал).

6.3.3 Временно отсъствие на мениджъра на акаунти на COMSEC

По време на временно отсъствие на мениджъра на акаунти на COMSEC заместникът ще поеме всички задължения. Отсъствието на мениджъра на акаунти на COMSEC за период по-дълъг от 60 дни е продължително отсъствие и трябва да бъде назначен нов мениджър на акаунти на COMSEC. В случай на оперативна необходимост, COR може да представи отказ.

6.4 Закриване на акаунт на COMSEC

Когато необходимостта от акаунт на COMSEC вече не съществува, контролиращото длъжностно лице ще представи меморандум на КОР с искане сметката да бъде закрита. Впоследствие назначенията на мениджъра на акаунти на COMSEC и заместник мениджъра ще бъдат прекратени като такива.

6.4.1 Провеждане на окончателния опис

Съвместно със заявката за закриване на акаунта, мениджърът на акаунти на COMSEC и заместник мениджърът извършват физическа инвентаризация на всички материали на COMSEC, заредени в акаунта, и изпраща отчета за инвентаризацията в COR, като изисква инструкции за разпореждане на материала.

6.4.2 Инструкции за разпореждане

COR ще извърши окончателно съгласуване на собствеността на акаунта и ще предостави на мениджъра на акаунти на COMSEC инструкции за разпореждане за всички

останали материали на COMSEC. Счетоводните записи на COMSEC и файлове, отнасящи се до акаунта на COMSEC, ще бъдат препратени към COR.

6.4.3 Прекратяване поради слабости в управлението на акаунт в COMSEC Акаунти на DHS COMSEC могат да бъдат закрити от DHS CIO, ако два последователни одитни доклада или други констатации от COR показват, че акаунтът е управляван неправилно или представлява възможна заплаха за националната сигурност.

6.4.4 Прекратяване / Доклад за унищожаване
След приключване на необходимите стъпки за закриване на акаунт на COMSEC, акаунтът трябва да представи доклад за прекратяване / разпореждане в COR. Докладът трябва да посочва, че всички материали са били правилно прехвърлени/унищожени в съответствие с инструкциите, получени от COR, и за този акаунт отчетите са актуални и правилни. Докладът трябва също така да включва точки за контакт и текущи телефонни номера на лица, които имат познания за детайлите на закрития/възстановен акаунт (обикновено COMSEC Account Manager / Alternate).

6.5 Отговорности на мениджърите на акаунти на COMSEC и свидетели Мениджърът на акаунти на COMSEC е отговорен за получаването, съхранението, издаването, защитата, отчитането и, когато е необходимо, унищожаването на материали на COMSEC.

Задълженията на COMSEC Account Manager включват следното:

• Осигуряване на всички материали на COMSEC, издадени или генерирани и държани от акаунта на COMSEC да бъдат защитени и контролирани в съответствие с изискванията на настоящата инструкция или предписанията за оперативна сигурност за свързаното оборудване/система COMSEC в организацията.

• Поддържане на файловете на акаунта на COMSEC и подготовка, и подаване на счетоводни отчети в COR при необходимост

• Осигуряването на нови или допълнителни COMSEC материали е правилно реквизирано или генерирано в съответствие с директивите на министерствата или агенциите

• Провеждане или надзор на материалните запаси, изисквани от този документ

• Коригиране на всички недостатъци, свързани с процедури по акаунта

• Гарантирането, че изменения в публикациите на COMSEC се публикуват своевременно и остатъчните (б.а. – временни работни документи или страници) страници в резултат на подмяната на страници се унищожават своевременно и непосредствено

• Осигуряването на всички задължителни изменения на оборудването на COMSEC в акаунта

• Гарантиране, че материалите на COMSEC се издават само на надлежно проучени или упълномощени лица, чиито задължения изискват това, и ги съветват за тяхната отговорност за правилното опазване и контрол на COMSEC материалите.

• Поддържане на записи на всички материали на COMSEC, издадени на потребителите на ръка

• Започване на организационни процедури, гарантиращи, че хората не напускат организацията, без първо да се върнат или унищожат материалите на COMSEC, издадени им на ръка

• Осигуряването на рутинно унищожаване на материали на COMSEC се извършва в съответствие с изискванията на настоящата инструкция и CNSSI № 4004.1, Процедури за защита от унищожаване и аварийни ситуации за COMSEC и класифицирани материали (Препоръка у)

• Осигуряване на стандартни оперативни процедури (SOP), аварийните планове за защита или унищожаване се изготвят в съответствие с изискванията на CNSSI № 4004.1 (Препоръка у), предоставят се на всички притежатели на материали на ръка, и присъстват във всички съоръжения на COMSEC, обслужвани от COMSEC акаунти

• Уверете се, че COMSEC материалите, обработвани в рамките на CMCS, са добре опаковани за транспортиране и всички получени опаковки се изследват за наличие на подправяне. (Всички случаи на подправяне трябва да бъдат докладвани в съответствие с изискванията на CNSSI 4003 (Препоръка k))

• Осигуряването на инспектиране на защитните технологии в съответствие с инструкциите, публикувани от Отдела за защитни технологии на NSA. (Всички случаи на подправяне трябва да бъдат докладвани в съответствие с изискванията на CNSSI 4003 (Препоръка k))

• Осигуряването на получени или прехвърлени от акаунта материали на COMSEC е в съответствие с материали, посочени в придружаващия отчет за прехвърляне

• Осигуряване на докладване на инциденти в COMSEC в съответствие с изискванията на CNSSI 4003 (Препоръка k)

• Уреждане на транспорта и осигуряване на само разрешени средства да се използват за транспортиране на COMSEC материали, в съответствие с раздел XIV на CNSSI 4005, Транспортиране на COMSEC материал

• Гарантиране, че акаунта на COMSEC съдържа само основни материали на COMSEC.

• Обучение на потребители за правилни процедури за защита и контрол на COMSEC материали

ЗАБЕЛЕЖКА: Мениджърът на акаунти на COMSEC е отговорен за обучение на функции за сигурност и и отчетност на получателите на ръка и за обучението на потребителите в работата на достъпното за тях оборудване.

• Работа с потребители на COMSEC, за да се гарантира, че има продължаващо изискване за конкретен ключ, или, ако няма изискване, препоръчва се на контролиращия орган или управляващия орган, акаунтът да бъде ограничен от разпространението на този конкретен ключ

ЗАБЕЛЕЖКА: В този документ позоваванията на контролиращия орган включват ролята на командния орган при използване на актуален ключ.

• Изпълняване ролята на представител на потребителя или продуктов заявител за модерен ключ, както е упълномощен и препоръчан

• Осигуряване правилното прехвърляне на акаунта на новоназначения мениджър на акаунти на COMSEC преди преназначаване, разделяне или оттегляне на изходящия мениджър на акаунти на COMSEC чрез правилно попълване на Промяна на инвентаризационния списък на мениджъра на COMSEC съгласно параграф 97.в от Препоръка dd. Изходящият мениджър на акаунти на COMSEC остава отговорен за всички материали в акаунта на COMSEC до приключване на съгласуването съгласно параграф 97.с.3) от Препоръка dd.

ВНИМАНИЕ: Ръководителите на акаунти на COMSEC, които напускат акаунта си преди да изпълнят съвместна инвентаризация с лицето, назначено да ги замени (вж. параграф 97.в), и след като получат разрешение за освобождаване от COR, подлежат на повикване.

• Свързване с COR за информация за криптографски достъп при назначаване на позицията на COMSEC Account Manager и подписва информацията за криптографски достъп

• На всеки 6 месеца извършва самостоятелна проверка на акаунта, използвайки контролния списък на DHS COMSEC и поддържа копие от самоинспекцията до следващия одит на DHS

• Провеждане на шестмесечната инвентаризация на COMSEC материали съгласно изискванията на COR

• Координира поръчките за оборудване или ключов материал на COMSEC с COR.

• Провежда и документира, изисквано за съответната година запознаване или обучение или извънредно разпоредено по указание на COR.

• Спазва всички COMSEC Консултации, директиви, меморандуми и др., Публикувани от COR и Агенцията по национална сигурност.

• Провежда необходимите проверки на страници в съответствие с CNSSI 4005, параграф 94.e

• При временно отсъствие на персонал на акаунта, всички промени, направени в акаунта на COMSEC, трябва бъдат преразгледани.

• Осигурява всички алтернативни мениджъри на акаунти на COMSEC да бъдат еднакво включени в акаунта.

(Б.а. – ЗЗКИ и ППЗЗКИ също притежават текстове, подобни на горните. Приемаме, че в закона и правилника към него не е възможно да се разпишат подробно, както в тази инструкция задачите на акаунт мениджъра – с общо 31 различни булета и забележки към някои от тях за яснота), но за целта имаме подобна на превежданата американска инструкция - НАРЕДБА за сигурността на комуникационните и информационните системи, приета с ПМС No 28 от 24.02.2020 г., обн., ДВ, бр. 18 от 28.02.2020 г., в сила от 28.02.2020 г. Тук обаче също не виждаме толкова широко и подробно разписване на функции и задачи на отделните органи в системата за защита на информацията в КИС – за пример правим извадка от Наредбата за сигурността на КИС:

„…Чл. 5. Служителят по сигурността на КИС (б.а. – може да бъде всяко лице, не се изисква да е перфектно в областта на информационните технологии):

1. създава необходимата организация и осъществява контрол на сигурността на КИС в организационната единица;

2. координира изготвянето на документите по сигурността на КИС и на изработените на тяхна основа експлоатационни документи по сигурността;

3. съгласува изготвените документи по сигурността на КИС и ги предоставя на служителя по сигурността на информацията;

4. координира обучението по сигурността на КИС;

5. при случаи или съмнения за компрометиране на сигурността на КИС:

а) незабавноуведомява отговорните длъжностни лица по сигурността в ОЕ;

б) предприема действия за ограничаване или предотвратяване на вредите;

в) координира и участва в процеса по установяването и анализирането на обстоятелства, свързани с компрометиране сигурносттана КИС;

г) докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОАС….

Администратор по сигурността на КИС

…. Чл. 7. (1) За всяка КИС със заповед на ръководителя на организационната единица по предложение на ОРЕ съгласувано със служителя по сигурността на информацията се възлагат функции по чл. 9, ал. 1 на администратор по сигурността на КИС

(3) Функции на администратор по сигурността на КИС в случаите по ал. 2 се възлагат със заповед на компетентния орган на държавната власт по предложение на ръководителя на организационната единица, в която ще се изпълняват функциите на администратор по сигурността на КИС, съгласувано с ръководителя на организационната единица, в състава на която е служителят…. (Б.а. - Притеснителна е неопределеността във функциите на практика на най-важното длъжностно лице по сигурността на информчацията в КИС)

…. Чл. 9. (1) Администраторът по сигурността на съответната КИС:

1. участва в изготвянето и актуализирането на процедурите за сигурност на КИС;

2. изготвя експлоатационни документи по сигурността на КИС на базата на утвърдените процедури за сигурност;

3. изпълнява възложените му процедури за сигурност в КИС;

4. периодично информира потребителите по въпросите за сигурността на КИС;

5. предоставя на потребителите достъп до ресурсите на КИС в съответствие с определените им права;

6. осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в КИС, като:

а) следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на КИС;

б) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в КИС;

в) следи за правилното функциониране на механизмитеза сигурност, включително на механизмите за защита на границата;

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата;

д) осигурява резервиране и съхраняване на одитните записи в определените срокове;

7. участва заедно със служителя по сигурността на КИС и с ОРЕ в установяването и анализирането на обстоятелствата, свързани с компрометиране на сигурността на КИС;

8. може да изпълнява функциите на администратор по криптографска сигурност на информацията, ако в КИС се прилагат криптографски методи и средства, одобрени и регистрирани по реда на наредбата по чл. 85 от ЗЗКИ;

9. уведомява служителя по сигурността на КИС за случаи или съмнения за компрометиране на сигурността на КИС;

10. провежда обучение по сигурността наконкретната КИС на администраторите на КИС и потребителите.

(2) Функциите по ал. 1 могат да бъдат разпределени между няколко администратори по сигурността на КИС.

Т.като тази американска инструкция касае „комуникационна сигурност“, то, за да бъдем честни, трябва да споменем и наличието у нас на друга подобна наредба, която има пряко отношение към дейността: НАРЕДБА за криптографската сигурност на класифицираната информация, приета с ПМС No 263 от 11.11.2003 г., обн., ДВ, бр. 102 от 21.11.2003 г., изм., бр. 44 от 9.05.2008 г., доп., бр. 57 от 24.07.2009 г., изм., бр. 5 от 19.01.2010 г., бр. 27 от 5.04.2016 г., в сила от 5.04.2016 г., изм. и доп., бр. 35 от 10.05.2016 г., в сила от 10.05.2016 г. Аналогични са разглежданите органи и длъжностни лица (безспорно достойнство при една национална система). От тях показваме само:

…Чл. 10.(1) Администраторът по криптографската сигурност:

1. организира въвеждането в експлоатация на криптографската мрежа;

2. контролира спазването на правилата за експлоатация на криптографските средства и организационните правила от потребителите на криптографски средства и периодично ги информира за техните задължения във връзка с използването на криптографските средства;

3. осигурява снабдяването с ключови материали, необходими за работа на криптографската мрежа;

4. експлоатира системи за автоматизирано генериране и разпределяне на криптографски ключове при наличие на такива системи;

5. контролира съхраняването, използването и унищожаването на ключовите материали;

6. извършва периодична инвентаризация на използваните в подчинената мукриптографска мрежа криптографски средства и ключови материали, за резултатите от която представя отчет на служителя по криптографската сигурност;

7. извършва проверка за целостта на защитната опаковка на ключовите материали при получаването им, при инвентаризацията им и преди тяхното предаване и/или използване;

8. разработва и предлага на служителя по криптографската сигурност изменения и допълнения на организационните правила;

9. следи за правилното функциониране на криптографските средства и за извършването на регламентираните профилактични дейности и проверки;

10. при установяване на неизправна работа на криптографските средства организира своевременното им изваждане от експлоатация и техния ремонт;

11. регистрира в паспорта на криптографското средство дейностите по т. 9 и 10;

12. участва заедно със служителя по криптографската сигурност в установяването на обстоятелствата, свързани с компрометиране на криптографската сигурност…)

6.5.1 Алтернативен COMSEC Account Manager (заместник-мениджър)

Алтернативният мениджър на акаунти на COMSEC трябва да е запознат с ежедневните операции на акаунта на COMSEC и трябва да може да изпълнява всички необходими задължения при всяко отсъствие на мениджъра на акаунта на COMSEC. Поне един заместник-мениджър на акаунти на COMSEC трябва бъде назначен за всеки акаунт на COMSEC. При необходимост могат да бъдат назначени допълнителни заместници, за да се поддържа непрекъснатостта на операциите, подлежащи на одобрение на COR (напр. при многосменен режим на работа).

• Алтернативен мениджър на акаунти в COMSEC трябва да отговаря на същите изисквания за гражданство и разрешение за сигурност като този на мениджъра на акаунти на COMSEC. Персоналът, назначен като заместник-мениджъри на акаунти на COMSEC, трябва да има опит в областта на COMSEC и трябва да притежава най-малко GS-5 свидетелство или държавен изпълнител на еквивалентна длъжност като отговорност.

• Всички заместник мениджъри на акаунти на COMSEC трябва да бъдат официално обучени за своите задължения и отговорности.

6.5.2 Проверен (със сертификат) свидетел

Въпреки че политиката позволява използването на надлежно проверени свидетели при работата на акаунти на COMSEC, те не трябва да се считат като заместители на заместник-мениджъри на акаунти на COMSEC. COR реши, че на Свидетелите НЯМА да бъде разрешен достъп до CARDS.

В ISOLATED случаи, свързани с недостиг на правилно определен персонал на акаунта на COMSEC (т.е., мениджър на акаунти на COMSEC и алтернативни), надлежно проверените и криптографски брифирани лица могат да бъдат използвани за завършване на

критични спешни функции на COMSEC акаунта, като разрушения, инвентаризации и т.н. в такива случаи акаунтът трябва да извърши транзакцията и да изпрати попълнения COMSEC материал счетоводен отчет (SF-153), подписан правилно от мениджъра или заместник и свидетел, на COR (факс, сканиране и имейл и т.н.), по това време COR ще прегледа отчета и ще финализира транзакцията в CARDS от името на акаунта. Такива случаи трябва да бъдат координирани с COR.

Ако оперативните нужди (темп, време за извършване) и разписанията на персонала на акаунта представят многократна необходимост от персонал, който не е COMSEC, да служи като Свидетели, които дават възможност за непрекъснато изпълнение на функциите на акаунта, трябва да се обмисли назначаването на допълнителни заместник-мениджъри на акаунти на COMSEC, които ще бъдат задължени да присъстват на DHS COMSEC Account Manager курс на обучение.

Когато използват разрешени свидетели за извършване на транзакции по сметка на COMSEC, те трябва да станат свидетели на транзакцията (физическа инвентаризация, унищожаване и т.н.) на материали на COMSEC. Отговорностите на свидетеля включват, но не се ограничават до следното:

• Подписване отчета за инвентаризацията, записа за използване / разпореждане на ключови материали или доклад за унищожаване, потвърждаващ, че изброените материали на COMSEC са инвентаризирани или унищожени.

• При никакви обстоятелства свидетелят не подписва опис, без лично да е видял материала, който е инвентаризиран, нито да подписва протокол за унищожаване, без лично да е бил свидетел на унищожаването на материала.

6.6 Субакаунти на COMSEC

За по-нататъшно оптимизиране на операциите между определени акаунти на COMSEC, които се координират с по-голям, по-добре зает персонал, в групата могат да бъдат създадени субакаунти (б.а. - помощни, подакаунти или вторични акаунти) вместо пълни акаунти. Критериите включват, но не се ограничават до географска близост или функционална връзка. Създаването на субакаунти под същински акаунт непременно ще носи по-голяма отговорност на мениджъра на акаунти на COMSEC на този същински (б.а. - постоянен, на висше/старше ниво) акаунт.

Субакаунтите функционират по същество като пълни акаунти на COMSEC, но не са присвоени NSA разпознати шестцифрени номера на акаунти. Те работят под егидата на старшия акаунт и директно взаимодействат само с този акаунт. Изискванията за създаване на субакаунти и възлагане на персонала на COMSEC към субакаунти са идентични на тези за същинските/старши акаунти на COMSEC. Персоналът на COMSEC е предмет на същите квалификационни изисквания като старшите акаунти на COMSEC, включително COMSEC обучение в курс на обучение на DHS COMSEC Account Manager. Субакаунтите могат да използват разрешени Свидетели, както е необходимо по същия начин, както е посочено в раздел 6.5.2.

6.6.1 Задължения на мениджъра на старшия акаунт COMSEC

Мениджърът на акаунти в COMSEC осъществява първичен надзор на субакаунти. Този надзор включва следните отговорности:

• Осигуряване на полугодишни самопроверки и инвентаризации на материалите на COMSEC, поддържани от субакаунта

• Провеждане на одити на субакаунта на непериодична основа, базирана на определени събития и явления (напр. нови технологии или изменения на правила), на интервали, които не надвишават на всеки 36 месеца.

• Предоставяне на COMSEC материали според изискванията.

6.6.2 Отговорности на COMSEC персонала на субакаунт

Персоналът на субакаунта се определя по същия начин, както за старшите акаунти на COMSEC. Всеки субакаунт трябва да има мениджър на акаунти на COMSEC и поне един заместник. Отговорностите са същите като за старшите акаунт на COMSEC.

6.6.3 Процес на управление на материалите на COMSEC за субакаунти

Субакаунти ще придобият всички свои COMSEC материали изключително от съответните си старши акаунти. Съхраняването на материални поръчки, реквизити за криптографско оборудване и др. се координира чрез старшия акаунт, който от своя страна ще обработва ключови поръчки и реквизити.

Счетоводните отчети между старши акаунт и субакаунт ще включват уникална последователност от номера на транзакциите. Тези транзакции не се отчитат пред COR.

6.6.3.1 Физически материал

Физическите материали на COMSEC от външни (национални) акаунти, предназначени за субакаунта, трябва да бъдат прехвърлени в старшия акаунт, който от своя страна ще прехвърли материала в субакаунта. Няма изключения от тази политика.

6.6.3.2 Електронен ключ

Субакаунтите ще изпращат поръчки за ключ към старшия акаунт, който ще препраща към COR за поръчка от Службата за криптографски услуги за сигурност (CAO - Cryptographic Assurance Operations (Office)). След получаване от офиса на CAO, COR ще качи ключа в системата за счетоводство, отчитане и разпространение на COMSEC (CARDS) за прехвърляне към старшия COMSEC акаунт, който трябва да обработи и потвърди този превод. Старшият акаунт от своя страна ще прехвърли ключа към субакаунта в CARDS, като по този начин ще предостави ключ на субакаунта за изтегляне (виж Таблица 2 към Приложение D).

7.0 Отчетност на COMSEC материалите

Одобрените от HCA електронни отчетни системи се използват от мениджъра на акаунти на COMSEC за поддържане на записи за разпореждане и поддържане на изискванията за отчитане на материали от всички класове.

След предаване на какъвто и да е материал на COMSEC към акаунт, подписана разписка трябва да бъде изпратена на подателя (и COR, ако е приложимо) не по-късно от три работни дни след получаването.

7.1 Отчетни системи за COMSEC

Отчетността за материалите и оборудването на COMSEC е от съществено значение за сигурността на програмата DHS COMSEC. COR има няколко одобрени системи за отчитане на материали и оборудване на COMSEC. Две от тези системи са дистрибутирана отчетна система INFOSEC (DIAS -Distributed INFOSEC Accounting System) и система за счетоводство, отчитане и дистрибуция на COMSEC (CARDS - COMSEC Accounting, Reporting, and Distribution System). DIAS или CARDS се предоставят безплатно на акаунти

на COMSEC и използването им ще позволи на мениджърите на акаунти на COMSEC да предоставят отчети в електронен формат на други акаунти на COMSEC. Вижте приложение D за подробна информация.

7.2 Електронни записи

Електронните записи са уязвими към загуба или унищожаване; следователно е необходимо да се поддържат хартиени копия на всички транзакции на COMSEC минимум три години. Мениджърите трябва също да архивират своите електронни данни на всеки 30 дни или по-често, ако е настъпил голям обем транзакции (ако се използва DIAS).

7.3 Кодове за легендиране на отчетността (ALC - Accountability Legend Codes)

Отчетният материал на COMSEC в рамките на системата за контрол на материалите COMSEC (CMCS) е присвоен код на отчетно легендиране (ALC), за да посочи минималните счетоводни контроли, необходими за този материал.

• ALC 1, 2 и 4 са присвоени на материали, които трябва да бъдат физически инвентаризирани от COMSEC Account Manager.

• ALC 6 и 7 са присвоени на материали в електронна форма, които не могат да бъдат физически инвентаризирани, но трябва да бъдат инвентаризирани по електронен път.

• Министерствата и агенциите не могат да пренасочват материали на друг ALC без предварително одобрение от NSA, освен когато такова преназначаване е присъща част от процеса на разпространение на електронни ключове, извършен от EKMS или KMI.

ЗАБЕЛЕЖКА: За допълнителна информация относно ALC, включително правилното отчитане на ключ 0, вижте Препоръка (dd), параграф 81.

7.4 Файлове и отчети на COMSEC

Всеки мениджър на акаунти на COMSEC ще създаде и поддържа COMSEC отчетност и свързани с него файлове. Акаунтите, използващи одобрени електронни отчетни програми, не трябва да водят дневник на транзакции на хартия и могат да използват електронния дневник.

7.4.1 Отчетни записи

Отчетните записи се изготвят на SF-153 и се използват за записване на прехвърляне, притежание, опис и унищожаване на COMSEC материали. Следните отчети ще бъдат подготвени по електронен път, като се използва одобрен от DHS материал за счетоводен COMSEC софтуер:

• Отчет за прехвърляне. Използва се за отчитане на прехвърляне на материали на COMSEC от един акаунт на COMSEC в друг.

• Доклад за унищожаване. Използва се за съобщаване за физическо унищожаване на COMSEC материал или за нулиране на електронния ключ.

• Доклад за инвентаризацията. Използва се за отчитане на физическия (зрителен) и / или виртуален опис/инвентаризация на COMSEC материали.

• Доклад за притежание. Използва се за съобщаване за притежанието на COMSEC материали.

• Получаване на ръка. Използва се за документиране на издаването на COMSEC материали на оторизирани потребители за оперативна употреба.

7.4.2 Притежаване / освобождаване от доклади за отчетност

Всеки път, когато COMSEC материалът бъде открит извън системата на отчетността или е просто изгубен, се изисква доклад за инцидентите на COMSEC, последван в повечето случаи от доклад за притежание или облекчение на отчетността, според случая. Докладът за притежание или освобождаване от отговорност трябва да бъде придружен от номер на дело, издаден от Националната система за докладване на инциденти на COMSEC (NCIRS - National COMSEC Incident Reporting System) (освен както е посочено по-долу).

7.4.2.1 Притежаване

Когато материалът на COMSEC е открит извън отчетността, независимо дали материалът е обезопасен или не в рамките на съоръжението COMSEC или друго сигурно пространство, трябва да се докладва инцидент COMSEC в съответствие с раздел 10.1, докладване на инциденти в COMSEC. CIMA ще проведе разследване в координация с НСА и ще се опита да определи дали материалът отговаря на който и да е акаунт на COMSEC. В случай, че отчетността за материалите не може да бъде определена, CIMA ще инструктира отчитащият се акаунт да попълни отчет за притежание. Докладът за притежание не се попълва преди това определяне и инструктиране.

В случай, че материал (т.е. CCI) е получен от други агенции, които не отчитат този материал в своите CMCS, не се изисква доклад за инцидентите на COMSEC, въпреки това трябва да бъде попълнен доклад за притежание. В този случай не се изисква инструкция от CIMA за попълване на отчет за притежание.

7.4.2.2 Освобождаване от отчетност

В случай на загуба на материал на COMSEC, трябва да се докладва за инцидент COMSEC в съответствие с раздел 10.1, докладващ инциденти на COMSEC. Субектът на откритието трябва да оцени инцидента и да възложи на акаунта на COMSEC да попълни отчет за освобождаване от отговорност, за да премахне материала от списъка на акаунта.

7.4.3 Отчетност на COMSEC и свързаните файлове

Всеки мениджър на акаунти на COMSEC трябва да създаде и поддържа подходящи файлове, съдържащи следните отчети на COMSEC:

• Доклади за входящи / изходящи трансфери, доклади за притежание и промяна на отчетите за инвентара на COMSEC Account Manager

• Доклади за унищожаване

• Доклади за инвентаризация

• Разписки за получаване на ръка

• Дневник на транзакционните номера. (Ако се използва одобрен от DHS автоматизиран регистър файл, не се изисква физически дневник на транзакциите.)

В допълнение към счетоводните файлове на COMSEC, мениджърът на акаунти на COMSEC ще съхранява следните свързани с COMSEC файлове:

• Съобщения за състоянието, получени от всеки контролен орган за въвеждане на материал

• Куриерски, пощенски и пакетни разписки

• Документи за назначаване на мениджъра и заместника му:

o Писма за номинации и назначения

o Сертификати за криптографски брифинг

o Карта за личен подпис (DHS формуляр 580)

o Годишно четене на COMSEC препоръки и задължения.

• Копия на куриерски писма или куриерски карти за целия персонал на акаунта на COMSEC
• Писмо за установяване на акаунт
• Писмо за акредитация на COMSEC
• Кореспонденция, отнасяща се до акаунта
• Доклади за инциденти на COMSEC
• Одитни доклади
• Меморандуми за коригиращи действия
• Телефонни номера на всички издадени защитени телефони
• ПИН кодове на производителя и потребителя за сигурни мобилни телефони, безжични терминали и телефони Iridium, поддържани от мениджъра и съхранявани на подходящо ниво на класификация

7.4.3.1 Класификация на отчети и досиета на COMSEC

Класификацията на акаунтовите отчети и файлове на COMSEC е отговорност на мениджъра на акаунти. COMSEC счетоводните отчети и файлове обикновено са некласифицирани // Само за официална употреба (Unclassified//For Official Use Only) и се маркират в съответствие с указанията на NSA. Когато е включена класифицирана информация, файлът ТРЯБВА да бъде маркиран според най-високото ниво на класификация, съдържащо се във файла.

7.4.3.2 Маркиране на счетоводните отчети и досиета на COMSEC

Всеки файл или доклад на COMSEC, който съдържа класифицирана информация, освен класификацията, ще съдържа и следното изявление:

Класифицирано от: [Име на мениджъра на COMSEC]

Получава се от: NSA / CSSM 1-52 Датиран на 30 септември 2013 г.

Декласифициране на: [25 години от датата на документа]

COMSEC файлове или доклади, които съдържат НЕКЛАСИФИИРАН // FOUO, се маркират и контролират по същия начин като отговарящата/съответната информация.

7.4.3.3 Период на задържане на COMSEC файлове и свързани документи

Всички COMSEC файлове и свързани документи ще се съхраняват за период от три години със следните изключения:

• 90 дни:
o SF-701
o SF-702

(б.а. - SECURITY CONTAINER CHECK SHEET или листове за проверка на контейнери за сигурност. SF 701, „Списък за сигурност на дейността“, се използва за записване на такива проверки. Неразделна част от системата за проверка на сигурността е обезопасяването на всички сводове, сигурни помещения и контейнери, използвани за съхранение на класифициран материал. SF 702 е форма, състояща се от две колони на листа, които могат да бъдат сгънати наполовина. Същата информация се събира и на двете половини на листа. Има място за събиране на информация за датата, часа и инициалите на всеки, който е отворил, затворил или проверил защитния контейнер.)

• 2 години:
o Регистър на посетителите
• 5 години:
o Доклади за инциденти на COMSEC и свързани документи
• Постоянен срок:

o Писмо за установяване на акаунта

o Сертифициране за физическа сигурност

ЗАБЕЛЕЖКА: Трябва да се сертифицира отново при физически промени в стаята или съоръжението.

7.5 Получаване на COMSEC Материал

Материалите на COMSEC могат да се получават от различни източници чрез препоръчана поща или куриерски услуги.

Мениджърът на акаунти на COMSEC ще предостави процедурите за обработка на поща, необходими за материалите на COMSEC, получени в акаунта. Служителите за обработка на поща се уведомяват, че пакетите, адресирани до мениджъра на COMSEC, трябва да му бъдат доставени неотворени.

Fbricj за доставка на DHS може да отвори външната опаковка. Всяка пратка ще съдържа отчет за прехвърляне на SF-153 на съдържанието на пакета. Мениджърите трябва да проверят съдържанието на пакета спрямо предоставения SF-153. Всички несъответствия трябва да бъдат докладвани на подателя и на COR.

7.5.1 USTRANSCOM / J3 (DCD) IMT 10 Запис на отчет на куриер от службата за куриерски услуги на MO (DCD – Defence Courier Division)

DCD изисква от персонала си, който въвежда пратки в или приема пратки от DCD, да попълва USTRANSCOM IMT 10 Defense Courier Account Record, преди да въведе или да получи материали.

ЗАБЕЛЕЖКА: Допълнителна информация за DCD може да бъде намерена на: www.transcom.mil/dcd.

7.5.2 Преглед на пакетите

След получаване на COMSEC материали, опаковките ще бъдат изследвани за доказателства за подправяне или излагане на съдържанието. Ако едно от тях е очевидно и съдържанието е класифицирано или маркирано CCI или CRYPTO, доклад за инцидент ще бъде представен в съответствие с раздел 10.1, докладване на инциденти на COMSEC. Пакетите, показващи доказателства за подправяне, не трябва да се отварят, докато не бъдат получени допълнителни инструкции от COR, или Отдела за защита на технологиите на NSA (I23121), Tamper Solutions and Inspections.

Ако пакетът съдържа TOP SECRET ключови материали, получаващият COMSEC акаунт мениджър трябва незабавно да инициира TPI контролите. И двамата участници в TPI трябва внимателно да проверят защитната опаковка за наличие на повреди или подправяне и да поставят TOP SECRET ключа в TPI съхранение.

Когато пакетите бъдат отворени, етикетите на материалите COMSEC ще бъдат инвентаризирани спрямо приложения отчет за прехвърляне на SF-153. Всяко разминаване в кратко заглавие, сериен номер или количество ще бъде докладвано на изпращача и на COR. Коригираните копия на отчета за прехвърляне SF-153 трябва да бъдат генерирани от доставчика на пратката и да се препратят към COR и приемащата сметка с подходящи забележки, идентифициращи корекции. Ако материалът е класифициран и несъответствието не може да бъде разрешено между изпращача и получателя, инцидентът COMSEC ще бъде подаден от предвидения получател.

След проверка на COMSEC материалите, докладът за прехвърляне ще бъде подписан и разпространен, както следва:

• Върнете оригинала на акаунта на доставката

• Едно копие в COR (качване в CARDS)
• Запазете едно копие от файла.

7.5.3 Препоръки за оборудването

Оборудване, получено в запечатани картонени опаковки, които не са отворени или не показват признаци на подправяне, може да бъде получено без физическо преглеждане на материала от вътрешната страна, стига етикетът върху картонената опаковка да е съгласен с доклада за трансфер (това е решение на мениджърът на акаунта на COMSEC дали да се отворят или не тези картонени кутии). Ако има несъответствия, съдържанието трябва да бъде физически описано.

7.5.4 Проверка на страници

COMSEC материалите ще бъдат проверени в съответствие с инструкциите за работа. Потребителите се насърчават периодично да гарантират, че страниците на техническите наръчници са непокътнати. Следните проверки на страниците се извършват:

• Когато материалите на COMSEC са получени в акаунта на COMSEC;

ЗАБЕЛЕЖКА: Ако са получени множество копия на документ, мениджърът на акаунти на COMSEC може да избере да отложи проверката на страниците и да я завърши по-късно съвместно с притежателя на разписката при издаване на документа.

• При връщане от получаване на ръка;
• След публикуване на изменение;
• При промяна на мениджъра на акаунти на COMSEC;
• Преди прехвърляне или унищожаване; и
• Всяка изминала година след проверка от последната дата, ако не се прилагат други изисквания.

Запечатаният физически материал COMSEC не може да се отваря до момента на готовност за употреба. Запечатаният физически COMSEC материал не се проверява по страници, ако уплътнението или печата са счупени.

7.5.5 Ключове

Определени артикули от COMSEC материали са опаковани предпазно към момента на производство и в повечето случаи няма да бъдат отваряни, докато не бъдат използвани от реалния потребител. За да се гарантира целостта на ключа, ще бъде завършена проверка на всички внедрени защитни технологии при първоначално получаване, по време на инвентаризацията и преди всяка употреба. Защитните опаковки, приложени към отделни артикули от ключа TOP SECRET, не трябва да се премахват, освен при TPI условия. Специфичните процедури за инвентаризация на защитно опакованите материали са изложени по-долу:

• Вграденият материал, който се доставя в запечатани прозрачни пластмасови опаковки, няма да бъде отворен до 72 часа преди проверката на инвентара / страница. Следователно проверка на страница при получаване на материала не е разрешена. Материалът за изпитване не се отваря, докато не бъде използван. Описът при получаване ще бъде с кратко заглавие, издание и номер на регистъра. Когато защитната опаковка се отстрани от ключовия материал при подготовката за използването на материала, по това време ще се извърши проверка на страниците.

• Ключовите записи в предпазните кутии се описват при получаването им, като се отбележи краткото заглавие, издание и регистър номер на предния ръб на сегмента на лентата, който се появява в прозореца на пластмасовия контейнер. Ключовите ленти/записи

няма да бъдат премахнати от кутиите за целите на инвентара или проверката на страниците. Лентата/записът ще бъде премахната само от потребителите на материал на датата на влизане в сила. Ключовата лента може да бъде премахната и поставена на електронно устройство за ползване до 30 дни наведнъж. Когато се зареждат в електронно устройство, сегментите и лентата за ключове, извлечени от предпазната кутия, трябва да бъдат осигурени до нивото на класификация на ключа, докато сегментът или предпазната кутия не бъдат заменени, по това време те ще бъдат унищожени и унищожаването на ключова лента ще бъде записана в доклад за унищожаване.

ЗАБЕЛЕЖКА: Зареждането от 30 дни наведнъж в електронното устройство за работа е разрешено с разбирането, че контролиращият орган (CA) приема риска да замени цялото издание на ключа, ако възникне компрометиращо събитие.

• Етикетите с баркод, приложени към касетите с ключови ленти, не са класифицирани. След като бъде получена кутия, етикетът с баркода трябва да бъде премахнат преди употреба. Областта под отстранения етикет трябва да бъде проверена за наличие на подправки. Отстраненият етикет трябва да бъде приложен върху лист обикновена хартия и унищожен по одобрен метод.

Всеки мениджър на акаунти на COMSEC е отговорен за поддържането на информация за състоянието (влизане в употреба и датите за сесия) за всички ключови материали в акаунта си. Тази информация е достъпна от контролиращия орган (CA) на ключовия материал, а не от COR.

7.6 Прехвърляне на COMSEC материал

Мениджърът, изпращащ материала на COMSEC, трябва да потвърди официалния адрес на получаващата агенция, номера на акаунта на COMSEC и разрешението да държи материала, който се изпраща. Когато валидността на адреса за доставка или органа за доставка е под въпрос, мениджърът на акаунти на COMSEC трябва да се свърже с COR преди да извърши пратката. Материалът на COMSEC, независимо от присвоен код на легенда на акаунта, няма да бъде доставен, освен ако не бъде предоставен номер на акаунт на COMSEC с адрес за доставка. Съхраняващите материали няма да бъдат прехвърляни между акаунти на COMSEC без одобрението на контролния орган (CA). Освен това, мениджърът на доставките отговаря за проверката на страницата или инвентаризацията на материалите на COMSEC преди доставката, правилното опаковане на материала и гарантира, че класифицираният COMSEC материал се доставя само от разрешени видове транспорт. Той трябва да гарантира, че всички материали на COMSEC, доставени извън съоръжение на COMSEC, са опаковани и изпратени в съответствие с раздел XIV от Препоръка dd.

7.6.1 Разрешени видове транспорт

В тази инструкция се използва терминът (или вариант на термина) „транспорт“, когато не се прави разлика по отношение на метода на транспортиране. „Изпращане“ се използва за обозначаване на метод на транспортиране, който не позволява лично пазене или контрол на материала по време на транзит. „Куриерът“ и „пренасянето“ се използват взаимозаменяемо, за да означават метод на транспортиране, позволяващ лична охрана или контрол на материалите, докато са в транзит (напр. DCD, куриерска служба на Държавния департамент, пощенска служба на САЩ, служба за защита на сигурността (виж параграф 130.b) .3 от Препоръка dd)).

7.6.2 Подготовка за транспорт

Всички материали за физическо набиране и други класифицирани физически COMSEC материали трябва да бъдат двойно опаковани или поставени по друг начин в два непрозрачни контейнера и сигурно запечатани преди транспортиране. Материалът, използван за опаковане, трябва да е достатъчно здрав и устойчив, за да осигури защита по време на транзитиране, предотвратяване на пробив на контейнери и улесняване откриване на всяко подправяне на контейнера. Външната обвивка не трябва да съдържа никакви индикации, че опаковката съдържа класифициран материал или материал за въвеждане.

ЗАБЕЛЕЖКА: Явната лента за вътрешната обвивка е достъпна (безплатно в разумни количества) от клона на защитните технологии на NSA, (301) 688-5861 или 688-6816.

Некласифициран COMSEC материал, различен от ключ, трябва да бъде добре опакован, за да открие подправяне или проникване и предпазване от повреди. За CCI се обърнете към CNSSI № 4001 (Препоръка h) и правилата на отдела или агенцията.

Когато се носи материал, куфарче, чанта или кутия е подходяща външна обвивка.

Ако класифицираният материал е вътрешно поставен като част от оборудването, обвивката или тялото на оборудването може да се считат за вътрешна обвивка. Специализираните контейнери за превоз на оборудване могат да се считат за външната обвивка или капак; въпреки това, всяка класификация или маркировка COMSEC трябва да бъдат залепени с лента (б.а. – очевидно прикрити).

7.6.3 Транспортиране на ключов материал

Материалът за оперативни ключове не трябва да бъде превозван в един и същ контейнер със свързаното с него оборудване, освен ако физическата конфигурация на оборудването прави невъзможно отделянето на ключовия материал; въпреки това некласифициран ключ за поддръжка може да бъде доставен в същия контейнер като свързаното оборудване. Неясните и несигурни услуги на непроучени търговски куриери няма да се използват за изпращане на класифициран ключов материал с надпис CRYPTO.

7.6.3.1 Строго секретно и секретно

Всички материали за ключови ключове TOP SECRET и SECRET трябва да бъдат транспортирани по един от следните методи:

• USTRANSCOM / J3 (DCD);

• Куриерска служба на Държавния департамент;

• Официално определени и надлежно проучени куриери на отдели, агенции или изпълнители.

ЗАБЕЛЕЖКА: Всеки път, когато местни/собствени куриери транспортират TOP SECRET ключови материали от един акаунт на COMSEC до друг или до местоположението на притежателя на ръка, TPI контролите се прилагат в съответствие с Препоръка dd, раздел VII.C, Прилагане на контрол от две лица (TPI).

7.6.3.2 ПОВЕРИТЕЛНО

Поверителен ключ за маркиране CRYPTO трябва да се транспортира по един от следните методи:

• Всеки метод, одобрен за ключови материали за TOP SECRET или SECRET;

• Редовната поща за пощенски услуги на САЩ, включително местонахожденията на пощенски офиси на ВС на САЩ, при условие че материалът не преминава през чужда пощенска система или друга чуждестранна инспекция.

7.6.3.3 НЕКЛАСИФИЦИРАНИ МАТЕРИАЛИ

НЕКЛАСИФИЦИРАНИ материали с маркировка CRYPTO трябва да бъдат транспортирани по един от следните методи:

• Всеки метод, одобрен за TOP SECRET, SECRET или CONFIDENTIAL за ключови материали;

• за превози в границите на САЩ, нейните територии и владения, неразрешен превозвач, при условие че превозвачът отговаря на следните критерии;

o Трябва да е фирма, регистрирана в САЩ;

o Трябва да осигурява непрекъсната отчетност на пратки, еквивалентни на проследяването, достъпно чрез редовната пощенска служба в САЩ; и

o Предоставя се разписка за подпис в крайната точка на доставка.

7.6.4 Транспортиране на оборудване COMSEC

Оборудването на COMSEC не може да се превозва в състояние с инсталиран ключ, освен ако физическата конфигурация на оборудването прави невъзможно отделянето на ключовия материал; въпреки това, оторизираните куриери могат да носят ръчно COMSEC оборудване. Вж. Параграфи 137 и 138 от Препоръка dd.

ЗАБЕЛЕЖКА: Повечето ново оборудване на COMSEC е софтуерно защитено при транспортиране и съхранение. Такова оборудване изисква резервиране на батерията по време на транспортиране и съхранение. Изваждането на батериите (загуба както на основната, така и на батерията) прави оборудването неработещо. Вижте приложимите процедури за поддръжка / процедури на оператор и разпорежданията за оперативна сигурност за всяко устройство за повече подробности.

Оборудването за SECRET COMSEC и цялото ключово производствено оборудване трябва да бъдат транспортирани по един от следните методи:

• USTRANSCOM / J3 (DCD);

• Куриерска служба на Държавния департамент;

• Официално определени и надлежно проучени куриери, които са държавни служители.

Поверително оборудване на COMSEC (с изключение на ключово производствено оборудване) може да бъде транспортирано по един от следните методи:

• Всеки метод, одобрен за оборудване SECRET COMSEC;

• Военна или военно-транспортна авиационна служба на САЩ (напр. Командване на военновъздушните сили (AMC), LOGAIR, QUICKTRANS);

• Регистрирана поща за пощенски услуги в САЩ, включително местонахожденията на армейските пощенски офиси на САЩ, при условие че материалът не преминава през чужда пощенска система или друга чуждестранна инспекция.

Изискванията за транспортиране на CCI са изложени в CNSSI № 4001 (Препоръка h). НЕКЛАСИФИЦИРАНО COMSEC оборудване, различно от CCI, може да бъде транспортирано по всякакъв метод, одобрен за доставка на друг еквивалентен ценен/ чувствителен материал.

7.6.5 Подготовка на доклад за трансфер

Мениджърът на изпращащият COMSEC акаунт ще подготви SF-153 и оригинала и две копия с него ще придружават пратката. Копие ще бъде запазено от изпращащият COMSEC акаунт до момента на връщане на подписана разписка/опис. След това копие от подписаната разписка ще бъде изпратено в COR чрез CARDS.

7.6.6 Отговорност за получаване / проследяване

Изпращащият мениджър на акаунти на COMSEC е отговорен за своевременната проверка на получателя, който получава изпратените материали. Мениджърът по доставката определя дата на спиране, която не надвишава 45 дни, след което трябва да се предприемат действия за проследяване. Това действие може да бъде във всяка писмена форма, подходяща за дейността (например официална кореспонденция на бланки, имейл и т.н.), при условие че въпросните материали и номерът на транзакцията / датата на отчета са ясно идентифицирани. Ако проследяващите действия се провалят (няма отговор в рамките на две седмици след проследяването или отговор, показващ неполучаване на материала), мениджърът трябва да представи доклад за инцидента на COMSEC за физическа загуба на материал.

7.7 Разписки на ръка за COMSEC материал

Ръчна разписка се използва за записване на приемането и отговорността за материалите на COMSEC, издадени на потребителя от мениджъра на акаунти на COMSEC. Мениджърите на акаунти на COMSEC могат да издават материали на COMSEC чрез разписка на ръка САМО за проучен персонал с надлежен сертификат.

Когато оборудването на CCI бъде върнато на продавач за ремонт, ще се използва разписка за ръка. Продавачът ще подпише разписката и ще върне съхранява копие в акаунта на COMSEC. Ръчните касови бележки трябва да се държат както от акаунта доставчик, така и от получаващият акаунт и не се изпращат до COR. Ако артикулът не може да бъде поправен, продавачът трябва да поиска прехвърляне на продукта.

При издаване на ключ TOP SECRET с надпис CRYPTO, мениджърът на акаунти на COMSEC трябва да гарантира, че TPI се поддържа по всяко време, като изисква две упълномощени за това ниво и обучени лица да подпишат материала.

На потребителите ще бъдат издадени само пълни издания на COMSEC ключови материали с надпис CRYPTO в кутии. Индивидуалните сегменти никога не трябва да се издават на потребители или да се прехвърлят на друг акаунт на COMSEC, без писмено разрешение на контролиращия орган (CA).

Мениджърът на акаунти на COMSEC ще използва SF-153 за издаване на материали на COMSEC при получаване на ръка. Мениджърът на акаунти на COMSEC ще проверява непрекъснатото притежание на всеки шест месеца по време на полугодишния процес на инвентаризация, като физически наблюдава материалите и поддържа писмена документация за това. Съществуващите разписки за получаване на ръка не трябва да се актуализират за физически наблюдавани материали по време на полугодишна инвентаризация, при условие че съдържанието на разписките не е променено.

Материалът за електронни ключове може да бъде издаден на притежател на разписка с помощта на електронно устройство за предаване. Устройството ще записва използването на електронния ключ и зареждането и унищожаването на електронния ключ, когато той се прехвърля или зарежда на криптографско устройство.

7.7.1 Квалификации на притежателя на ръка

Преди да издаде COMSEC материал на потребител, мениджърът на акаунти на COMSEC ще провери дали потребителят:

• Необходимо е да знае, като разполага с писмо с разрешение преди издаването и, ако материалът е класифициран, притежава необходимото разрешение до ниво, равно или по-високо от този, който е издаден.

• Ще бъде действителният потребител на материала (чиновниците или други служители, които не са потребители, няма да подпишат разписката).

• Получил подходящ инструктаж и, ако е необходимо, да се проведе обучение на потребителя.

• Ще бъде изцяло отговорен за материала; и знае мерките за физическа сигурност, необходими за защита на материала и възможните последици от компрометиране.

• Има необходимите средства за физическа защита за съхранение и използване, съизмерими с класификацията на продукта.

7.7.2 Задължения на получателя на ръка на материал

Мениджърът на акаунти на COMSEC трябва да уведоми потребителя за следното:

• Материалите на COMSEC, при получаване на ръка, се подписват и контролират от действителния потребител, докато не бъдат върнати на мениджъра на акаунти на COMSEC. Потребителите на ръчни разписки нямат право да препредават COMSEC материали. Ако друг потребител се нуждае от материала, материалът трябва да бъде върнат на мениджъра на акаунти на COMSEC за преиздаване.

• Физически мерки за сигурност, необходими за защита на материала и възможните последици от компрометирането му. Всички възможни компрометиращи събития, достъп от неоторизирани лица или нарушения на правилата за сигурност, засягащи материалите, трябва незабавно да бъдат докладвани на мениджъра на акаунти на COMSEC.

• Потребителите, които трябва да транспортират COMSEC материали при получаване на ръка извън техните съоръжения, трябва да имат предварително съгласие от мениджъра на акаунти на COMSEC.

• Потребителят ще бъде освободен от отговорност за материали, получени при разписка на ръка, само когато материалът е върнат на мениджъра на акаунти на COMSEC. Мениджърът на акаунти в COMSEC незабавно ще завърши връщане / затваряне на разписка и ще предостави копие на потребителя.

• Всеки елемент от COMSEC, предаден при получаване на ръка, ще бъде върнат на мениджъра на акаунти на COMSEC преди прехвърлянето, преназначаването или всяко отсъствие над 30 дни на лицето, което го е получило.

7.7.3 Подновяване на ръчно получаване

Разписки за предаване на ръка, които не са се променили (т.е. материалите на COMSEC, посочени в разписката на ръка), не трябва да се преиздават на всеки шест месеца, при условие че материалът е физически прегледан от мениджъра на акаунта на COMSEC по време на полугодишни инвентаризации. В противен случай мениджърът на акаунти на COMSEC ще инициира на всеки шест месеца или при необходимост нова разписка за подпис от притежателя на ръчната разписка. Копие от разписката за предаване на ръка трябва да бъде запазено от мениджъра на акаунти на COMSEC.

7.8 Унищожаване на материал COMSEC

Необходими са национални стандарти за унищожаване на COMSEC и класифициран материал, за да се гарантира, че чувствителните данни не могат да бъдат възстановени от остатъците от този материал след унищожаването.

Вграденият в устройство материал (различен от дефектен или дефектен ключ) трябва да бъде унищожен възможно най-бързо, след като е бил заменен или по друг начин е изпълнил предназначението си. Унищожаването на заместено или остаряло криптооборудване и подкрепяща документация също е от съществено значение за

поддържането на задоволителна национална позиция на COMSEC сигурността, тъй като тези материали могат да бъдат от голяма полза за враждебни интереси, желаещи да използват американските комуникации за разузнавателни цели. Преди унищожаването на ключов материал, мениджърът трябва да провери всички съобщения за датите на сесия на такъв материал.

Мениджърите на акаунти на COMSEC трябва да гарантират, че персоналът за унищожаване е бил подходящо обучен.

ЗАБЕЛЕЖКА: НЕ разрушавайте дефектни или погрешни материали за въвеждане. Такива материали трябва да бъдат докладвани на COR и отдела за защитните технологии на NSA (301) 688-5861 или 688-6816 и да се съхраняват до получаване на инструкции за унищожаване.

7.8.1 Процедури за рутинно унищожаване на материали на COMSEC

С изключение на разрешеното от Раздел 9.0 (Процедури за спешни действия на COMSEC), рутинното унищожаване на материали на COMSEC обикновено се извършва от мениджъра на акаунти на COMSEC или заместник-мениджъра при негово отсъствие и свидетел - подходящо проучено лице. Краткото заглавие, издание и счетоводен номер, ако има такива, на всеки артикул се проверяват непосредствено преди унищожаването. Преди унищожаването ще бъдат извършени разпоредби за проверка на оборудването и проверка на страницата. Докладът за унищожаване SF-153 може да се използва като контролен списък по време на унищожаване. Следните процедури трябва да се спазват:

• Притежателите на разписки на ръка могат да завършат унищожаване на ключов материал и да записват унищожаване на запис на разположение. Този запис трябва да бъде предоставен на мениджъра на акаунти на COMSEC за съгласуване.

• Мениджърът на акаунти на COMSEC може лично да събира изтекли и / или заменени ключови материали, да ги замени с нови материали и да извърши навременното унищожаване на изтекъл и / или заменен материал в присъствието на свидетел, проучен и с валиден достъп.

• В мобилни случаи може да се извърши рутинно унищожаване от страна на потребителя и подходящ свидетел. Устното уведомяване трябва да бъде последвано от формуляр за запис на разпореждане, подписан, датиран и инициран от потребителя и надлежно потвърден свидетел на унищожаването възможно най-скоро. След получаване на писмено потвърждение, мениджърът на акаунти на COMSEC ще счита материала за унищожен.

7.8.2 Време за унищожаване

Материалите на COMSEC ще бъдат унищожени само когато бъде указано от подходящ орган или както е посочено по-долу:

• Материалите на COMSEC, поръчани за унищожение поради смяна с нови издания, ще бъдат унищожени при получаване на новото издание, освен ако друго не е указано от подходящ орган. (б.а. – признавам, че тук понятието „подходящ орган“ не е ясно, в оригинала на текста не става дума за конкретен/ни органи, нито за термин или словосъчетание)

• COMSEC ключов материал, обозначен CRYPTO, редовно и нередовно заменен, който е издаден за употреба, трябва да бъде унищожен в рамките на 12 часа след изтичането на отделните ключови сегменти и / или сесия на използване. Въпреки това, когато специални обстоятелства възпрепятстват спазването на 12-часовия стандарт (напр. безпилотно съоръжение през уикенда или празничния период), унищожаването може да

бъде удължено до максимум 72 часа. Ключов материал, и при двата случая редовно и нередовно заменени, трябва да бъдат унищожени веднага след употреба, когато са налични повече от едно копие на ключовия сегмент или възможно най-скоро след сесия и не може да се съхранява по-дълго от 12 часа след сесия. Материалите на COMSEC, участващи в компрометирани ситуации, трябва да бъдат унищожени в рамките на 72 часа след получаване на инструкции за разпореждане от съответния орган. За обстоятелства, които не са обхванати по-горе, свържете се с COR.

• Излишното, остаряло и неизползваемо COMSEC оборудване, устройства и други елементи ще бъдат изхвърлени, както е указано от COR.

• Пълните издания на заменени ключови материали, обозначени CRYPTO, които се съхраняват от акаунт на COMSEC, трябва да бъдат унищожени в рамките на 5 дни след сесия.

• Поддържането и проба на материали, които не са обозначени CRYPTO, не се извършва регулярно и трябва да се унищожават само когато не се използват физически.

• Заместените класифицирани публикации на COMSEC, които се съхраняват в акаунт на COMSEC, трябва да бъдат унищожени в рамките на 15 дни след сесията.

• Остатъкът и помощни файлове/материали при въведените изменения на класифицираните публикации на COMSEC трябва да бъде унищожен в рамките на 5 дни след въвеждането на изменението.

Възможно е да възникнат ситуации, които предотвратяват навременното унищожаване на материалите на COMSEC без вина на персонала на акаунта на COMSEC (т.е. обстоятелства, при които се отнема разрешението за работа, като министерство или правителство имат пропуснато финансиране и т.н.). В тези ситуации се прилагат следните политики:

• В случай на спиране на работата, засягащо персонала на акаунта на COMSEC, акаунти на COMSEC, съдържащи ключови материали, които ще бъдат заменени по време на изключването (или друго събитие, при което разрешението за работа е оттеглено), трябва да закрепят такъв материал в одобрен от GSA контейнер за сигурност.

o При никакви обстоятелства, различни от сценария за аварийно унищожаване, този материал не трябва да бъде унищожен преди сесия (т.е. превантивно). Всеки материал, така унищожен, подлежи на докладване като COMSEC инцидент, за унищожаване без разрешение на контролиращия / командващия орган.

o При възобновяване на нормалната работа замененият материал се унищожава незабавно. Ако такова унищожаване се извърши извън нормалните времеви граници, определени в този раздел, то докладът за инцидент на COMSEC за късно унищожаване се представя на DHS CIMA, на контролния / командния орган, както е уместно, и на NSA (I3132). Изложението на обстоятелствата показва, че унищожаването е било забавено поради спирането на отдела (и / или други фактори, които могат да се прилагат, ако има такива).

• Очаква се в акаунт на COMSEC, чиито служители се считат за обучени и квалифицирани, и имат разрешение да работят по време на спирането, да завършат унищожаване на заменен материал по график.

7.8.3 Доклад за унищожаване

За да съобщи за унищожаването на материали на COMSEC, мениджърът ще подготви SF-153. Подписаният оригинал ще бъде запазен за целите на файла, а копие се препраща към COR (качено в CARDS).

7.8.3.1 Ключов материал

Когато всички ключови сегменти, съдържащи се в определен тип ключови материали, се използват или заместват и са унищожени, мениджърът на акаунти на COMSEC трябва да подготви отчет за унищожаване и да го представи на COR.

Запазените материали, унищожени по време на оперативна употреба, независимо дали от притежатели на ръчни разписки или от мениджъра на акаунти на COMSEC / алтернативен мениджър на акаунти на COMSEC, трябва да бъдат документирани в протокол за разпореждане. Записът за разпореждане трябва да има два подписа, удостоверяващи унищожаване на сегменти. Докладът за унищожаване трябва да включва следното изявление под реда НИЩО НЕ СЛЕДВА: „Официалните записи, с които разполагам, показват, че гореизброените вещи / продукти са били унищожени правилно от надлежно упълномощени лица.“ В този случай се изисква само един подпис върху доклада за унищожаване.

Когато ключът, който не е влизал в употреба, е унищожен от мениджъра на акаунти на COMSEC и свидетел, докладът за унищожаване трябва да бъде подписан от мениджъра и свидетеля и изпратен на COR.

7.8.3.2 Основен ключ (б.а. – за съжаление не намираме по-добър превод от английски на „seed key“)

Когато основният ключ се зареди в устройство и се преобразува в операционен ключ, мениджърът трябва да завърши процеса на унищожаване в рамките на счетоводната система.

ЗАБЕЛЕЖКА: НЕ се прилага за STE ключ.

7.8.3.3 Всички останали материали

След унищожаването на всички останали материали на COMSEC, мениджърът и свидетелят на COMSEC трябва да попълнят и подпишат доклад за унищожаване и да го предадат на COR.

7.8.4 Рутинни методи за унищожаване

Методи за рутинно унищожаване на хартиен COMSEC материал ще бъдат изгаряне, разпадане (б.а - вкл. с химикали) или раздробяване с висока степен на сигурност . Криптографските ключови ленти трябва да бъдат „крайно“ унищожени (термично унищожените означават унищожаване на материал до точката, в която той не може да бъде реконструиран), като се използват само одобрени от NSA устройства, изброени в Списъка с оценени продукти (EPL - Evaluated Products List) за устройства за унищожаване на перфорирани ленти. Хартия COMSEC и друг класифициран материал чрез разпадане или напречно нарязване на шредерите се използват само одобрени от NSA устройства, както са изброени в EPL. EPL файлове могат да бъдат намерени на URL адрес: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml (на този URL адрес могат да бъдат намерени и шредери и дегаузери EPL (за съжаление и за дегаузери не намираме преводно понятие, устройство с което се унищожават матнитни носители, напр. дискове, на практика така се унищожава самото електромагнитно поле, което е носител на информацията, след което следва и физическо унищожаване на носителя - б.а.)).

Акаунтите на COMSEC трябва да имат план за действие в извънредни ситуации за рутинно унищожаване на материали на COMSEC (например изгаряне на открито в кутия за кафе от двама упълномощен персонал) като част от стандартните им експлоатационни

процедури (SOP) на COMSEC в случай на неизправност или повреда на оборудването. (б.а. – обръщаме внимание на прагматизма и простотата на подобен род унищожаване, важен е крайният резултат и спазване на двойният контрол, самото унищожаване не е толкова здраво заковано в текстовете. Фактът, че у нас нямаме понятие за дегаузери, скъпи технически устройства, показва, че не сме наясно с най-добрите възможности за унищожаване на носители на ключов и класифициран материал. Това обаче не пречи да се изпълняват изискванията на тази инструкция в пълен обем, като дори някаква консервена кутия може да свърши работа).

Планът за действие при извънредни ситуации трябва да отговаря на изискванията на CNSSI 4004.1 и да включва поетапни процедури за извършване на унищожаването.

7.8.4.1 COMSEC Материал на хартия

Критериите, дадени по-долу, се прилагат за класифицирани COMSEC ключови материали и медии, които въплъщават, описват или прилагат класифицирана криптографска логика. Такива носители включват пълни наръчници за поддръжка, криптографски описания, чертежи на криптографска логика, спецификации, описващи криптографска логика, и криптографски софтуер.

ЗАБЕЛЕЖКА: Тези критерии НЕ се прилагат към лентата за ключове, която е съставена от хартия-Mylar-хартия. (б.а. - вижте COMSEC материал на нехартиен носител по-долу.)

• При унищожаване на хартиен COMSEC материал чрез изгаряне, изгарянето трябва да е пълно, така че целият материал да се редуцира до бяла пепел и да се поддържа огън така, че да не избягат неизгорели парчета. Пепелта трябва да се инспектира и, ако е необходимо, да се разпадне или намали до утайка.

• При унищожаване на COMSEC и класифициран материал на хартия чрез пулпиране, материалът трябва да бъде напълно разграден до остатъци от нечетливи влакна.

• Когато шредерите с висока мощност се използват за унищожаване на хартиени COMSEC материали (напр. Книги с кодове, удостоверяващи материали и някои класифицирани публикации на COMSEC), трябва да се използва кръстосан шредер, включен в списъка на NSA EPL за високоефективни кръстосани шредери.

7.8.4.2 COMSEC Материал, който не е от хартия

Разрешените методи за рутинно унищожаване на нехартиен COMSEC материал са изгаряне, топене, разпадане и химическа промяна.

• Ключовата лента COMSEC трябва да бъде унищожена или чрез разпадане или изгаряне. Само дезинтеграторите, одобрени от NSA, се използват за унищожаване на ключова лента COMSEC. Отново потребителите могат да унищожат ключовите ленти чрез изгаряне на сегменти на открито в кутия за кафе с двама проучени свидетели.

ЗАБЕЛЕЖКА: НЕ РАЗПОЛАГАЙТЕ хартиена лента с ключове от Mylar-хартия или хартия с висока мокра сила и заместител на хартия с дълготрайна среда (например, TYVEC олефин, полиетиленово влакно). Тези материали няма да се сведат до целулоза и трябва да бъдат унищожени чрез изгаряне или разпадане.

(*б.а. – нямаме по-добър вариант да покажем милар-хартия, освен снимка, не е нищо друго освен аналогови ленти от преди петдесет и повече години*:

• Микроформите (микрофилм, микрофиш или други фото-негативи с намалено изображение) могат да бъдат унищожени чрез изгаряне или с химически средства, като потапяне в домакинска белина (за майстори на сребърни филми) или ацетон или метиленхлорид (за възпроизвеждане на диапозитиви) за приблизително пет минути. Когато са унищожени по химически начин, листовете от филм трябва да бъдат отделени и ролковият филм трябва да се разгърне.

ЗАБЕЛЕЖКА: Трябва да се внимава, за да се предотвратят потенциални опасности при използване на химически средства за унищожаване. OSHA стандартите трябва да бъдат спазени.

(Със Закона за безопасност и здраве на работното място от 1970 г. Конгресът създава Администрация по безопасност и здраве на труда (Occupational Safety and Health Administration - OSHA), за да осигури безопасни и здравословни условия на труд на работещите мъже и жени чрез определяне и прилагане на стандарти и чрез осигуряване на обучение, работа с хора, образование и помощ.)

• Магнитните или електронните носители за съхранение или запис се обработват индивидуално. Магнитните ленти могат да бъдат унищожени при разпадане или изгаряне. Магнитните ядра могат да бъдат унищожени чрез изгаряне или топене. Възможно е магнитен диск, пакети с дискове и барабани да бъдат унищожени чрез отстраняване на цялата повърхност за запис с помощта на шпилково колело, шлифовъчен диск или чрез изгаряне.

ВНИМАНИЕ

НЕ поставяйте МАГНИТНА ЛЕНТА НА АЛУМИНИЕВИ ПОВЪРХНИНИ И СЪДОВЕ КАТО ТОВА МОЖЕ ДА ПРИЧИНИ ЕКСПЛОЗИЯ.

• Материалите за въвеждане на COMSEC, съхранявани на електронни устройства за пълнене на COMSEC, трябва да бъдат редовно прочиствани чрез нулиране или според указанията в специфична Доктрина за оперативна сигурност.

• Пластмасови ключодържатели. Целта за унищожаване на пластмасови кутии е увреждането на двете големи плоски повърхности (страни) на кутията. Това може да се постигне чрез поставяне на кутията вътре в торбичка с цип или подобна запечатваема торбичка или чрез пробиване или разтрошаване на целия контейнер. Като държите торбата за ръбовете, огледайте вътрешността на кутията през пластмасовата торбичка, за да се уверите, че всички ключови ленти са премахнати. Изхвърлете цялата торба и кутия като НЕКЛАСИФИЦИРАН боклук или съгласно местните предписания.

ЗАБЕЛЕЖКА: Мениджърите на акаунти на COMSEC трябва да са наясно, че празна касетка от лента ще се счупи, ако бъде разбит с тъп инструмент.

• Оборудване и компоненти на COMSEC. Рутинното унищожаване на COMSEC оборудване и компоненти от потребителите НЕ Е РАЗРЕШЕНО. Само администраторът на акаунти на COMSEC и заместник мениджърът са упълномощени да изхвърлят или унищожават оборудването на COMSEC. Инструкциите за изхвърляне на оборудване, което не се използва и не може да бъде ремонтирано или което вече не се изисква, трябва да се получат от COR.

7.9 Изисквания за инвентаризация

Всички акаунти на DHS са длъжни да извършват 100-процентови инвентаризации на шестмесечна база. COR ще координира отчетите, за да предостави необходимата документация за попълване на полугодишните инвентаризации. Инвентаризациите трябва да бъдат попълнени и върнати в COR (качени в CARDS) не по-късно от 20 работни дни след получаването им.

7.9.1 Провеждане на физически опис

Физическата (огледална) инвентаризация на всички материали на COMSEC в рамките на CMCS ще бъде извършена от мениджъра на акаунти на COMSEC и надлежно проучен свидетел. След като инвентаризацията започне, ако някое от двете лица не е в състояние да завърши целия процес, процесът на инвентаризация трябва да започне отначало. Следните процедури се прилагат при извършване на физическата инвентаризация:

• COMSEC Ключовите материали ще се отчитат по регистърния номер.

• Оборудването се отчита по сериен номер.

• Материалите ALC 6 и 7 се отчитат чрез кратко заглавие, издание и количество

o Ключът SDNS се отчита от идентификатора за управление на ключове (KMID)

o Всички клавиши Reg 0 са отговорни за своя ALC

o Профилът е отговорен на COR за само едно копие на определен ключ Reg 0, въпреки че могат да бъдат направени множество копия за използване в акаунта.

o Ако в акаунта е издаден ключ Reg 0, запасите от инвентаризация на COR няма да бъдат променени. Местният инвентар на акаунта ще бъде увеличен, за да посочи броя копия на издадения ключ Reg 0.

• Оборудването, което остава в заводски запечатани картонени опаковки, ще бъде инвентаризирано спрямо маркировката върху картонените кутии или каси, идентифициращи съдържанието в тях. Всеки контейнер ще бъде проверен за доказателства за подправяне.

• Отчетните публикации на COMSEC (KAO, KAMs и др.) Трябва да бъдат проверявани всяка година, ако не се прилагат други изисквания.

• STE се изисква да бъдат физически инвентаризирани по количество на полугодие.

7.9.2 Опис на запечатан или единичен материал

Някои артикули от COMSEC материали са запечатани или единични опаковани по време на производството и в повечето случаи няма да бъдат отворени, докато не бъдат използвани от реалния потребител. Мениджърът на акаунти на COMSEC трябва да има предвид, че въпреки, че отварянето на някои видове материали не трябва да се извършва преди реално използване, трябва да се остави време между отваряне и използване, за да се получат заместители на непълни или дефектни елементи. Отговорност на мениджъра на акаунти на COMSEC е да докладва за всички несъответствия на пратките на COR, веднага след като бъдат открити. Специфичните процедури за инвентаризация на запечатан или опакован от единица материал са изложени по-долу:

• Външните контейнери на COMSEC оборудване могат да бъдат маркирани с краткото заглавие и сериен номер на съдържанието. Когато са маркирани, контейнерите за оборудване не трябва да се отварят само за целите на инвентара, ако са получени в оригиналната опаковка на изпълнителя. В случаи на пакети, които са били отворени, мениджърът на COMSEC акаунти и заместникът му могат да проверят съдържанието спрямо етикета на пакета за точност, след което да запечатват отново пакетите, използвайки CAMO подходяща лента с лого, получена от клон на защитните технологии на NSA, (301) 688-5861 или 688-6816 (НЕ канална лента, опаковъчна лента и др.). Мениджърът и заместникът трябва да инициализират повторно запечатания етикет на пакета, потвърждаващ точността на посочените кратки заглавия и сериен номер. И в двата случая инвентаризацията оттук нататък ще бъде извършена чрез проверка на пакета за подправяне и проверка на краткото заглавие и сериен номер на етикета на контейнера спрямо инвентара.

• Ключовите ленти в защитните кутии се описват чрез отбелязване на краткото заглавие, издание, номер на регистъра и номер на сегмента на предния ръб на сегмента на лентата, който се появява в прозореца на номенклатурата на кутиите. Ключовите ленти в защитните кутии не трябва да се премахват, освен от потребителя на датата на влизане в сила. Отстранените сегменти трябва да бъдат отбелязани в свързания запис на разположение.

• Всяка единична опаковка ще бъде инспектирана, за да няма доказателства за подправяне.

• Публикациите на COMSEC не трябва да бъдат проверявани по страници, освен когато са получени или прехвърлени, при въвеждане на промяна в страницата за публикации или по време на промяна на инвентара на мениджъра.

7.9.3 Полугодишен опис

Всички материали на COMSEC трябва да бъдат инвентаризирани от мениджъра на акаунти на COMSEC ежегодно. Този опис трябва да се проведе с подходящо проучено физическо лице, за предпочитане заместник-мениджъра на акаунти на COMSEC или притежателя на разписка за материали на ръка, който е подписал за материала на COMSEC, като точно той служи за свидетел. Материалите, получавани на ръка от потребителите на отдалечени сайтове, не трябва да се виждат физически от мениджъра на акаунти на COMSEC; Вместо това, мениджърът на акаунти на COMSEC може да насочи притежателя на разписка за инвентаризация на материала. След това притежателят на разписка ще подпише нова разписка за проверка на притежанията си и ще я изпрати на мениджъра на акаунти на COMSEC.

Информацията в пакета за регистрация на акаунти на COMSEC трябва да бъде валидирана в COR заедно с всеки полугодишен / годишен опис.

ЗАБЕЛЕЖКА: Ако промяната на инвентаризацията на мениджъра на акаунти на COMSEC в раздел 7.9.4 или одитът, изискван в раздел 8.0 по-долу, включва попълнен 100% опис, следващият полугодишен опис може да бъде насрочен шест месеца след тази инвентаризация / одит по преценка на COR.

7.9.4 Промяна на записите на мениджъра

Инвентаризацията на всички материали на COMSEC (включително ALC 4 и 7 материали) трябва да се прави на всеки акаунт преди смяна на мениджърите на акаунти на COMSEC.

Този опис трябва да се проведе съвместно от изходящия мениджър на COMSEC акаунт и входящия. Изходящият мениджър на акаунти на COMSEC остава отговорен за всички материали по акаунта на COMSEC, докато новия мениджър на акаунти на COMSEC официално не бъде назначен от COR.

7.9.4.1 Изходящият мениджър напуска без провеждане на съвместна инвентаризация

В случай, че напускащ мениджър на акаунти на COMSEC се оттегли, без да попълни съвместна инвентаризация и да получи официално разрешение от COR, номиниращото длъжностно лице незабавно спира операциите по акаунтите и предприема действия, както е посочено в референтен параграф, параграф 97.e. (Вижте Препоръка dd, параграф 76.v относно отзоваването на бивш мениджър на акаунти на COMSEC.)

7.9.4.2 Неправомерно отсъствие или внезапно постоянно заминаване на мениджъра на COMSEC

Инвентаризацията на всички материали на COMSEC трябва да се извърши незабавно при неоторизирано отсъствие (както е определено от директивите на отдела или агенцията) или внезапно постоянно напускане на мениджъра на акаунти на COMSEC. Заместник-амениджърът на акаунта на COMSEC с подходящо проучен свидетел ще проведе тази инвентаризация и ще докладва резултатите на COR. Докладът трябва да бъде анотиран, за да отразява свързаните обстоятелства и ще бъде подписан както от заместник-мениджъра на акаунта на COMSEC, така и от свидетеля. След това официално ще бъде назначен нов мениджър на акаунти на COMSEC. Ако впоследствие свидетелят или заместник-мениджърът на акаунти на COMSEC бъде назначен за мениджър на акаунти на COMSEC, COR може да изтрие изискването за промяна на инвентаризацията на мениджъра на акаунти на COMSEC, при условие че инвентаризацията е успешно изпълнена. Криптографските, персоналните и физическите COMSEC инциденти, открити по време на инвентаризацията, трябва да бъдат докладвани, както е посочено в CNSSI 4003 (Препоръка k).

7.9.5 Попълване на отчета за инвентаризацията

Физическата инвентаризация може да се проведе с неофициален отчет за инвентаризацията, който ще служи като работно копие на официалния опис. Инвентарът ще отразява наличността на акаунта към датата на инвентаризиране.

След приключване на инвентаризацията ще се генерира Официален отчет за инвентаризацията, а мениджърът и свидетелят ще подпишат сертификационните блокове най-малко на първата и последната страница и могат да инициират всички други страници да се подписват. Оригиналното копие на официалния опис ще бъде запазено от мениджъра на акаунти на COMSEC и трябва да бъде сканирано и качено в CARDS. Освен това всички работни копия и документи, използвани при извършване на физическия инвентар, ще бъдат задържани от мениджъра за неговите / нейните файлове. Тези работни копия трябва да са на разположение на одиторите за преглед.

8.0 COMSEC ОДИТИ

COR трябва да извършва одити на базата на непериодични събития, за да не надвишава три (3) годишен период между одити. Такива одити се провеждат, за да се гарантира, че акаунтите на COMSEC отговарят на приложимите изисквания, регулиращи отчетността, обработката и защитата на материалите на COMSEC. COR трябва да гарантира, че честотата на одита се основава на стабилни принципи за управление на риска. Сметките в сайтове, които имат значителни технически заплахи или са особено уязвими

(например в чужбина), могат да изискват годишни одити по преценка на COR. Одитите могат да се извършват по всяко време, обявени или необявени предварително (т.е. планирани или извънпланови). По-честите одити могат да бъдат оправдани, ако акаунтът многократно показва несъответствия в своите процедури за счетоводство, обработка или контрол.

Одитът трябва да включва административен преглед на процедурите и 100% преглед на всички материали на COMSEC (както физически, така и електронни), включително проверка дали всички разписки на ръка са валидни (актуализирани през последните 6 месеца, ако материалът физически не е видян от мениджъра на акаунта на COMSEC). Акаунтът на COMSEC трябва също да предостави документация за инвентара от STE телефони (по количество), както и текущо сертифициране за проучванията за персонала на акаунта на COMSEC.

ЗАБЕЛЕЖКА: Докато одиторите не съгласуват материалите на ALC 4 или 7, трябва да се положат всички усилия, за да се гарантира местната отчетност на материалите на ALC 4 и ALC 7.

8.1 Достъп

Представителите на COR, когато действат в официалното си качество като одитори, могат да получат достъп до акаунтите на COMSEC, при условие че при пристигането им се представят подходящи идентификационни данни. Одиторът / инспекторът трябва да представи правилна идентификация преди да получи достъп до акаунта на COMSEC.

8.2 Одитен доклад

След приключване на одита всяка забелязана ситуация, изискваща незабавни мерки, ще бъде докладвана към мениджъра на акаунти на COMSEC. Ще се проведе изходен инструктаж с ръководството. Състоянието на акаунта, включващо коригирани по време на одита позиции, други позиции, които изискват корекция, и действия за подобрение, се обсъждат по време на изходящия брифинга. Официален одитен доклад, в който се очертават констатациите, състоянието на акаунт на COMSEC и препоръките за подобрение ще бъдат препратени на ръководството на организацията и на мениджъра на акаунти на COMSEC. Този отчет се съхранява в архивите на акаунтите.

8.3 Меморандум за коригиращи действия

Всички несъответствия, установени в одитния доклад, трябва да бъдат коригирани. Коригиращите действия се определят в Меморандум за коригиращи действия, който се представя на COR съгласно указанията в официалния одитен доклад. Този меморандум се съхранява в архивите на акаунтите.

8.4 Одитна оценка

Нивото на управление на акаунт на COMSEC се определя по време на одита на COMSEC въз основа на установен контролен списък. Определянето на рейтингови категории, които да отразяват резултатите от одита, ще предостави набор от измерими данни, използвани за оценка на COMSEC акаунта. Вижте приложение F за допълнителна информация.

9.0 COMSEC ПЛАНИРАНЕ ПРИ ИЗВЪНРЕДНИ СИТУАЦИИ

Всички акаунти на COMSEC трябва да поддържат текущ писмен план за спешни случаи за защита на материалите на COMSEC при извънредни ситуации. Планът за

действие при извънредни ситуации трябва да бъде част от изискваните стандартни оперативни процедури на COMSEC (SOP).

9.1 Планиране на аварийната защита

Извън континенталните Съединени щати (Outside the Continental United States - OCONUS) планът за извънредни ситуации трябва да отчита както природни бедствия, така и враждебни действия (като враг или терористична атака, мафиотски действия или гражданско въстание). Плановете за спешни случаи в организациите на OCONUS трябва да включват процедури за аварийно унищожаване (Emergency Destruction Procedures (EDP)).

Вътре в континенталните Съединени щати планът за извънредни ситуации ще се съсредоточи върху защитата на материал на COMSEC, уязвим на заплахи като природни бедствия, които вероятно ще възникнат в тяхното местоположение (например урагани на юг, торнадо или наводнения в Средния Запад, диви пожари на Запад, и т.н.). Освен това всички организации на CONUS (Continental United States) провеждат първоначално писмено определяне на риска, за да оценят потенциала за враждебни действия срещу техните съоръжения (като враг или терористична атака, мафиотски действия или гражданско въстание). Въз основа на чувствителността на операциите или съоръжението служителят по сигурността или удостоверява (писмено), че при прегледа е установено, че не е необходимо планът за действие при извънредни ситуации да анализира случаи на враждебни действия, или, ако се установи, че съществуват потенциални рискове, да разработи Emergency Destruction Procedures за включване в аварийния план.

По своя преценка ръководителите на отдели могат да изискат всяко съоръжение да създава план за спешни случаи, когато счита за възможни някои враждебни действия, независимо от местния риск.

Аварийната защита на COMSEC материали се прилага за всички съоръжения на DHS или компонент, които произвеждат или съхраняват COMSEC материали, и всички други съоръжения, които са определени да осигуряват резервна COMSEC възможност.

Оперативните процедури в съоръженията на COMSEC трябва да бъдат структурирани така, че да намалят броя и сложността на действията, които трябва да бъдат предприети по време на извънредни ситуации за защита на COMSEC материали. Например:

• По всяко време трябва да се съхранява само минималното количество COMSEC материали; т.е. рутинното унищожаване трябва да се извършва срочно и незабавно, когато това е разрешено, а излишъкът от COMSEC материал трябва да бъде изхвърлен в съответствие с DHS директивите. Изискванията на COMSEC се преразглеждат най-малко веднъж годишно, за да се потвърди необходимостта от материали, които са на разположение.

• Материалите на COMSEC трябва да се съхраняват по начин, който ще улесни аварийната евакуация или унищожаване.

Всички планове за спешни случаи се разработват в съответствие с процедурите, посочени в този раздел, и се преразглеждат ежегодно и се актуализират при необходимост, или когато промените в местната среда за сигурност налагат това.

9.1.1 Планиране на готовност за природни бедствия / аварии

Планирането за работа в условия на природни бедствия трябва да бъде насочено към поддържане на контрол върху сигурността на материала, докато ситуацията се стабилизира, като се вземе предвид евентуалната загуба на нормалната защита за физическа сигурност, която може да възникне по време на и след природно бедствие. Това планиране включва:

• Процедури за получаване на сигнал към първи реагиращи лица, като местна полиция, пожарникари, фелдшери и екипажи с опасни материали (HAZMAT).

• Докладване на пожар и първоначално гасене на пожар от определен персонал.

• Възлагане на отговорности на място за осигуряване на защита на съхраняваните материали на COMSEC.

• Осигуряване или премахване на класифициран материал на COMSEC и евакуация на зоната / местата.

• Защита на материала, когато е необходимо допускане на първи реагиращи лица в защитената (ите) зона (и).

• Оценка и докладване на вероятна експозиция/изтичане на класифицирани материали на COMSEC към неоторизирани лица по време на извънредната ситуация.

• Инвентарен опис на класифицирани и CCI COMSEC материали и отчитане на евентуални загуби или неоторизирани експозиции към ценните книжа на HCA IA (I31132) и COR.

9.1.2 Планиране на готовност за враждебни действия

Планирането на враждебни действия трябва да се съсредоточи върху процедурите за безопасно евакуиране или сигурно унищожаване на материалите на COMSEC, включващи осигуряване на подходящ тип и достатъчен брой устройства за извършване на аварийно унищожаване и провеждане на необходимото обучение за всички лица, които могат да изпълнят необходимите процедури на унищожение. Такова планиране трябва да осигурява:

• Оценка на заплахата от различни видове враждебни действия при конкретната дейност и заплахата, която тези потенциални аварийни ситуации представляват за съхраняваните материали на COMSEC.

• Наличие и адекватност на възможностите за защита на физическата сигурност (например, периметър, охрана и физическа защита в отделните сгради и други места, в които се съхранява материалът на COMSEC).

• Съоръжения за извършване на аварийна евакуация на COMSEC материали при аварийни условия, включително оценка на вероятните рискове, свързани с евакуацията.

• Съоръжения и процедури за ефективно безопасно аварийно унищожаване на задържания материал на COMSEC, включително адекватни доставки на устройства за унищожаване, наличие на електрическа енергия, сигурни съоръжения за съхранение в близост, адекватно защитени зони за унищожаване, задачи на персонала и отговорности за прилагане на аварийно унищожаване.

• Предохранително унищожаване на материали на COMSEC (*б.а. – В ДКСИ също се води спор дали защитата на информацията включва нейното унищожаване, т.е. защита чрез унищожаване. Спорът е както юридически, така и технологичен*), по-специално наръчници за поддръжка и ключов материал, които не са необходими оперативно, за да се гарантира непрекъснатостта на операциите по време на аварийната ситуация. При влошаваща се ситуация трябва да бъдат унищожени всички ръководства за пълна поддръжка (т.е. тези, съдържащи криптографска логическа информация), които не са абсолютно необходими за продължаване на мисията. Когато при аварийни условия няма достатъчно време за пълно унищожаване на подобни ръководства, трябва да се положат всички разумни усилия за премахване и унищожаване на техните чувствителни страници (т.е. тези, съдържащи криптографска логика). Чувствителните страници в произведените от САЩ ключови материали се намират в Списъците на ефективни страници (Lists of Effective Pages). Освен това, някои ключови материали също така идентифицират своите

чувствителни страници с помощта на сиви или черни диагонални или правоъгълни маркировки в горната част на подвързващия ръб.

За да се подготвите за възможно аварийно унищожаване на чувствителни страници от ръководствата за поддръжка на COMSEC по време на ситуации или в райони, където е възможно прихващане от враждебни сили, се предлага следното:

1. Нанесете отличителни маркировки (напр. Червени ивици) върху ръба на корицата и кориците на всички ключови материали, съдържащи идентифицирани чувствителни страници.

2. Отстранете винтовите стълбове или свързващи пръстени или отворете свързващото устройство с много пръстени, което от двете е приложимо.

3. Извадете всяка чувствителна страница от KAM и отрежете горния ляв ъгъл на страницата, така че първият отвор за свързване да бъде отстранен. Трябва да се внимава да не се изтрие текст или диаграма.

4. Сглобете документа и извършете проверка на страницата.

Ако се наложи да се извърши аварийно унищожаване, чувствителните KAM страници могат да бъдат премахнати, както следва:

1. Отстранете винтовите стълбове или свързващи пръстени или отворете свързващото устройство с много пръстени и премахнете всички страници от KAM.

2. Поставете тънка метална пръчка (напр. Жица или отвертка) през останалите горни леви отвори на документа.

3. Хванете пръта в двете си ръце и разклатете енергично документа; чувствителните страници трябва да изпадат свободно.

Външните комуникации по време на извънредни ситуации трябва да бъдат ограничени до контакт с една отдалечена точка. Тази точка ще действа като център за разпространение на трафик на изходящи съобщения и като филтър за входящи заявки и насоки, като по този начин ще освободи персонала и съоръженията на сайта от множество действия по време на извънредни ситуации. Когато има предупреждение за враждебни намерения и защитата на физическата сигурност е недостатъчна, за да се предотврати превишаването на съоръжението, сигурните комуникации трябва да бъдат прекратени навреме, за да се даде възможност за цялостно унищожаване на всички класифицирани и CCI COMSEC материали, включително класифицирани и CCI елементи на COMSEC оборудването.

9.2 Изготвяне на авариен план

Подготовката на аварийния план е отговорност на мениджъра на акаунти на COMSEC. Планът трябва да бъде съгласуван с подходящ персонал за охрана и пожарна безопасност. Ако планът изисква унищожаване на COMSEC материал, всички материали за унищожаване, устройства и съоръжения трябва да бъдат лесно достъпни и в добро състояние. Планът трябва да е реалистичен; той трябва да е работещ и да постига целите, за които е подготвен.

Всички задължения по плана трябва да бъдат ясно и кратко описани.

Целият оторизиран персонал в съоръжението трябва да е наясно с наличието на плана, като планът трябва да бъде обозначен за бърза готовност за достъп и използване. Всеки човек, който има задачи, определени по плана, трябва да получи подробни инструкции как да изпълнява тези задължения, когато планът влезе в сила. Целият персонал трябва да е запознат с всички задължения, така че при необходимост да бъдат направени промени в заданието. Това може да се постигне чрез периодично завъртане на аварийните задължения на целия персонал, т.е. да се познават повече от една процедура и задачите в цялост.

Периодично трябва да се провеждат тренировъчни упражнения (препоръчват се тримесечни упражнения), за да се гарантира, че всички, особено новоназначеният персонал, който трябва да участва в действителна извънредна ситуация, ще е в състояние да изпълнява своите задължения. Ако е необходимо, планът трябва да бъде променен въз основа на опита от тренировъчните упражнения.

Трите налични варианта при спешни действия за противодействие на враждебни намерения са обезопасяването на материала, отстраняването му от мястото на аварийната ситуация или унищожаването му. Планиращите трябва да обмислят кое от тях може да бъде приложимо за техните съоръжения, поотделно или в комбинация. Кой вариант да изберете в различни ситуации трябва да бъде ясно посочено в плана. Например, ако се окаже, че гражданското въстание ще бъде краткотрайно, а съоръжението COMSEC да бъде само временно изоставено, действията, които трябва да предприемат, биха могли да бъдат:

• Уверете се, че всички заменени ключови материали са унищожени.

• Съберете сегашния и бъдещия материал за въвеждане и го вземете, ако е осигурена адекватна защита за сигурност. В противен случай съхранявайте този материал в одобрен контейнер за сигурност.

• Нулирайте (б.а. – превод на „Zeroize“) криптографското оборудване, което не може да бъде евакуирано.

• Осигурете вратите на помещенията и напуснете.

• След завръщането си направете внимателен и пълен опис на всички материали на COMSEC.

• Или, ако изглежда, че съоръжението е вероятно да бъде пренаселено с външни лица, трябва да се приложат процедурите за аварийно унищожаване.

9.3 Приоритети за аварийно унищожаване

Три широки категории материали на COMSEC, които могат да изискват унищожаване при извънредни ситуации с враждебни действия, са ключови материали, други средства за COMSEC (напр. Ръководства за поддръжка, инструкции за експлоатация и общи доктринални публикации) и оборудване на COMSEC (б.а. – обърнете внимание на трите категории Комсек материали). В зависимост от наличието на достатъчно персонал и съоръжения за унищожаване, трябва да се спазват следните приоритети:

• Приоритети за унищожаване в категории от материали на COMSEC. Когато има достатъчно съоръжения за унищожаване, трябва да се поемат отговорности от различни лица за унищожаване на материала във всяка категория чрез отделни съоръжения за унищожаване, както е посочено в следните алинеи:

Ключов материал. Приоритетите за аварийно унищожаване на ключовите материали са следните:

1. Заменен ключов материал, обозначен CRYPTO.

2. Понастоящем ефективен ключов материал, обозначен CRYPTO (за включване на нулиране на ключови променливи, съхранявани електрически в крипто оборудване и устройства за зареждане).

3. Бъдещи издания на TOP SECRET ключови материали, обозначени CRYPTO.

4. Бъдещи издания на SECRET и CONFIDENTIAL keying material, обозначен CRYPTO.

5. Ключ за обучение, поддръжка и пример.

Други средства за COMSEC. Приоритетите за аварийно унищожаване на класифицираните помощни средства на COMSEC, различни от ключовите материали, са следните:

1. Попълнете ръководствата за поддръжка на крипто- или чувствителни страници от тях.

2. Документи за състоянието, показващи ефективните дати за COMSEC ключови материали.

3. Съхраняване на списъци и директории на притежателите на материали.

4. Оставащи класифицирани страници на ръководствата за поддръжка на крипто.

5. Криптографски и некриптографски оперативни общи публикации (KAGs или NAGs).

6. Криптографски инструкции за експлоатация (Cryptographic Operating Instructions - KAO).

7. Оставащи класифицирани COMSEC документи.

8. Министерства, агенции и служебните публикации с общи доктринални указания.

COMSEC Оборудване. Трябва да се положат разумни усилия при влошаващи се ситуации за евакуация на COMSEC оборудването. В действителна спешна ситуация, непосредствената цел е да направи оборудването на COMSEC неизползваемо и непоправимо. Когато има предупреждение за враждебни намерения, сигурните комуникации трябва да бъдат прекратени предварително, за да се даде възможност за цялостно унищожаване на оборудването на COMSEC. Приоритетите за аварийно унищожаване на оборудването на COMSEC са следните:

1. Обезценете/Нулирайте оборудването, ако ключовият елемент не може да бъде физически изтеглен.

2. Извадете и унищожете печатни платки с етикет CCI или класифицирани (забележка: червен етикет може също да показва, че печатни платки са CCI или класифицирани).

3. Унищожете останалите класифицирани и CCI елементи.

ЗАБЕЛЕЖКА: Не трябва да се унищожават корпусите на оборудването и некласифицираните елементи, които не са маркирани CCI. Ръководствата за поддръжка на COMSEC оборудване съдържат списъци с компоненти, които идентифицират класифицирани и CCI елементи.

• Приоритети за унищожаване са комбинирани категории материали на COMSEC. Когато съоръженията за персонал и / или унищожаване са ограничени, трите категории материали на COMSEC ще бъдат комбинирани и унищожаването ще се извърши в съответствие със следния списък на приоритетите:

1. Всички ключови материали, обозначени CRYPTO, в следния ред: заменен ключ, действащ в момента ключ и бъдещ ключ;

2. Чувствителни страници от класифицирани ръководства за поддръжка или цялото ръководство (ако чувствителните страници не са обозначени отделно). Класифицирани и CCI елементи от класифицирано и CCI COMSEC оборудване;

3. Всички останали класифицирани COMSEC или свързани материали.

ЗАБЕЛЕЖКА: Корпусите на оборудването, некласифицираните елементи, които не са маркирани CCI, и некласифицираните части от ръководства за поддръжка, инструкции за експлоатация и др., Не трябва да бъдат унищожавани.

9.4 Методи за аварийно унищожаване и докладване

Всеки от одобрените методи за рутинно унищожаване на класифициран COMSEC материал може да се използва за аварийно унищожаване. По-долу са представени насоки за аварийното унищожаване на определени категории материали на COMSEC и за провеждането на аварийно унищожаване в конкретни оперативни ситуации.

• Хартиен COMSEC материал. Хартиените материали на COMSEC, като публикации и справочници, трябва да бъдат унищожени след реконструкция. Всяко от устройствата за унищожаване на хартия, изброени в EPL-тата за шредер или дезинтегратор, ще извърши терминалното унищожаване на хартиения COMSEC материал. Унищожаването на класифицираната хартия COMSEC може да се извърши и чрез изгаряне. Изгарянето може да се извърши в мангали, конструирани чрез отстраняване на горния край на метален барабан и пробиване на дупки в страната на барабана близо до дъното. Трябва да се оформя телена мрежа, която да пасва на върха на мангала; метален прът или тръба може да се използва за разбъркване на пепелта.

• Нехартиен ключ за COMSEC. Нехартиен ключ за COMSEC, като например лента за ключове (много пъти имахме колебание за превода на key tape), трябва да бъде унищожен след реконструкция. Всяко от устройствата за унищожаване, изброени в Disintegrator EPL, ще извърши терминалното унищожаване на нехартиен ключ за COMSEC материал. Унищожаването на нехартиен ключ за COMSEC може да се извърши и чрез изгаряне. Изгарянето може да се извърши в мангали, конструирани чрез отстраняване на горния край на метален барабан и пробиване на дупки в страната на барабана близо до дъното. Трябва да се оформя телена мрежа, която да пасва на върха на мангала; метален прът или тръба може да се използва за разбъркване на пепелта.

• Електронни устройства за съхранение Данните на COMSEC, съдържащи се в електронните устройства за съхранение, се изчистват чрез нулиране съгласно инструкциите за оборудването. Електронните устройства за съхранение, като KSD-64A, които в някои случаи не могат да бъдат нулирани, трябва да бъдат унищожени чрез най-лесно достъпното средство за разпадане, чукане или топене.

• Оборудване на COMSEC. При действителна враждебна ситуация класифицираното оборудване на COMSEC и означените като CCI трябва да бъдат унищожени толкова старателно, колкото времето и обстоятелствата позволяват. Когато има предупреждение за враждебни намерения, сигурните комуникации трябва да бъдат прекъснати последни, но навреме, за да се позволи пълно унищожаване на COMSEC оборудването. По време на унищожаването на оборудването и компонентите на CCI трябва да се даде същия приоритет като класифицираното оборудване и компоненти. Класифицираните и CCI компоненти на оборудването трябва първи да бъдат премахнати и унищожени.

• Аварийно унищожаване на борда на самолети и кораби. Когато се сблъскате с неизбежна загуба, залавяне или компрометиране на самолет или кораб, нулирайте цялото оборудване на COMSEC и унищожете или изтрийте целия ключов материал. Ако условията позволяват, изтриване на COMSEC материали, преносимо оборудване и устройства на COMSEC, носители за съхранение на информация и др.

Точната информация относно степента на аварийно унищожаване е абсолютно важна за ефективната оценка на въздействието на събитието върху сигурността и е на второ място по важност само за провеждането на цялостно унищожаване. Мениджърът на акаунти на COMSEC или длъжностното лице, отговорно за опазването на материалите на COMSEC, които са били подложени на аварийно унищожаване, е отговорен за съобщаването на съпътстващите факти в съответния отдел или агенция по най-бързите налични средства до DIRNSA, ATTN: I3132 (клон на IA ценни книжа), и към COR. Докладите трябва ясно да посочват разрушения материал, метода (ите) на унищожаване и степента на унищожаване. Те трябва също да идентифицират всички предмети, които не са били унищожени напълно и за които може да се предположи, че са компрометирани.

Във всички случаи на аварийно унищожаване се представя доклад за инцидентите на COMSEC в съответствие с CNSSI 4003.

10.0 ИНЦИДЕНТИ НА COMSEC

От съществено значение е незабавно да се съобщава за всеки инцидент, който може да е подложил на компрометиране материали и / или контролирано криптографско изделие (CCI). За да бъде ефективна, националната система за докладване на инциденти на COMSEC трябва да получава бърза и ясна информация, свързана с обстоятелствата около инцидента. В повечето случаи навременното отчитане ще намали до минимум въздействието на нарушението или загубата на материал и оборудване. Колкото по-дълго е забавянето на докладването на инциденти, толкова по-трудно е да се определи и минимизира въздействието върху националната сигурност. Докладите за инциденти също служат като основа за установяване на тенденциите в инцидентите и за разработване на процедурни и доктринални мерки за предотвратяване на повторение на подобни инциденти. Потребителите на материали на COMSEC, включително CCI, се насърчават да докладват незабавно за инциденти на COMSEC.

10.1 Докладване на инциденти на COMSEC

Мениджърът на акаунти на COMSEC трябва да съобщава за инциденти с COMSEC, както е предписано в този раздел и CNSSI 4003. Докладите за инциденти трябва да бъдат изпращани незабавно и не трябва да бъдат забавяни по административни канали по някаква причина, освен основно за събиране на факти. Вижте CNSSI 4003, параграфи 30. до 32. за срокове за докладване.

Следните процедури се спазват при докладване на инциденти на COMSEC:

• Незабавно обадете се на горещата линия на COR (540-542-2737)

• Всички акаунти на COMSEC са длъжни да изпращат доклади за инциденти на COMSEC чрез мрежата HSDN (Homeland Secure Data Network) само на следния имейл адрес: DHS_CIMA@dhs.sgov.gov. Този адрес представлява централна публична папка в HSDN Outlook, създадена с изричната цел за изпращане на доклади за инциденти на COMSEC в CIMA. Той е достъпен за всички членове на CIMA в рамките на COR; Следователно е ненужно и нежелателно да изпращате доклади за инциденти на всеки човек. Изискването за подаване на отчети чрез HSDN НЕ предполага, че отчетите трябва да бъдат класифицирани (класификацията на докладите за инциденти на COMSEC се основава единствено на съдържанието на тези доклади). Попълнете и представете писмения доклад в съответствие с приложение B към Препоръка (к) в рамките на изискуемите срокове. Не отлагайте представянето на този първоначален доклад за задълбочено събиране на факти. Докладвайте всички уместни известни факти; представете допълващи доклади, ако е необходимо.

Отговорността за уведомяването за контролен орган/ и (CA / CmdAuths), както е приложимо, се носи от отчитащия се акаунт на COMSEC. Адресирайте писмените доклади до ConAuths / CmdAuths заедно с CIMA, ако е възможно. Уведомете най-малко по телефона.

Хората не бива да се обезсърчават да съобщават за инцидент в COMSEC поради страх от възмездие. Въпреки това ще бъдат предприети дисциплинарни действия срещу извършителя или извършителите на грубо небрежни или умишлени действия, които застрашават сигурността на материалите на COMSEC. Лицата не трябва да бъдат дисциплинирани изрично за подаване на сигнал за инцидент в COMSEC, освен ако:

• Установено е, че те са причинили нарушението чрез съзнателно пренебрегване на изискванията за сигурност или груба небрежност, или

• Инцидентът не е преднамерен по своя характер, но отразява модел на небрежност или небрежност (например многобройни нарушения за период от 12 месеца) или

• Умишленото или небрежно разкриване на неоторизирани лица на всяка класифицирана криптографска информация.

10.2 Видове инциденти на COMSEC

Има три типа инциденти: криптографски, личен и физически. Вижте CNSSI 4003, РАЗДЕЛ VIII, за допълнителна информация и примери за всеки тип.

10.3 Видове доклади за инциденти

Има три типа, ако има съобщения за инциденти: първоначален, допълващ и окончателен. Вижте CNSSI 4003, приложение C, за допълнителни указания и формуляра за доклад на инцидентите COMSEC.

Изводи от превода на Инструкцията Комсек 4300 на САЩ:

1. Необходими са указания чрез нарочни документи за покриване на минимални стандарти по защита на информацията. Тези документи задават точно минималните стандарти. Не се задължава никой, но и не се ограничават организациите след покриването на минималните стандарти да повишават и подобряват защитата на материалите и ключовете за тях чрез повишаване на изискванията и покриване на допълнителни критерии. Тази политика се установява от държавата, т.като там се намират очевидно най-сериозните аналитични способности и познаване на средата за сигурност. С тези политики се задължават и всички органи и институции, които са контрактори на държавата или по някаква причина трябва да работят със защитена информация;
2. Допускат се различни варианти на съхранение на материали и ключовете към тях, но с ясно и категорично съобразяване с нивото на защитената информация и съответните минимални стандарти;
3. Няма никакви указания или предписания какви/откъде трябва да бъдат технологиите или самите устройства, които се използват. Т.е. от пазара може да се вземе това, което е най-подходящо за конкретния случай. Материалите и устройствата просто трябва да отговарят на минималните определени стандарти за сигурност. В редките случаи, когато се препоръчва някакво устройство, се препоръчват поне няколко разновидности. Пример са устройствата за достъп: Federal/DoD Public Key Infrastructure (PKI), Personal Identity Verification (PIV), или Common Access Card (CAC);
4. Двойният ТПИ контрол над използваните криптографски кодове и ключове намалява до минимум възможността за злоупотреби, нарушения и грешки при тяхното използване. У нас такъв контрол не се използва, поне за сега;
5. Изключително гъвкаво се използват комбинации от класифицирани и некласифицирани (но с ограничен публичен достъп) обозначения на материали и съответните мерки за защита. Т.е. от една страна се търси ограничаване на достъпа до ключове и кодове, вкл. и до информация от високо ниво на защита чрез класифициране на информация и достъп, от друга – използване на по-широка експертиза в полза на защитата, на самата информация и на процедури за осведомяване на професионалисти и заинтересовани, като не им се дава знание за заключването, предаването, съхранението и вида на информацията, чрез обозначенията НЕКЛАСИФИЦИРАНО или ЗА ОФИЦИАЛНО ИЗПОЛЗВАНЕ. Тази система напомня в известна степен на съществуващата у нас преди 2002 г., когато всяко ведомство създаваше своя система за защита на различните тайни от публичен достъп по своите нужди с подзаконов нормативен акт;
6. Очевидно е, че контролът е по всяко време и повсеместен. У нас за обучение се правят протоколи в свободна форма на всяка организация, тук се водят дневници по образец

и се съхраняват непрекъснато. Тук достъпът до материалите (кодове и ключове) се защитава най-малко на същото ниво като самите материали, като многократно се подчертава този факт, ние също го имаме като текст в ЗЗКИ, но съхранението на ключове за помещения, компютърни пароли, ключове за РАК-шкафове и т.н. не се спазва толкова стриктно. Отчетността и строгата отговорност при получаване на достъп до кодове и ключове за криптиране разшифроване тук е очевидно по-сериозна. Всъщност защитата на ключовете е по-лесно реализируема, т.като става дума за ограничен брой обекти за защита, държавата не може да контролира самите ползватели толкова ефективно през работно и още повече в извънработно време, но може да „закове“ процедурите по използването;

7. Много подробно са разписани някои ключови процедури като приемане на материали на ръка, сдаване, съответно приемане на длъжности като Комсек мениджър, инвентаризация, ангажименти на изходящия мениджър и т.н. Вниманието на процедурата по сдаване/приемане на длъжности по защита на информацията очевидно се счита за критична по отношение на сигурността. В такива текстове документът прилича много повече на наръчник;

8. Подробно са разработени варианти за действие при критични и кризисни ситуации, при компрометиране на сигурността. Тези варианти са много полезни в извънредни положения, при бедствия, аварии и катастрофи, при преместване на офиси и помещения на организацията и дори при масово текучество на кадри. Отново имаме прилика с наръчник за действие с прости и ясни последователности от действия;

9. Правилата, създадени в този документ в огромната си част са превърнати в стандарти, т.е. в някои случаи това дори е директно заявено (напр. в §7.8., където за унищожаването са заявени „необходими национални стандарти за Комсек“). Такова отношение към настоящия документ показва възприемането му като норма/закон, дори догма по отношение на комуникационната сигурност;

10. Изключително внимание се обръща на унищожаването на материали и информация. Редът и изискванията са строги, но методите са многобройни, съобразени със съответните физически носители на информацията. При спазване на процедурата се търси ефективен краен резултат, а самите методи на унищожаване не са толкова важни и могат да бъдат импровизирани, в зависимост от ситуацията;

11. Вероятен общ извод от този документ е: защитата на информация се гради на нивото на потребителите с най-ниска квалификация, т.е. защитата на информацията чрез Комсек трябва да е понятна и достъпна на абсолютно всички лица, които имат достъп до защитена така. Тук няма място за самопроизволни действия или някакво особено творчество. Опирайки се на традициите на прецедентното право в САЩ очевидно е извършена огромна събирателна и аналитична работа, изследвани са множество случаи (това е просто очевидно при вмъкваните забележки и забрани в текстовете тук, както и при приложенията по-долу към документа) и добри практики;

12. Министерството на вътрешната сигурност е създадено непосредствено след атентатите от 9/11 през 2001 г. То представлява най-голямата административна реформа в САЩ след Втората световна война. Очевидната му връзка с атентатите е изисквала нови и ултрасъвременни подходи както към защитата на необходимата информация, така и към нейното своевременно разпространение и предаване към съответните органи за предотвратяване на преки или косвени заплахи за територията или гражданите на страната. Този последен факт е причина за формата и съдържанието на документа. Поради което този документ още е и елемент от една сериозна и мащабна нормотворческа тенденция в началото на века.

ПРИЛОЖЕНИЯ

Б. а. - Следват приложения към документа. Приложенията са конкретни образци, други документи, препратки и т.н., които няма да превеждаме, поради тяхната вътрешна национална специфика за САЩ. Ще ги покажем и изброим обаче, т.като е важно да се разбира, какви готови бланки и образци се използват, от една страна, и от друга, т.като в текста сме ги споменавали и сме оставили да бъдат видяни като съпътстващи и необходими. Тези готови бланки улесняват и подпомагат системата за защита на информацията при реализирането на Комсек.

Приложение А

Препратки (б.а. – документи в оригинал, за да могат да бъдат търсени от читателите)

Изискванията на референтните публикации се прилагат към настоящата инструкция и техните приемни документи в посочената степен.

a. National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990

b. CNSS Policy No. 1, National Policy for Safeguarding and Control of COMSEC Materials, dated September 2004

c. CNSS Instruction No. 4009, National Information Assurance (IA) Glossary, dated 6 April 2015

d. CNSS Directive No. 502, National Directive on Security of National Security Systems, dated 16 December, 2004

e. AMSG-773, Policy and Procedures for Handling and Control of Two-Person Controlled (TPC) NATO Sealed Authentication System (SAS), dated January 1993

f. SDIP-293, NATO Cryptographic Instructions, dated May 2007, Rev. 1 dated January 2009.

g. CJCS Instruction 3260.01B, Joint Policy Covering Positive Control Material and Devices, dated February 2006

h. CNSS Instruction No. 4001, Controlled Cryptographic Items, dated 7 May 2013

i. Intelligence Community Directive (ICD) No. 705, Sensitive Compartmented Information Facilities, dated 26 May 2010

j. Federal Specification FF-P-110J, Padlock, Changeable Combination (Resistant to Opening byManipulation and Surreptitious Attack), dated February 1997, as amended 20 January 2004

k. CNSS Instruction No. 4003, Reporting and Evaluating Communications Security (COMSEC) Incidents, dated May 27, 2014

l. Federal Specification FF-L-2890A (Type III), Lock Extension (Pedestrian Door, Deadbolt), dated 1 April 2004

m. Federal Specification FF-L-2740A, Locks, Combination, dated January 1997, as amended 25 May 2001

n. CNSS Instruction No. 7000, TEMPEST Countermeasures for Facilities, dated May 2004

o. DoD Instruction 5240.05, Technical Surveillance Countermeasures (TSCM) Program, dated 22 February 2006

p. CNSS Policy No. 3, National Policy for Granting Access to U.S. Classified Cryptographic Information, dated October 2007

q. CNSS Policy No. 14, National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Authorized U.S. Activities That Are Not a Part of the Federal Government, dated 1 November, 2002

r. CNSS Policy No. 8, Release and Transfer of US Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments, dated 1 Aug, 2012

s. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006

t. DoD Instruction 8500.2, Information Assurance (IA) Implementation, dated February 6, 2003

u. Intelligence Community Standard Number 500-16, Password Management, Effective 16 March 2011

v. Federal Specification FF-L-2937, Combination Lock, Mechanical, dated January 21, 2005, as amended 1 February 2007

w. Federal Standard 809A, Neutralization and Repair of GSA- Approved Containers, dated 10 May 2005

x. Office of Management and Budget Memorandum M-05-24, Subject: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, dated 5 August 2005

y. CNSS Instruction No. 4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material, with ANNEX B as amended 24 October 2008

z. CNSS Instruction No. 4006, Controlling Authorities for Traditional Communications Security (COMSEC) Material, dated April 17, 2012

aa. CNSS Instruction No. 4000, Maintenance of Communications Security (COMSEC) Equipment, dated 12 October, 2012

bb. CJCS Instruction 6510.06B, Communication Security Releases to Foreign Nations, dated 31 March 2011

cc. CNSS Instruction No. 1002, Management of Combined Secure Interoperability Requirements, dated August 2007

dd. CNSS Instruction No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, dated 22 August, 2011

ee. CNSS Instruction No. 4032, Management and Use of Secure Data Network Systems (SDNS) Firefly Keying Material and Related Equipment, dated 22 June, 2015

Приложение Б

Електронни устройства за зареждане

1. Увод

Устройствата за електронно пълнене (напр. Устройство за пренос на данни (DTD), сигурна система DTD2000 (SDS), прост ключов товарач (SKL) или наистина прост ключов товарач (RASKL) са ръчни устройства, предназначени за безопасно съхраняване, транспортиране и прехвърляне на COMSEC ключов материал по електронен път между устройства за зареждане и свързаното с тях COMSEC оборудване. Страната на хоста е малък компютър, използван за управление на функциите на устройството за зареждане или пускане на некласифициран потребителски приложен софтуер (UAS) за специални функции. COMSEC изпълнява криптографските функции и е одобрено устройство за съхранение на ключови материали…..

Приложение С

Безопасни телефонни устройства ….

Раздел 1 към анекс С : Абревиатури, използвани в този документ

(Tab 1 to Annex C Abbreviations)

(б.а. - най-малко 80% от тях бяха обяснени с нарочни текстове в документа, поради което си позволявам да ги представя само в оригинал)

ALC – Accounting Legend Code
CAO – Cryptographic Assurance Office
CCI – Controlled Cryptographic Item
CDMA – Carrier Demand Multiple Access
CF – Central Facility
CIK – Crypto Ignition Key
CMCS – COMSEC Material Control System
CNSSI – Committee on National Security Systems Instruction
COMSEC – Communication Security
COR – Central Office of Record
CTTA – Certified TEMPEST Technical Authority
DAO – Department/Agency/Organization
DCD – Defense Courier Division
DCS – Defense Courier Service
DHS – Department of Homeland Security
DIAS – Distributed INFOSEC Accounting System
DOD – Department of Defense
DoDAAC – Department of Defense Activity Address Code
DSS – Defense Security Service
DTD – Data Transfer Device
ECC – Enhanced Cryptographic Card
EKMS CF – Electronic KeyManagement System Central Facility
FAQ – Frequently Asked Question(s)
FCL – Facility Clearance Level
FSO – Facility Security Officer
GSA – General Services Administration
GSM – Global System for Mobile Communications
HAIPE – High Assurance Internet Protocol Encryption
IA – Information Assurance
IAD – Information Assurance Directorate
INFOSEC – Information Systems Security
IPv4 – Internet Protocol, version 4
IPv6 – Internet Protocol, version 6
ISDN – Integrated Services Digital Network
ISM – Iridium Secure Module
KMI – KeyManagement Infrastructure
KMID – KeyManagement Identification
MSS – Mobile Subscriber Service
NATO – North Atlantic Treaty Organization
NSA – National Security Agency
NSTISSI – National Security Telecommunications and Information Systems Security Instruction
OCONUS – Outside the Continental United States
PCMCIA – Personal Computer Memory Card International Association
PDA – Portable Data Assistant
PIN – Personal Identification Number

PSTN – Public Switched Telephone Network
SBU – Sensitive but Unclassified
SCI – Sensitive Compartmented Information
SCIF – Sensitive Compartmented Information Facility
SCIP – Secure Communications Interoperability Protocol (Formerly FNBDT)
SDNS – Secure Data Network System
SGSM – Secure Global System for Mobile Communications
SME PED – Secure Mobile Environment Portable Electronic Device
STE – Secure Terminal Equipment
SVoIP – Secure Voice over Internet Protocol
T1DSW – Type 1 Default Software
TA – Terminal Administrator
TPA – Terminal Privilege Authority
TRI/TAC – Tri-Service Tactical Communications System
TS/SCI – TOP SECRET Sensitive Compartmented Information
UPV – User Privilege Vector
VoIP – Voice over Internet Protocol

Tab 2 to Annex C
Secure Telephone User Briefing

Annex D Electronic Key Management System (EKMS) / Key Management Infrastructure (KMI)

(Приложение D
Електронна система за управление на ключове (EKMS) / Инфраструктура за управление на ключове (KMI))

Tab 1 to Annex D
Local Management Device/Key Processor (LMD/KP) Management

Раздел 1 към Приложение D Управление на локално устройство / ключов процесор (LMD / KP)

Tab 2 to Annex D
COMSEC Accounting, Reporting, and Distribution System (CARDS) Management

Раздел 2 към Приложение D
Управление на акаунти, отчитането и дистрибуцията на COMSEC (CARDS)

Annex E
Cryptographic High Value Products (CHVP)

Приложение E
Криптографски продукти с висока стойност (CHVP)

Annex F
COMSEC Account Checklists

Приложение F
Контролни списъци на акаунти на COMSEC

Tab 1 to Annex F COMSEC Audit Checklist
Department of Homeland Security
COMSEC Central Office of Record (COR)
COMSEC AUDIT CHECKLIST

Раздел 1 към Приложение F

Контролен списък на COMSEC
Департамент за вътрешна сигурност
Централен офис на регистъра на COMSEC (COR)
ЧЕКЛИСТ за КОМСЕК ОДИТ (*б.а. – изключително подробен, разработен за бърза работа на около 10 страници*)

Tab 2 to Annex F Electronic Key Management System (EKMS) Checklist

Раздел 2 към Контролния списък на системата за управление на електронни ключове (EKMS) от приложение F

Tab 3 to Annex F Account Establishment Checklist

Раздел 3 към Приложение F Контролен списък за създаване на акаунти

Tab 4 to Annex F Account Disestablishment Checklist

Раздел 4 към Приложение F Контролен списък за закриване на акаунт

Annex G COMSEC Forms and Templates

Приложение G Форми и шаблони на COMSEC

Tab 1 to Annex G STE Installation / History Record

Раздел 1 към Приложение G STE Инсталация / история на записа

Tab 2 to Annex G COMSEC Personnel Nomination Letter Template and Worksheet

Раздел 2 към Приложение G Шаблон и работен лист за номинация на персонала на COMSEC

Tab 3 to Annex G Electronic Fill Device Audit Trail Review Log

Раздел 3 към Приложение G Журнал за преглед на проверка на електронните устройства за зареждане

Tab 4 to Annex G SF 700 Tamper Check Log

Раздел 4 към Приложение G SF 700 Журнал за проверка на подправки

Tab 5 to Annex G Access List Template

Раздел 5 към Приложение G Шаблон на списъка за достъп

Име на автора: Иво Великов Великов
Месторабота: Член на Държавна комисия по сигурността на информацията, експерт и изследовател в областта на сигурността.
e-mail: manoflight@abv.bg

INTERNET OF THINGS (IOT) DESIGN

DRAGOMIR I. VASILEV

ABSTRACT: *The Internet of Things system begins with the simplest sensors located at the farthest reaches of space and the transformation of analog physical actions into digital signals. The advantage of IoT is that it is not just a single sensor signal, but a sum of signals from hundreds, thousands, maybe millions of sensors, points and devices. This report includes the identification of Core Segments of IoT, IoT vs. Machine-to-Machine Communication (M2M), Network Utility. Law of Metcalfe and Beckstrom, IoT architecture.*

KEYWORDS: *IoT, M2M, IoT architecture, Network Utility.*

ПРОЕКТИРАНЕ НА ИНТЕРНЕТ НА НЕЩАТА (IOT)

ДРАГОМИР И. ВАСИЛЕВ

АБСТРАКТ: *Системата на Интернет на нещата започва с най-простите сензори, разположени в най-отдалечените краища на пространството и трансформирането на аналоговите физически действия в цифрови сигнали. Предимството на IoT е в това, че не е просто единичен сигнал от сензор, а сума сигнали от стотици, хиляди, може би милиони сензори, точки и устройства.*

Освен, че ще се спрем на архитектурата на IoT, също ще определим ролята на архитекта (проектанта) в изграждането на перспективна, сигурна и мащабна архитектура на IoT. За да направи това, архитектът трябва да може ясно да формулира как проектът ще бъде от полза за клиента, анализирайки всички необходими технологични и бизнес процеси. Архитектът също така трябва да може да решава инженерни и спомагателни проблеми, маневрирайки между възможните варианти за изпълнение на проекта.

Тази индустрия активно използва множеството устройства, софтуер и услуги, които IoT предлага. На практика всяка голяма технологична компания инвестира или е инвестирала в Интернет на нещата. Вече са се формирали нови пазари и технологии (и някои от тях са успели да се провалят или са били препродадени) [5].

Основни сегменти на IoT:

- *Сензори* – цялостно разработени системи, специализирани системи за наблюдение в реално време, непрекъсваеми захранвания, микроелектромеханични системи;
- *Връзка между сензорите* - зоната на покритие на безжичните персонални мрежи е 0 - 100 м. За обмен на данни между сензорите се използват нискоскоростни информационни канали с ниска мощност, които основно не са изградени на база IP протокол;
- *Локални мрежи* - обикновено това са IP-базирани системи за обмен на данни, например 802.11 Wi-Fi мрежа за бърза радиокомуникация, често peer-to-peer или мрежи звезда;
- *Агрегатори, рутери, шлюзове* – цялостни системи с компоненти съобразени с бюджета, включващи: процесори, памети и система за съхранение. Могат да

бъдат модули, пасивни компоненти, тънки клиенти, клетъчни и безжични радио системи, софтуер, инфраструктура за изчисляване, инструменти за анализ, защита на крайни устройства, системи за управление на сертификати;

- *Цялостно мрежово решение* - клетъчни оператори, сателитни оператори, оператори на глобални мрежи с ниска мощност (Low Power Wide-Area Network, LPWAN). Обичайно се използва транспортен протокол за IoT и мрежови устройства (MQTT, CoAP и дори HTTP);
- *Облак* – доставчик на услуги: инфраструктура, платформа, поддръжка на бази данни, стрийминг и пакетни услуги, инструменти за анализ на данни, софтуер, SDN / SDP оператори;
- *Анализ на данни* - огромни количества информация се прехвърля в облака. Работата с големи количества данни и получаването на стойност от тях е задача, която изисква сложна обработка на събития, анализи;
- *Сигурност* - когато всички части на архитектурата се обединят, възникват проблеми със сигурността. Безопасността се отнася до всеки компонент: от физически сензори до процесори и хардуер, радио системи и самите комуникационни протоколи. На всяко ниво трябва да се осигури сигурност, надеждност и цялост. В тази верига не трябва да има слаби звена, тъй като IoT се превръща в основната цел за злонамерени атаки.

Такава разработена екосистема включва специалисти от различни технически области, като разработчици на устройства (проектиращи нови видове сензори и захранвания), програмисти, мрежови инженери, специалисти по обработка на данни, DevOps инженери. IoT винаги ще се нуждае и от доставчици на услуги като изпълнители на проекти, системни интегратори, доставчици на системи и OEM производители [2], [7].

IoT срещу комуникацията машина – машина (M2M)

Технологиите на комуникация M2M и IoT са много сходни по своята същност, но има значителна разлика:

M2M - обща концепция за комуникация на едно самостоятелно устройство с друго самостоятелно устройството. Комуникацията е директна. Автономията се отнася до способността на възела да създава и да предава информация на друг възел без човешка намеса. Формата на предаване на данни може да бъде различна. Често се случва специализираната функционалност за пренос на информация да не е интегрирана в устройството M2M. Това веднага измества типичните устройства за интернет достъп, който редовно се използва за работа с облачни услуги и съхранение. В M2M система обменът на данни може да се извършва и без участието на IP протокол - например чрез сериен порт или потребителски протокол;

IoT - IoT системите могат да съдържат няколко M2M възли (например Bluetooth Mesh мрежа, която осъществява обмен на данни без участието на IP протокола), но данните се агрегират в крайния рутер или шлюз. Крайно устройство служи като точка за влизане в Интернет. Или някои сензори с по-голяма процесорна мощност могат сами да се свързват в мрежовия слой на Интернет. Независимо къде се осъществява достъпът до Интернет, отличителният белег на IoT системата е, че тя винаги е свързана с интернет по един или друг начин.

Чрез преместване на данни от сензори, крайни и интелигентни устройства в Интернет става възможно свързването на най-простите устройства към утвърдения свят на облачните

услуги. Преди облакът и мобилните комуникации да станат част от ежедневната реалност, най-простите сензори и вградени системи нямаха начин да изпращат данни до други устройства за секунди, да съхраняват информация толкова дълго, колкото искате, и да анализират данните, за да идентифицират тенденциите и моделите [3], [6].

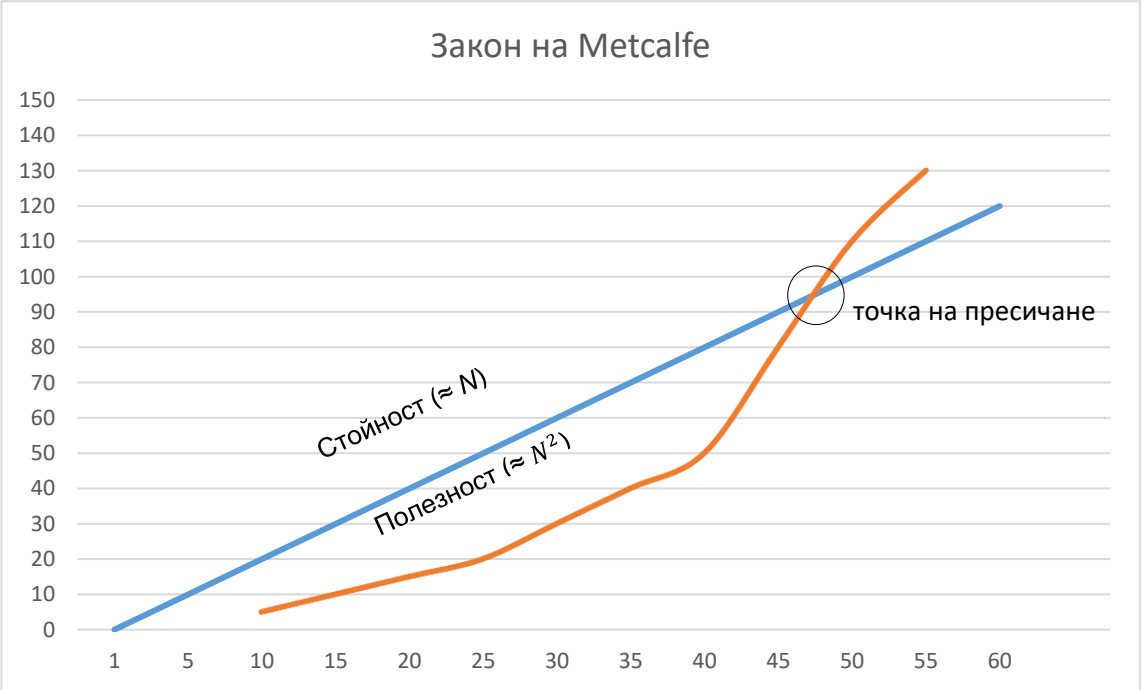
Полезността на мрежата. Закон на Metcalfe и Beckstrom

Традиционно полезността на мрежата се изчислява в съответствие със закона на Metcalfe. През 1980 г. Robert Metcalfe формулира идеята, че полезността на която и да е мрежа е пропорционална на квадрата на броя потребители на системата. Що се отнася до IoT, сензорите или крайните устройства могат да се възприемат като потребители. Като цяло законът на Metcalfe се изразява със следната формула:

(1) $$V \infty N^2$$

където: V – полезност на мрежата; N – количество потребители в мрежата.

Графично формулата е представена на фиг. 1, като показва точка на пресичане, маркираща прага, над който може да се очаква възвръщаемост на инвестицията (положителна възвръщаемост на инвестициите).



Фиг. 1 Закон на Metcalfe

Законът на Metcalfe не взема предвид влошаването на качеството на комуникацията, което може да се дължи на увеличаване на броя на потребителите и/или обема на данните, като същевременно се запазва първоначалната честотна лента на мрежата. Също така законът на Metcalfe не взема предвид разликите в нивата на мрежовите услуги, ненадеждната инфраструктура (например 4G LTE комуникации в движещо се превозно средство) или неблагоприятните фактори, влияещи върху производителността на мрежата (например DoS атаки).

За да се коригират тези обстоятелства, се прилага закона на Beckstrom:

$$\sum_{i=1}^{n} V_{i,j} = \sum_{i=1}^{n} \sum_{k=1}^{m} \frac{B_{i,j,k} - C_{i,j,k}}{(1+r_k)^{t_k}}, \quad (2)$$

където: $V_{i,j}$ - полезност на мрежата j за устройство i в даден момент от време;

i – отделен потребител или устройство;

j – самата мрежа; k - единична транзакция;

$B_{i,j,k}$ – преимущество, което транзакция k дава на устройството i в мрежата j;

$C_{i,j,k}$ – стойност на транзакцията k за устройството i в мрежа j;

r_k – стойност на отстъпката в момента на транзакция k;

t_k – изминалото време за транзакция k;

n – количество на ползвателите;

m – количество на транзакциите.

Според закона на Beckstrom, за да изчислим полезността на мрежата (например IoT решение), трябва да оценим всички транзакции от всяко устройство и да сумираме тяхната полезност. Ако мрежа j по някаква причина се провали, колко ще струва на потребителя? Най-трудната част от това уравнение за изчисляване на показателя B. Ако разглеждаме всеки IoT сензор поотделно, стойността на този параметър може да бъде много малка и незначителна (например, температурният индикатор на дадено устройство не е предавал данни за един час). В други случаи тази стойност може да бъде много значителна (например батерията на сензора за вода се е изтощила и складът на магазина е бил наводнен, което е довело до големи разходи и увеличение на разходите за застраховка).

Когато разработва IoT решения, първото нещо, което архитектът трябва да направи, е да разбере каква ще е ползата от проекта. В най-лошия случай IoT системата се превръща във финансова тежест и носи само загуби за клиента.

IoT архитектура

IoT архитектурата обхваща много технологии.

Всеки архитект трябва да разбере какво въздействие ще има избраното дизайнерско решение върху цялата система като цяло и всяка от нейните части поотделно. Сложността и гъвкавостта на IoT се дължи на факта, че тази технология е много по-сложна от традиционните технологии: тя се отличава не само с големия си мащаб, но и с комбинация от различни, често несвързани видове архитектура. Броят на възможните дизайнерски решения е невероятен. Например в момента в света има повече от 700 доставчици на IoT, предлагащи облачно съхранение, SaaS компоненти, IoT системи за управление, IoT системи за сигурност и всякакъв вид анализ на данни. Също така има и огромен брой различни протоколи от лични, локални и глобални мрежи, които непрекъснато се променят и адаптират в зависимост от региона [1], [4].

Изборът на грешен PAN протокол може да доведе до проблеми с комуникацията и забележимо ниско качество на сигнала, като ситуацията може да се поправи само, чрез добавяне на повече възли към мрежата. Архитектът трябва да вземе предвид намесата в локални и глобални мрежи: как се събират данни от крайни устройства и се предават в Интернет, да оцени устойчивостта на системата и разходите за потенциална загуба на данни [6], [8], [9].

Архитектът също трябва да избере интернет протоколите: MQTT или CoAP и AMQP - и също така трябва да помисли как всичко това ще работи в случай на преход към друга облачна услуга. Също така трябва да реши в кой момент данните ще бъдат обработени. На този етап може да се предпочете обработка на данни в близост до източника, което решава проблема със закъснението, и което е по-важно позволява да се намали натоварването на мрежата и разходите при прехвърляне на данни през WAN и облачни услуги. След това да се разглеждат всички възможности за анализ на получените данни. Неподходящ инструмент за анализ може да претовари система с излишни данни или да наложи използване на алгоритми, които са твърде изчислително интензивни, за да се изпълняват в крайни възли. Как заявките от облака към сензора ще повлияят на работата на батерията на самия сензор. В допълнение към цялата тази широка гама от възможни опции, не трябва се забравя и за системата за сигурност, тъй като създадената IoT система се превръща в най-голямата цел за атаки. Както виждаме изборът е огромен и всяко решение засяга останалите.

ЛИТЕРАТУРА:

[1] Николов, Н.Р., Цанков, Ц.С. Хардуерна реализация на генератор на псевдослучайни последователности описван с полином от 1024 степен и програмно управление на обратните връзки. Научна сесия на факултет „Артилерия, ПВО и КИС“, Шумен, ISSN 1313-7433 (2010).

[2] Петров, Ю. Алгоритъм за определяне и анализ на точните и приближени амплитудно-честотни и фазочестотни характеристики на трептящи кръгове. Научна конференция TechCo, Ловеч, ISSN 2535-079X (2019).

[3] Петров, Ю. Един алгоритъм за определяне на практическата ширина на спектъра на непериодични сигнали. Научна конференция TechCo, Ловеч, ISSN 2535-079X (2019).

[4] Boyer, S. SCADA: Supervisory Control and Data Acquisition, ISA — The Instrumentation, Systems, and Automation Society, Triangle Park, NC, U.S.A. (1999).

[5] Bedzhev, B., Nikolov, N., Tsankov, Ts. Training artificial immune system using “good” paths for synthesis of signals with optimal autocorrelation properties. Scientific Conference with international participation MATTEX 2018 (2018).

[6] Iliev, M.P., Nikolov, N.R., Tsankov, T.S. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Journal "Electrotechnica & Electronica", Vol. 46, ISSN 0861-4717 (2011).

[7] Mazadzhiev, G.N., Evlogiev, S.S., Atanasov, V.T. Conceptual model of smart home mobile technological system. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2019, Collection of papers, ISSN 2367-7902 (2019).

[8] Sharma, R., Stearns, B., and Ng, T. J2EE(TM) Connector Architecture and Enterprise Application Integration, Pearson Education, Harlow, U.S.A. (2001).

[9] Rao, A.S. and Georgeff, M.P. An Abstract Architecture for Rational Agents, in Proceedings of Knowledge Representation and Reasoning KR&R-92 (1992).

Име на автора: Драгомир Иванов Василев, гл. ас., д-р
Кат. ККТ, ФТН на Шуменски университет „Епископ Константин Преславски“
E-mail: d.vasilev@shu.bg

THE ROLE OF THE ARCHITECT IN DESIGN THE INTERNET OF THINGS (IOT)

DRAGOMIR I. VASILEV

ABSTRACT: *The architect term is often used in technical disciplines. There are software architects, system architects and solution architects. These are people who are well versed in these fields, professionals in their field. These vertical subject areas intersect with a large number of horizontal technologies. Every architect must be familiar with the theoretical aspects in order to understand how an IoT system is formed. At some point, pure theory, such as information and communication theory, must be resorted to. In other cases, it will be necessary to look for a link between the IoT and other related technologies.*

KEYWORDS: *IoT, IoT architect, Network Utility.*

РОЛЯТА НА АРХИТЕКТА ПРИ ПРОЕКТИРАНЕТО НА ИНТЕРНЕТ НА НЕЩАТА (IOT)

ДРАГОМИР И. ВАСИЛЕВ

АБСТРАКТ: *Терминът архитект често се използва в техническите дисциплини. Съществуват софтуерни архитекти, системни архитекти и архитекти на решения. Дори в тесни области, като компютърни науки и програмиране, има специалности, чиито имена звучат като SaaS архитект, архитект облачни решения, архитект интелигентни решения и др. Това са хора, които са добре запознати и професионалисти в своята област. Тези вертикални предметни области се пресичат с голям брой хоризонтални технологии. Всеки архитект трябва да е запознат с теоретичните аспекти, за да разбере как се формира една IoT система. В някои моменти трябва да се прибегне до чиста теория, например теорията на информацията и комуникацията. В други случаи ще налага да се търси връзка на IoT с други свързани технологии. Всеки един архитект на IoT трябва да има минимум базови познания относно.*

1. Сензори и захранване

Интернет започва или завършва с едно събитие: просто движение, промяна в температурата или някакво действие. За разлика от много съществуващи ИТ устройства, IoT се отнася най-вече до физическо действие или събитие. Той дава реакция на някакъв фактор в реалния свят. Понякога един датчик може да генерира огромно количество данни, например акустичен сензор за рутинна проверка на оборудването. В други случаи само един бит данни е достатъчен, за да предаде жизненоважна информация за здравето на пациента. Каквато и да е ситуацията, сензорните системи са се развили и свили до субнанометрични размери, като са станали и доста по евтини.

Основно изискване е архитектът да определи система от сензори и датчици, която да замести обичайните стандарти за свързване между устройствата и контролерите. Връзката между устройства и контролните функции да е оптимална като цена, качество и да позволява връзка с друга по спецификация комуникационна техника. Достъпът до данните от мрежата трябва да бъде стандартизирана а местоположението на устройствата да бъде достъпен за потребителя. Системата трябва да бъде изградена така, че да отговаря на

необходимите изисквания за надеждност, като се използват едни и същи основни компоненти.

Архитектът трябва да анализира потоците от данни и функциите на полевите устройства и контролното оборудване с цел идентифициране на специални нужди на потребителя. Обменените данни идващ от сензорите към контролното оборудване в по голямата си част са известни и идентифицирани (температура, налягане, скорост, позиция и т.н.), но други данни не се идентифицират и не са известни но трябва да се предават и анализират заедно с обичайните съобщения [4], [5], [11].

Проектирани специално за сферата на Интернет на нещата (IoT), технологиите LPWA са оптимизирани за употреба в евтини устройства, които трябва да прехвърлят малки количества данни. Целта типично е да се дава евтина и енергийно ефективна свързаност на голям брой уреди в малка географска област. Подобни устройства включват сензори, които могат да следят градска инфраструктура, екологични условия, мобилни активи и вериги за доставки, както и измервателни уреди за електроенергия, газ и вода. Тези уреди изпращат регулярно показания или превключват други механизми при настъпване на дадени събития, дефинирани от потребителя (като достигната температура или замърсяване на въздуха). При технологиите LPWA също има два типа, като стандартизираните използват лицензионен честотен спектър, плащан най-често от телеком операторите, и частни мрежи, които оперират в нелицензния спектър. Частните LPWA технологии като Sigfox или LoRa, вече се използват за свързване на сензори и други IoT устройства. Тъй като не преминават през стандартизиращи процеси и затова стигат по-бързо до пазара. Те обаче са доста уязвими по-отношение на интерферентни въздействия от другите радиосигнали, използващи същите блокове в нелицензния спектър. Освен това се поддържат от малко производители и обикновено няма международен роуминг, което е сериозна пречка пред широкото им разпространение.

Стандартизираните LPWA технологии, включват 3 нови варианта - NB-IoT, LTE-M и EC-GSM-IoT, стандартизирани от 3GPP за работа в лицензния спектър. Мобилни оператори от целия свят адаптират клетъчните си мрежи за поддръжка на тези технологии. Те използват съществуващата инфраструктура на операторите, но са създадени да предоставят по-добро покритие от традиционните клетъчни услуги. Първите тестове показват, че съвместимите с 3GPP, 4G а вече и 5G технологии, LPWA могат да предоставят свързаност на труднодостъпни места като подземни обекти (паркинги, мазета, гаражи) и работни помещения в центъра на огромни сгради. Освен това употребата на лицензен радиоспектър означава, че няма интерференции, а това води до по-високо качество на услугата и по-голяма надеждност [6], [9].

В частност NB-IoT и EC-GSM-IoT са оптимизирани да пренос на кратки съобщения, с дължината на един SMS. Тези технологии разчитат на мащаба и поддръжката на добре разработените клетъчни екосистеми, т.е. решенията ще се предлагат от голям брой производители в целия свят. В резултат коли, смарт часовници, фитнес гривни и други мобилни устройства ще останат свързани и след пресичане на границите, а производителите им ще успеят да доставят свързани продукти в огромен, международен мащаб.

Стандартизираните технологии обещават икономии от мащаба и при разгръщане на голям брой свързани сензори в относително малки райони като ферми или индустриални предприятия. Технологиите LPWA в лицензния спектър се възползват и от изградените от мобилните оператори системи за сигурност и контрол от край до край над свързаността. Операторите могат да предоставят защитена свързаност и поддръжка на автентификация, подходяща именно за IoT областта.

Прогнозите сочат, че милиарди устройства ще бъдат свързани към Интернет на нещата. Голямо разпространение имат Microelectromechanical systems (MEMS), сензори и други видове евтини крайни устройства и техните електрофизични свойства. Не на последно място трябва да се обърне внимание на захранващи и енергийни системи са необходими за захранването на тези крайни устройства. Не може да се приеме, че крайните устройствата се захранват по подразбиране. Милиарди малки сензори все още се нуждаят от много енергия. В някои случаи на минимални безобидни промени в облачната услуга могат да повлияят коренно на цялата енергийна архитектура на системата като цяло.

2. Предаване на данни

IoT не може да съществува без надеждни технологии за предаване на данни от най-отдалечените и труднодостъпни райони до най-големите центрове за данни, като Google, Amazon, Microsoft и IBM и др. Фразата „Интернет на нещата“ съдържа думата „Интернет“, така, че основните дейности са свързани с работата в мрежа, обмена на данни и дори теорията на сигнализирането. Основният стълб на Интернет на нещата не са сензори или приложения, а свързаността. Успешният архитект разбира всички сложности на свързването на компонентите с WAN и обратно.

Предаването на данни и мрежовата връзка започва с теоретичните аспекти и математическите основи на комуникацията и работата с информация. Успешните архитекти ще се нуждаят от инструменти за обучение и модели - не толкова, за да разберат защо определени протоколи не са много ефективни, а за да проектират бъдещи системи, които могат да се разширяват за достигане мащабите, необходим за IoT. Тези инструменти включват динамичните характеристики на радиосигнала като анализ на спектъра и мощността, съотношение сигнал/шум, загуба на траекторията и смущения. Тази част също така подробно описва основите на теорията на информацията и ограниченията, които влияят върху общата производителност и качеството на предаването на данните.

Спектърът на безжичния сигнал също не е неограничен и се разпределя между няколко устройства, а архитектът, разработващ мащабна IoT система, трябва да разбере как ще се разпределя спектърът [1], [8].

Предаването на данни и установяването на мрежова връзка се основава предимно на комуникационни системи с малък обсег - лични мрежи (PAN), изградени без спазване на правилата на IP протоколите. Като пример за разнообразие личните мрежи (PAN) включват Bluetooth 5, Zigbee и Z-Wave, Освен тях се използват и безжични LAN и IP-базирани комуникационни системи, включително широка гама от Wi-Fi мрежи, базирани на IEEE 802.11, 6LoWPAN и Thread технология. Все повече се използват и нововъзникващите Wi-Fi стандарти като 802.11p за транспортиране на информация между превозните средства. Комуникации на дълги разстояния, базирани на клетъчни стандарти (4G LTE), нововъзникващите IoT и стандартите M2M, като Cat-1 и Cat-NB. Не бива да се пропускат и най-обещаващите свойства на 5G стандарта, който се разработва, за да подготви архитекта за планираното увеличаване на обхвата на сигнала, както и върху факта, че всяко устройство ще използва тесен честотен диапазон. Напълно различен тип архитектура може да се покаже и чрез протоколи LoRaWAN и Sigfox.

3. Интернет маршрутизация и протоколи

За предаването на данни от сензори в Интернет са необходими две технологии: рутер-маршрутизатор и интернет протоколи, които осигуряват ефективността на предаването на данни. Рутерът е особено важен в аспекти като сигурност, управление и посока на данните.

Edge рутерите управляват и наблюдават състоянието на съответните mesh - мрежи, а също така подравняват и поддържат качеството на данните. Също така от голямо значение е поверителността и сигурността на данните. Тази част обяснява ролята на рутера при създаването на VPN, VLAN и софтуерно дефинирани WAN. Те могат буквално да съдържат хиляди възли, обслужвани от един Edge рутер, и до известна степен да служи като увеличаване покритието на облака. IoT отваря път за нови протоколи, които са наравно с традиционните HTTP и SNMP протоколи използвани от няколко десетилетия. IoT трансферът на данни изисква ефективни протоколи с ниска латентност, които могат лесно и сигурно да предават данни към и от облака. Такива могат да бъдат и MQTT, AMPQ и CoAP.

4. Изчисления и анализ на данни

На този етап архитектът трябва да реши какво да правите с потока от данни, влизащ в облачната услуга от крайния възел, например при различните аспекти на облачната архитектура (модели SaaS, IaaS и PaaS). Архитектът трябва да разбере какво представлява потокът от данни и какви са типичните облачни услуги. Приемайки OpenStack като модел на облачна система се разглеждат различни компоненти: от модули Ingestor до масиви с данни и инструменти за анализ, за да се научи как правилно да преценява системата развитието и растежа и, необходимо е да разбере всички тънкости и сложности на архитектурата на облачните системи. Архитектът също трябва да разбере как латентността влияе върху системата на IoT. Освен това не е необходимо всичко да се изпраща в облака. Преместването на всички IoT данни е значително по-скъпо от обработката им на ръба на мрежата или включването на крайния рутер в зона, обслужвана от облачна услуга, така наречените OpenFog стандарти.

Данните, получени чрез преобразуване на аналогов физически стимул в цифров сигнал, могат да бъдат много тежки. Тук влизат в действие системният анализ на IoT и процесорите на правила. Сложността на въвеждане на IoT система в експлоатация зависи от решението, което се проектира. Друга пример е, че огромно количество структурирани и неструктурирани данни се предават в реално време към облак, което изисква висока скорост на обработка (за прогнозна аналитика) и дългосрочно прогнозиране, основано на високотехнологични модели, сложни манипулатори на събития и формирането на невронни мрежи [2], [3].

5. Заплаха и сигурност в IoT

Много IoT системи не са ограничени до сигурното пространство на дом или офис. Те са разположени на обществени места, в много отдалечени райони, в движещи се превозни средства. IoT е огромна основна цел за всички видове злонамерени атаки. Свидетели сме на безкраен набор от прицелни IoT атаки, добре подредени хакове и дори пробиви в сигурността в цялата страна. Всеки архитект трябва да е наясно със спецификите на тези уязвимости и как те могат да бъдат премахнати, ако иска да въведе лична или корпоративна IoT система. Подготвят се много законопроекти, като мярка за гарантиране на сигурността на IoT, стимулите и възможните последици от подобна стъпка от страна на законодателя.

Архитектът трябва да разбере как се преплитат тези много различни технически дисциплини, необходими за създаване на цялостна, оптимизирана система с потенциал за разширяване. Освен това архитектът трябва да може да докаже, че IoT системата носи добавена стойност за крайния потребител или клиент [7].

ЛИТЕРАТУРА:

[1] Николов, Н.Р., Цанков, Ц.С. Хардуерна реализация на генератор на псевдослучайни последователности описван с полином от 1024 степен и програмно управление на обратните връзки. Научна сесия на факултет „Артилерия, ПВО и КИС“, Шумен, ISSN 1313-7433 (2010).

[2] Петров, Ю. Алгоритъм за определяне и анализ на точните и приближени амплитудно-честотни и фазочестотни характеристики на трептящи кръгове. Научна конференция TechCo, Ловеч, ISSN 2535-079X (2019).

[3] Петров, Ю. Един алгоритъм за определяне на практическата ширина на спектъра на непериодични сигнали. Научна конференция TechCo, Ловеч, ISSN 2535-079X (2019).

[4] Станева, Л.А., Цанков, Ц.С. Компютърна лаборатория за синтез на сложни дискретно честотни сигнали. Научна конференция MATTEX 2012, Шумен, ISSN 1314-3921 (2012).

[5] Boyer, S. SCADA: Supervisory Control and Data Acquisition, ISA — The Instrumentation, Systems, and Automation Society, Triangle Park, NC, U.S.A. (1999).

[6] Bedzhev, B., Nikolov, N., Tsankov, Ts. Training artificial immune system using “good” paths for synthesis of signals with optimal autocorrelation properties. Scientific Conference with international participation MATTEX 2018 (2018).

[7] Iliev, M.P., Nikolov, N.R., Tsankov, T.S. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Journal "Electrotechnica & Electronica", Vol. 46, ISSN 0861-4717 (2011).

[8] Mazadzhiev, G.N., Evlogiev, S.S., Atanasov, V.T. Conceptual model of smart home mobile technological system. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2019, Collection of papers, ISSN 2367-7902 (2019).

[9] Sharma, R., Stearns, B., and Ng, T. J2EE(TM) Connector Architecture and Enterprise Application Integration, Pearson Education, Harlow, U.S.A. (2001).

[10] Tsankov, T., Trifonov, T., Staneva, L. An algorithm for synthesis of phase manipulated signals with high structural complexity. Journal Scientific & Applied Research, Vol. 4, ISSN 1314-6289 (2013).

[11] Rao, A.S. and Georgeff, M.P. An Abstract Architecture for Rational Agents, in Proceedings of Knowledge Representation and Reasoning KR&R-92 (1992).

Име на автора: Драгомир Иванов Василев, гл. ас., д-р
Кат. ККТ, ФТН на Шуменски университет „Епископ Константин Преславски“
E-mail: d.vasilev@shu.bg

XCPU SIMULATOR AS A LEARNING APP

VALENTIN T. ATANASOV, LINKO G. NIKOLOV

ABSTRACT: *This publication represents an implementation of a Web-based application with integration of a student model for the purposes of a digitally based learning process. Approaches for synthesis of component models, intended for simulations of the processor work, based on CISC architecture, are presented. The presented approach for instruction encoding allows a wide range of code segments that would contribute to a better understanding of the operation of the processor unit by the students. The implementation of the application follows the perceptions of the so-called highly-interactive generation, which circumstance would lead to higher efficiency of the learning process.*

KEYWORDS: *CPU, simulation, processor, registers, digital based learning, highly-interactive generation, digital learning model.*

XCPU СИМУЛАТОР КАТО ОБУЧАВАЩО ПРИЛОЖЕНИЕ

ВАЛЕНТИН Т. АТАНАСОВ, ЛИНКО Г. НИКОЛОВ

АБСТРАКТ: *Настоящата публикация представя една реализация на Уеб базирано приложение с интеграция на модел на обучавания за целите на цифрово базиран учебен процес. Изложени са подходи за синтез на компонентни модели, предназначени за симулации на процесорна обработка, базирана на CISC архитектурен набор от инструкции. Представеният подход за кодиране на инструкции позволява широк кръг от кодови отрязъци, които биха допринесли за по-доброто разбиране работата на процесорното устройство от страна на обучаваните. Реализацията на приложението следва възприятията на т.н. високоинтерактивно поколение, което обстоятелство би довело до по.висока ефективност на процеса на обучение.*

1 Въведение

Приети термини и постановки

Следвайки принципите и подходите, представени в кръг от проучвания, изложени в редица предишни публикации [1], [4], [5], [6], [7], разглеждащи обучаващите приложения в цифрово базиран учебен процес, за целите на настоящото проучване се приемат следните основни постановки и термини:

- Дадено ИКТ базирано програмно средство, използващо дидактическа методология, с дефинирана педагогическа цел в дадена научна област или области, може да бъде определено като обучаващо приложение;
- Устойчива времево-доминираща интерактивна технологична среда на индивида, получаващ, изменящ, съхраняващ и споделящ информация с използването на цифрови технологии може да бъде определена като пълно високотехнологично обкръжение (ПВТО);
- Социално обособена общност, в среда на ПВТО [8], може да бъде определена като високоинтерактивно поколение.

ПВТО установява една преносима и повсеместна точка на достъп до глобалната мрежа. Поради способността на мозъка за невропластичност и формираните у

високоинтерактивното поколение нови умения и начини за взаимодействие с околния свят, водещо до трайни неврокогнитивни промени в кортикалните области на мозъка [9], свързани със сензорната и двигателна дейност се дефинира отличителната характеристика на това на високоинтерактивното поколение.

2 Проблемни страни на съществуващите цифрови реализации на учебен процес и възможно решение.

В среда на Уеб са представени редица решения, предлагащи симулации на централен процесор (ЦП) [11][12][13][14]. В определена степен предоставените функционалности на тези решения биха били ценен инструмент за развойни центрове, научни лаборатории и изследователски трудове, при все по-растящите изисквания към симулацията като метод [14], но стои въпросът в каква степен тези решения биха удовлетворили постигането на педагогическата цел на преподавателя, включил ги в набора от свои обучаващи приложения. С оглед на дидактическия принцип, на който се основава разбирането за обучаващо приложение в сферата на образованието, следва водеща характеристика да бъде интегрираният дидактически модел и модела на обучавания. В цитираните по-горе Уеб базирани решения за симулации отсъстват или не са представен експлицитно тези модели, което обстоятелство не обуславя ефективното постигане на педагогическата цел на процеса на обучение. Друга констатация от настоящото проучване бе недостатъчния набор от предлагани технологични Уеб базирани решения за симулация на ЦП в архитектури с разширен набор от инструкции (CISC), който набор да даде солидна емпирична основа за изследвания за използването на обучаващи приложения от този клас в образователната сфера.

Въз основа на горните постановки и характеристика инициирахме междууниверситетски проект за разработване на Уеб базиран дидактически инструмент за обучение в предметни дисциплини, изследващи организацията на компютъра чрез опростена симулация на основните принципи, залегнали в централния процесор, условно обозначен в проекта като xCPU, от т.н. CISC архитектури.

3 Концептуализация на реален учебен процес. Модел.Разработка.

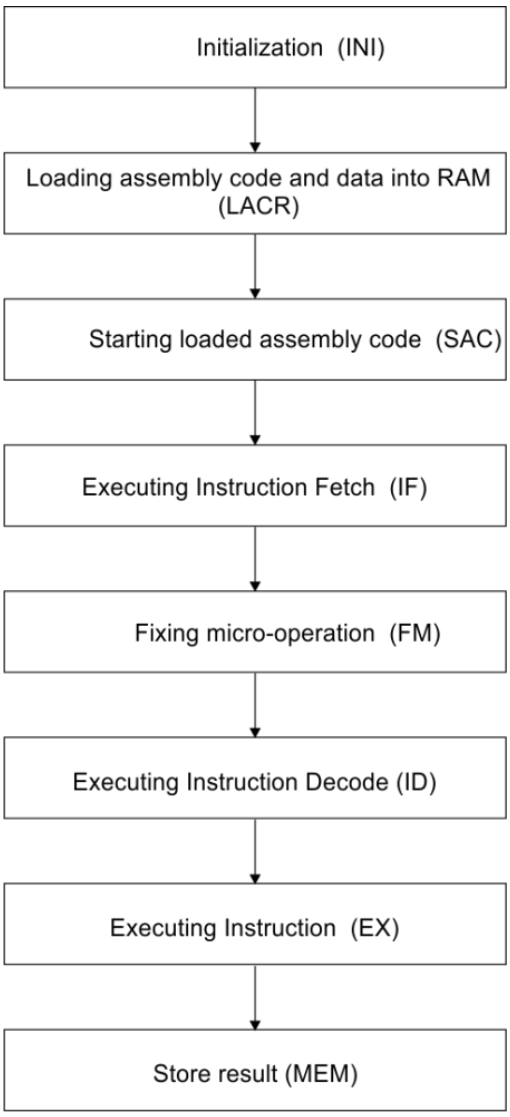
Проектът стартира, дефинирайки своите етапи в съответствие с установената добра практика на софтуерна разработка на приложения [14], [15]. Основната цел, формулирана от екипа, бе да се акцентира върху процеса, а не върху конкретна архитектура, за да не се изпадне в ограниченията на специфичното инженерно пространство на дадена архитектура, реализирайки предоставянето на знание, обхващащо принципите на работа на симулирания процесор. По тази причина не се разглеждат въпроси като производителност, оптимизация, конфигурация.

Във фазата на планирането бяха дефинирани основните принципи, на които се основава разработваното обучаващо приложение за симулация xCPU, изложени по-долу:

- аналитичност на използвания модел;
- високо ниво на абстрактно представяне на симулацията;
- стъпково-процесна визуализация;
- синхронизирано-функциониращ модел на обучавания;
- развит информационен поток;
- базирана на единично събитие за тактов цикъл последователност;
- автоматизирано управляема цикличност;
- псевдо-тактова цикличност;
- ограничен модел на паметта - x0000 - x07ff h;
- невключена функционалност на В/И устройства;

- изпълнение на предефинирани кодови отрязъци;
- итеративен подход при изграждане на функционалности за всяка продуктова реализация;
- CISC ориентирана архитектура.

Въз основа на горните основни принципи се пристъпи към фазата на проектирането. Синтезиран бе работен поток на симулация в приложението, представен на фиг.1. Представеният работен поток с определено ниво на абстракция, очертава състоянията през които следва да премине симулационният процес. Паралелно с работния поток се задават и потребителските събитийно базирани действия и техните последващи резултативни състояния на „*симулираната система*“.



Фиг.1 Работен поток на симулация в обучаващо приложение.

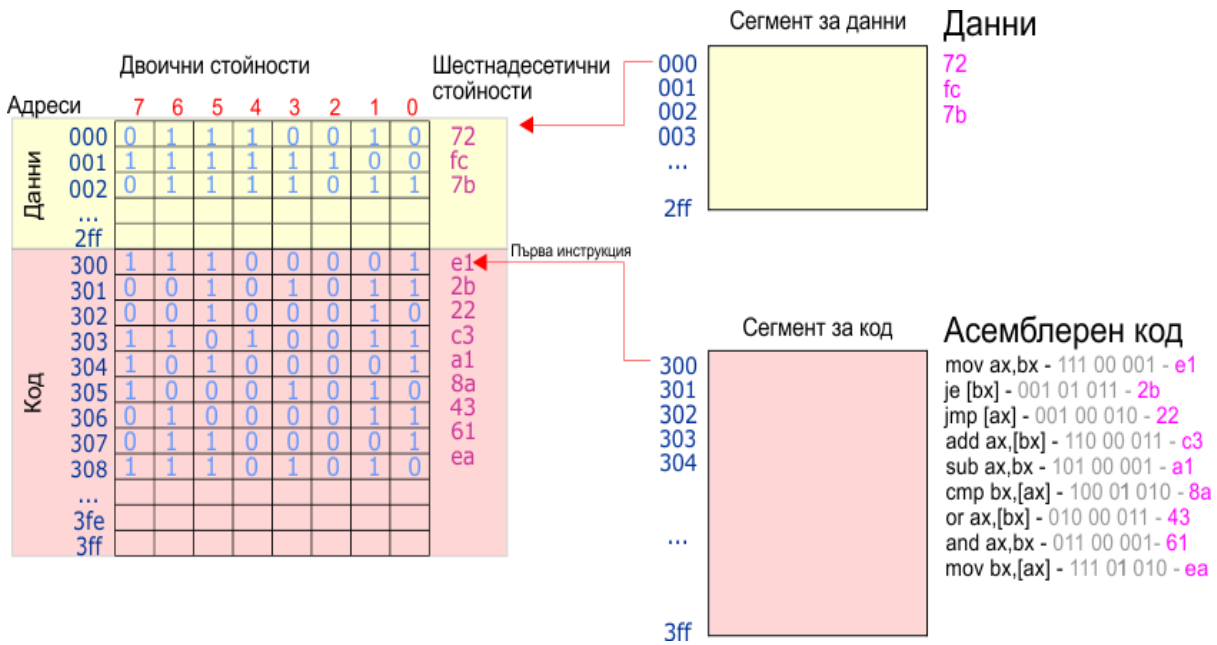
Назначението на стъпките по реализиране на функционалните задачи при всяко системно състояние на симулационния процес е описано в таблица 1.

Таблица 1. Постъпково назначение при системното състояние на симулационен процес в xCPU обучаващо приложение.

Системно състояние	Стъпки	Резултат
INI	• При първоначален старт • При активиране на събитийно ориентиран бутон Reset	• Всички клетки на ОП следва да съдържат само нулева стойност; • Буферната памет(кеш)следва да съдържа само нулева стойност; • Всички регистри с общо предназначение следва да съдържат само нулева стойност; • Изключение – BX регистърът следва да съдържа стойност (адрес) 0x311 h.
LAC	Стъпка 1	Избор от визуална контрола тип „select“ на предефиниран кодов отрявък в един ред.
SAC	Стъпка 1	При активиране на събитийно ориентиран бутон Start: • Установяване на функционално определени клетки от ОП със предефинирани стойности;. • Тези клетки следва да бъдат логическа част от ОП, представляваща сегментът за данни; • Незаетите клетки от ОП следва да съдържат нулева стойност; • Буферната памет (кеш) следва да съдържа нулеви стойности; • Всички регистри с общо предназначение следва да съдържат нулеви стойности; • Изключение – Регистърът - указател на инструкции (IP) следва да съдържа стойност (адрес) 0x300 h – адресът на първата инструкция, намираща се в сегмента за данни.
IF	Стъпка 1	При активиране на събитийно ориентиран бутон Step следва да бъде реализирана операцията четене на съдържанието от указаната в адресната шина клетка от ОП. Прочетеното съдържание следва да бъде поставено в L2 буферната памет. В регистър TLB prefetcher следва да постъпи инструкцията.
	Стъпка 2	В регистъра на инструкциите (Instruction register) следва да постъпи инструкцията.
FM		В регистъра указател IP се указва адресът на следващата инструкция, предстояща за извличане.
ID	Стъпка 1	Инструкцията се декодира от микро-кодова постоянна памет (micro-code Rom). Декодираната инструкция постъпва в регистри Instruction decoder и Trace cache.
EX	Стъпка 1	В целочисления регистров файл (Integer register file) постъпват операндите на декодираната инструкция. Ако местоназначението на резултата от

		операцията е регистър, то този резултат следва да постъпи в указания регистър.
	Стъпка 2	Ако се изисква аритметична операция, операндите постъпват в ALU U. Резултатът от операцията постъпва в Write Data Port1 и в указания регистър.
MEM	Стъпка 1	В случаите на използване на операция запис в ОП, изчислената стойност се записва в указаната от операцията клетка.

Както е разгледано в табл.1, работният поток има своите разклонения в зависимост от декодираната инструкция и операциите, които следва да бъдат извършени т.е. линейността му не е безусловна. В настоящата фаза се синтезира и модел на оперативна памет, чиято концепция е представена на фиг.2. За целите на проекта, в неговото първо издание, се изгражда опростен модел на оперативна памет с два сегмента – кодов и даннов. Това се обуславя от последователността на подходи за изграждане на абстрактно мислене у обучаваните при разглеждането на процесите, свързани с организирането на достъп до оперативната памет, чието първо проявление е реализиране на операции от тип регистър-памет.



Фиг. 2. Организация на оперативна памет при симулация в xCPU обучаващо приложение.

Съгласно насоките за базиране на CISC архитектура в набора от дефинираните по-горе принципи, бе формиран ограничен набор от инструкции, обект на симулационния процес, но който набор бе основан на принципите, залегнали в архитектурния набор от инструкции CISC. Една ключова характеристика на CISC набора от инструкции [16] е разширеното адресиране на операндите, включени при операциите четене/запис (load/store), чиито аритметични и логическите операции могат да се извършват както върху операнди,

разположени в процесорните регистри, така и върху операнди, намиращи се в по-ниско стоящия сегмент на паметта. Това води до реализиране както на операции тип регистър-регистър, така и на операции тип регистър-памет и памет-памет. В изпълнение на горното, стъпвайки върху базов формат на инструкция,

$$(\boldsymbol{opcode}, \boldsymbol{d}, \boldsymbol{s}, \boldsymbol{n}) \rightarrow \boldsymbol{IF}$$

където:

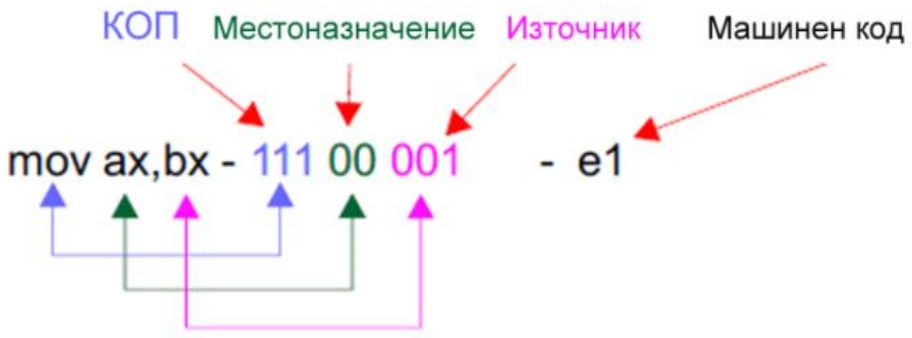
$\boldsymbol{IF}$- формат на инструкция;
$\boldsymbol{opcode}$ - код на операцията (КОП);
$\boldsymbol{d}$ - операнд местоназначение за резултата;
$\boldsymbol{s}$ - операнд източник за резултата;
$\boldsymbol{n}$ - адрес на следващата инструкция,

се синтезира показаният в табл.2 подход за кодиране на инструкцията в симулационния процес на xCPU:

Таблица 2. Схема за кодиране на полетата в кодов набор инструкции на xCPU процесор.

3 бита за КОП	**2 бита за поле местоназначение в инструкция от тип jmpx:**	**2 бита за поле местоназначение в инструкцията**	**3 бита за поле източник в инструкцията**
000 - special 001 - jmpx 010 - or 011 - and 100 - cmp 101 - sub 110 - add 111 – mov	00 - jmp 01 - je 10 - jne 11 – ja	00 - AX 01 - BX 10 - [AX] – с индексиране 11 - [BX] – с индексиране	000 – AX 001 - BX 010 - [AX] – с индексиране 011 - [BX] – с индексиране 100 - AX - AX съдържа отместването 101 - BX - BX съдържа отместването 110 - [AX] – източник + отместване 111 - [BX] - източник + отместване

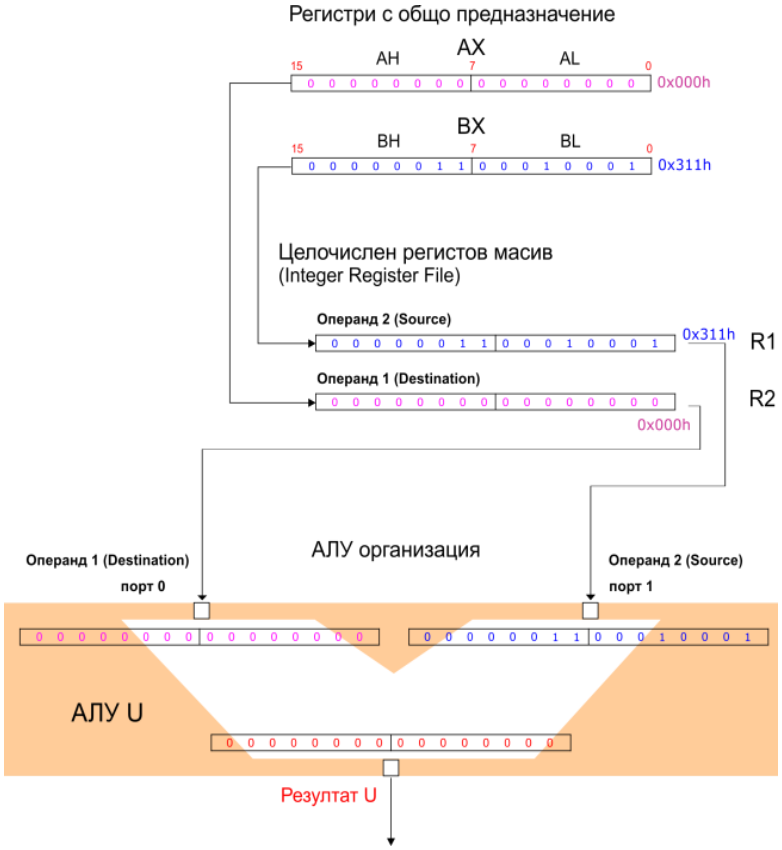
Следва да бъде отбелязано, че полето $\boldsymbol{n}$, адресът на следващата инструкция се формира от указателя на инструкции (Instruction Pointer) в архитектурата на xCPU. Като пример за кодиране, с използване на подхода в таблица 2, може да бъде посочен изразът, показан на фиг.3:



Фиг.3 Пример за кодиране на инструкция тип регистър-регистър от кодовия набор инструкции на xCPU.

Друга реализация на показаното в табл.2 кодиране може да бъде видяно и на фиг.2, в частта описваща асемблерния код. При разработката е приложено правилото “Big-Endian” за байтова поредност от старши към младши, при запис/четене в/от паметта, определящо, че старшата част се разполага в ***AH***(***BH***), а младшата част се разполага в ***AL***(***BL***).

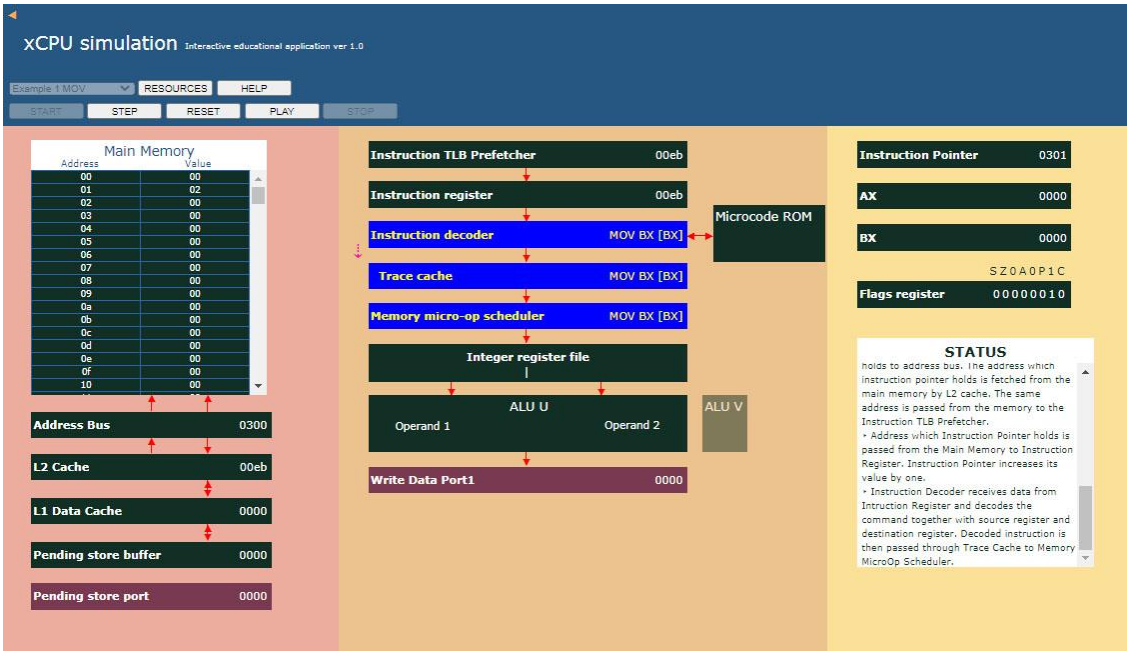
Разработката обхваща и изграждането на архитектура на симулирания процесор xCPU. На фиг.4 е показана фрагмент от организацията на симулирания процес при изпълнение на операциите в xCPU.



Фиг.4 Фрагмент от организация на процес при изпълнение на операциите в xCPU.

А, за да отговори на изискването, на което трябва да отговаря дадено обучаващо приложение, следваше да бъде интегриран модел на обучавания [2], [5]. Указаният модел на обучавания бе реализиран посредством изграждане област на взаимодействието, област на архетипа и област на компетенциите. В текущото издание на xCPU симулатора бе концептуализирана областта на архетипа и областта на компетенциите, а областта на взаимодействие получи своята програмна разработка, оптимизирайки кръга от предметно насочени взаимодействия при оперирането със системата. Областта на компетенциите предполага свързване на всички предефинирани потребителски взаимодействия с предефинирани показатели, които определят основата за формиране на дидактически подход при фазите на учебния процес [4], [9]. Всяка стъпка на обучавания извежда в обособен диалогов екран информация за текущия статус на операцията.

В текущата версия на xCPU симулатора, освен функционалните му характеристики са включени раздел помощ и раздел достъп до ресурси. Функции. На фиг.4 е показана екранна снимка от обучаващото приложение.



Фиг.4 Екранна снимка от издание 1.0 на xCPU симулатора.

4 Заключение

Работата по настоящия проект ще премине към своя следващ етап, в който ще бъдат добавени функционалности на приложението, обхващащи обработката на операндите от невключени в процеса отделни процесорни регистри (Instruction TLB Prefetcher и др.) и буферна памет (L1,L2,Trace cache и др.), Ще бъдат разгърнати в програмен код и двете концептуализирани области на модела на обучавания. Ще бъде увеличен наборът от кодови отрязъци, предназначени за симулация, с нови инструкции. Паралелно с процеса на разработка, екипът цели и изследване влиянието на този клас Уеб базирани обучаващи инструменти върху обучаващия процес на обучаваните, представители на високоинтерактивното поколение [3], [10].

ЛИТЕРАТУРА:

[1] Атанасов, В., „Концептуализация на умен образователен клъстер (Smart Educational Cluster Conceptualization)“, Международна научна конференция "Отбранителни технологии", стр.173-181, 2018, ISSN: 2367-7902;

[2] Христов, Х., Цанков, Ц. Използване на системата e-Learning Shell в обучението по инженерните дисциплини. Научна конференция на Факултета по технически науки, Шумен, 2010, ISSN 1311-834X, с. 63-69.

[3] Христов, Х,. Дянков, П. Съвременни методи и техники на преподаване по механика. Годишник на ШУ "Епископ Константин Преславски"- Технически науки, УИ "Епископ Константин Преславски", 2015 г. стр. 144-149, ISSN 1311-834X

[4] Atanasov, V., A Sight over Gaming Technologies in Pedagogical Context, Pedagogy, Bulgarian Journal of Educational Research and Practice, Volume 89, Number 5, 2017, pp.672-683, ISSN 0861 – 3982 (Print) ISSN 1314 – 8540 (Online);

[5] Atanasov, V., Ivanova, A., Student modelling in a web-based platform for learning games composing, The 13th International Scientific Conference eLearning and Software for Education, Bucharest, vol.2, 2017, pp.272-279, https://doi.org/10.12753/2066-026x-17-040;

[6] Atanasov, V., A. Ivanova. A WEB based Platform for Learning Games composing - Basic Concept and Architectural Aspects. IN: Proceedings of e-Learning'15 International Conference, Berlin, Germany, 2015, pp.256 - 261, ISBN 2367 – 6698;

[7] Atanasov, V., Ivanova, A., "A Framework for Measurement of Interactivity of Digital Learning Resources," 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2019, pp. 649-654, doi: 10.23919/MIPRO.2019.8757052;

[8] Kalev, K., A Conceptual Approach of Building Web Based Learning Tool, JDST., vol. 2, no. 2, p11-p18, 2020, e-ISSN 2534-9813, https://doi.org/10.46713/jdst.002.02;

[9] Firth, J., Trous, J., Stubbs, B., et all, The “online brain”: how the Internet may be changing our cognition,World Psychiatry, vol. 18(2), pp.119–129, 2019 doi: 10.1002/wps.20617;

[10] Hristo Beloev, Angel Smrikarov, Aneliya Ivanova et all , A Vision of the University of the Future, CompSysTech '20: Proceedings of the 21st International Conference on Computer Systems and Technologies '20June ,2020 ,Pages 307–312, https://doi.org/10.1145/3407982.3408027;

[11] Markovic, D.,Ivkovic, I., Popovic, R., SIMAS: A web-based computer system simulator, The International journal of engineering education, Vol. 26, no. Extra 4, pp.930-937, 2010, ISSN-e 0949-149X;

[12] Z. Radivojevic, Z., Stanisavljevic, Z., Punt, M., "Configurable simulator for computer architecture and organization", Computer Application and Engineering Education, vol.26 issue 5, pp.1711-1724, 2018, http://doi.org/10.1002/cae22034;

[13] García-Carballeira, F., Mateos, A., C. et all, "WepSIM: An Online Interactive Educational Simulator Integrating Microdesign, Microprogramming, and Assembly Language Programming," IEEE Transactions on Learning Technologies, vol. 13, no. 1, pp. 211-218, 2020, doi: 10.1109/TLT.2019.2903714;

[14] Heirman, W., Carlson, T. E., Hur, I. et all, The Sniper Multi-core Simulator, IEEE International Symposium on Workload Characterization, 2013, ISBN 1-4799-0555-0;

[15] Stahl, T., Völter, M., Model-Driven Software Development: Technology, Engineering, Management, John Wiley & Sons Ltd, 2006, ISBN-13: 978-0-470-02570-3;

[16] Stallings, W., Computer Organization and Architecture Designing for Performance - Tenth edition, Pearson, 2016, ISBN-10: 0-13-410161-8

Имена на авторите: Валентин Атанасов
Месторабота: Шуменски университет „Еп. Константин Преславски“
E-mail: v.atanasov@shu.bg
Линко Г. Николов
E-mail: linko.nikolov@aadcf.nvu.bg

CONCEPTUAL AND FUNCTIONAL MODEL OF THE WEB BASED LEARNING APPLICATION

VALENTIN T. ATANASOV

ABSTRACT: *This publication presents a possible approach to the system modeling of a web-based learning application. A conceptual model, a functional model and a workflow of a learning application are synthesized. The main roles and functions of the users of the learning application are considered. In terms of the educational context of the application and its integration in a given digitally based learning process, a didactic model of a digitally based learning process has been synthesized. This systematic approach of modeling does not set restrictions, rather it allows adaptations in the presence of specific requirements for the implementation of the digital form of educational process.*

KEYWORDS: *Learning app, ICT app, digital learning, WEB based learning, system modelling..*

КОНЦЕПТУАЛЕН И ФУНКЦИОНАЛЕН МОДЕЛ НА УЕБ БАЗИРАНО ОБУЧАВАЩО ПРИЛОЖЕНИЕ

ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *Настоящата публикация представя един възможен подход при системно моделиране на УЕБ базирано обучаващо приложение. Синтезирани са концептуален модел, функционален модел и работен поток на обучаващо приложение.В публикацията се разглеждат основните роли и функции на потребителите на обучаващото приложение. С оглед образователния контекст на приложението и интеграцията му в дадено обучение в цифрова среда е синтезиран дидактически модел на цифрово базиран учебен процес. Този системен подход на моделиране не поставя ограничения, а позволява адаптации при наличието на специфични изисквания за реализацията на дигиталната форма на образователен процес.*

1 Въведение

Фазата на формулирането на общите изисквания към дадено УЕБ базирано обучаващо приложение е съществена част от процеса на дадена софтуерна разработка. Може да бъде отчетено, че в обучаващото приложение съществено влияние оказват редица фактори, въздействащи върху потребителското преживяване [9,10] – емоциите, лекотата на употреба, моториката и когнитивните фактори на обучавания. Факторът „*потребителско преживяване*“ експлицитно има психологическа природа и в този смисъл следва бъде формиран набор от изисквания, обуславящ постигането на поставената пред обучаващото приложение цел, които изисквания следва да съответстват на тази психологическа природа. Изхождайки от психологическата характеристика на съвременния обучаван [4,7,8] за решаването на тази задача се подхожда посредством изграждане на обекти с високи показатели на интерактивност, оказващи въздействие по начин и форма в когнитивно-психологически аспект, допринасящи за постигането на поставената от преподавателя цел. Като следваща стъпка в тази фаза е необходимо да бъде изяснена и дефинирана концепцията на УЕБ базираното обучаващо приложение.

По своята същност обучаващото приложение е програмен продукт, чиято разработка е подчинена на концепцията, визираща неговия предметно-дисциплинарен характер. За целите на настоящата публикация, обучаващото приложение се разглежда в концептуален

план като образователен процес от общ характер. С цел избягване спецификите на определени дисциплини, които налагат доминация на определени стилове на учене, тук се приема и общият подход при образователен процес.

2 Концептуализация на УЕБ базираното обучаващо приложение

В концептуално отношение се разглежда интегрирането на дидактически модел, който би поставил обучавания в активна позиция при едно реално работещо УЕБ базирано обучаващо приложение, а също се предлага и механизъм за контрол на информационния поток в това приложение.

Ефективна насока при изграждането на концепцията на УЕБ базирано обучаващо приложение е следването на постановката за преход от репродуцирането на готови знания у обучавания към формиране на умения за самостоятелна организация на ученето.

Обучаващото приложение следва да предоставя на обучавания възможност да:

- *възприема информацията по мултисетивни канали;*
- *формулира казуси;*
- *решава проблемни ситуации;*
- *търси решения;*
- *конструира, прилага и надгражда знания*;

В настоящата фаза се концептуализират и:

- *ролите и ранговете (йерархията) на потребителите;*
- *обхватът и вревите рамки на правата;*
- *интерактивност на ниво взаимодействащи се обекти ;*
- *изборът на модел/модели;*
- *контролът и обратната връзка;*
- *степента на взаимодействие с други системи;*
- *системните процеси.*

Анализ на контекста

В тази фаза на анализ се определят изисквания и параметри на образователното обкръжение за прототип на образователно приложение, обхващащи следните категории:

- *Технологично обкръжение и инфраструктура;*
- *Потребители, които ще ползват приложението;*
- *Начин на ползване на приложението;*
- *Форма и място на ползване на приложението;*
- *Ограничения на приложението (педагогически и технологични).*

Дефиниране на роли и функции

При дефинирането на ролите и функциите се изяснява субектът, който ще ползва съответните части на приложението, какви действия или операции ще изпълнява, с какви и с кои артефакти ще оперира и какъв ще бъде резултатът от това.

Таблица 1. Дефинирани роли и функции

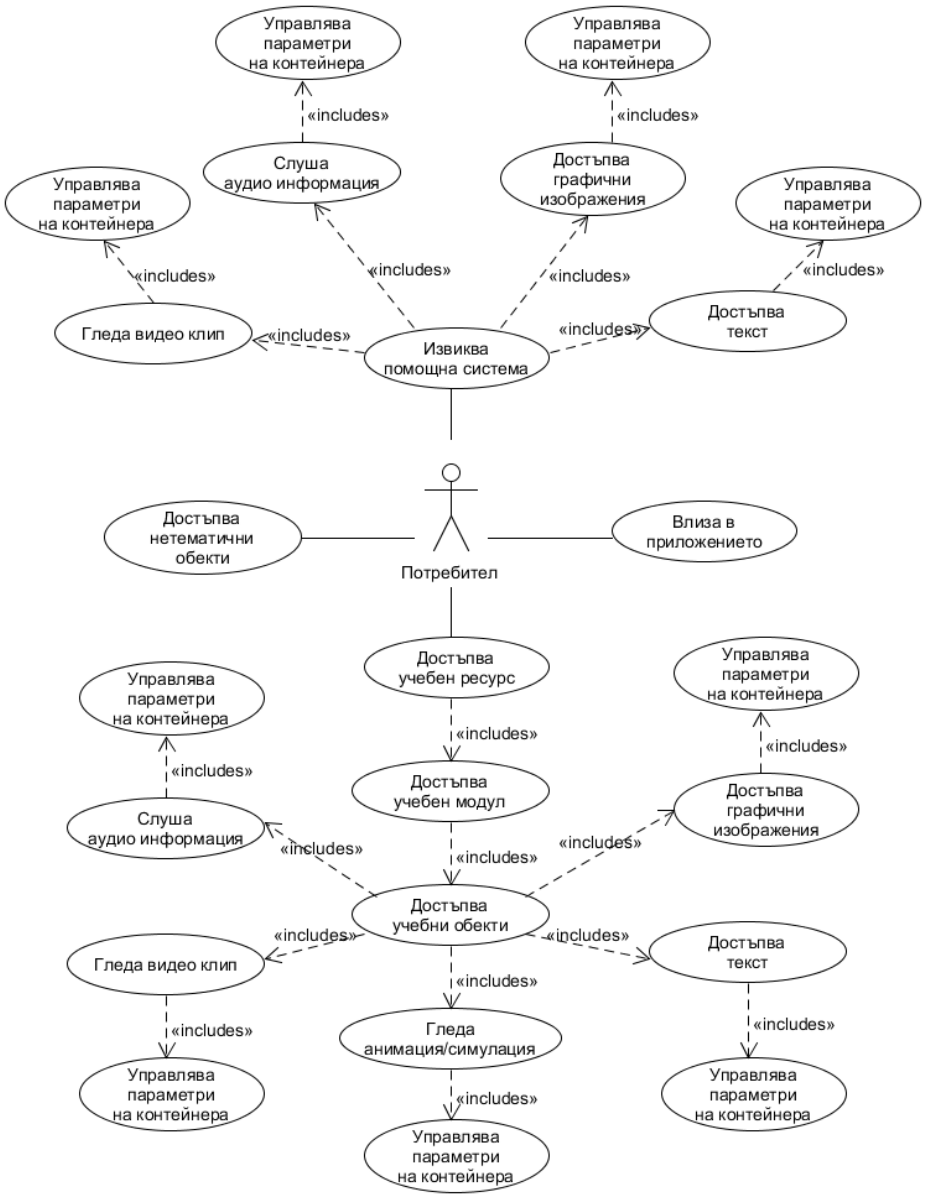
<table>
<tr><th colspan="2">Обучаван – потребител</th></tr>
<tr><td colspan="2">Регистриран в системата потребител.
Роля: Потребител</td></tr>
<tr><td colspan="2">Функции:
Получава права за достъп;
Избира входящи параметри;
Преглежда справочник за учебно съдържание;
Достъпва учебно съдържание;
Управлява програмна учебна среда;
Преглежда помощната информация;</td></tr>
<tr><td>Артефакти:
Учебно съдържание;
Обекти от учебното съдържание(обекти, представени от основните типове данни);
Обекти на потребителския интерфейс;
Помощна информация;</td><td>Предназначени за:
Конструиране и придобиване на знания;
Решаване на казуси;
Формиране на личностно-ориентирана учебна програмна среда;
Получаване на насоки, указания, напътствия и др.
Управление на информационния поток чрез потребителския интерфейс на обектите в учебното съдържание.</td></tr>
<tr><th colspan="2">Преподавател</th></tr>
<tr><td colspan="2">Регистриран потребител, упълномощен от администратор.
Роля: Обучаващ</td></tr>
<tr><td colspan="2">Функции:
Получава права за достъп;
Създава учебно съдържание;
Управлява обекти от учебно съдържание;
Управление на информационния поток чрез потребителския интерфейс на обектите в учебното съдържание.
Преглежда помощната информация;
Осъществява мониторинг.</td></tr>
<tr><td>Артефакти:
Учебно съдържание;
Обекти от учебно съдържание;
Система за мониторинг и управление на показатели;
Помощно ръководство.</td><td>Предназначени за:
Цифрово базиран образователен процес;
Наблюдение на постижения и показатели;
Информация и указания;</td></tr>
</table>

3 Функционален модел на обучаващо приложение

Моделиране на взаимодействията

След анализ на изискванията към обучаващото приложение се пристъпва към изграждане на функционалния му модел. Този функционален модел на УЕБ базираното обучаващото приложение предоставя определена информация за логическата процедурна обусловеност на компоненти му от перспективата на потребителя. За изграждането на модела се налагат принципите на обектно-ориентирания подход при моделирането. Отчита се, че системното поведение е в основата на този модел. В този случай, от потребителска перспектива, системата се описва посредством набора от нейните функционални характеристики. В този етап се формализира начинът, по който приложението ще работи и

по който ще взаимодейства с потребителите. Потребителят следва да се разглежда като външен за приложението субект, който ще взаимодейства с него, ще изпълнява предварително дефинирана роля и ще оперира с определени артефакти. Подходящо и ефикасно средство за моделиране са случаите на употреба на UML(фиг.1).



Фиг.1. Случаи на употреба на потребител в прототип на обучаващо приложение

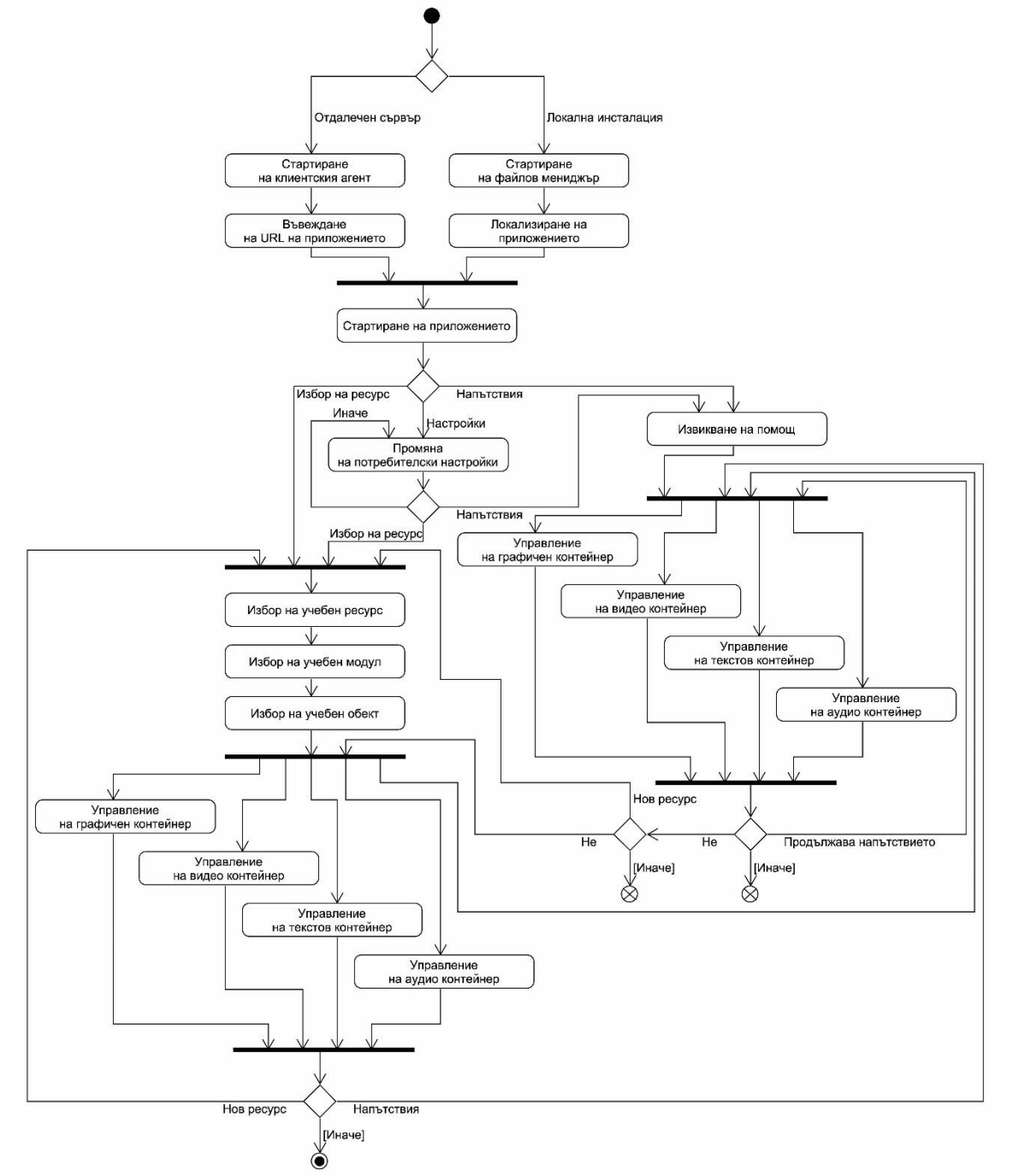
Моделиране на работния поток на обучаващо приложение

Подходът на моделиране при разработване на дадена система е утвърдена практика и фактор за ефикасност [1,5,6]. Утвърденият език UML предоставя редица възможности за моделиране, в това число и на основни процеси във функционален аспект. С нотациите на диаграмите на дейности е моделиран работният поток на обучаващото приложение (фиг.2.).

Работният поток, представен на фиг.2. дава ясно очертание на процесите в обучаващото приложение, като в потока са представени основните два процеса, обхващащи

непредметните и предметните взаимодействия [2,3] [1]. Изведените дейности са с един основен изпълнител – потребителят на системния прототип.

Не се разглеждат случаи, изискващи трансформация на изходящи параметри от дадено изходящо действие към входящи параметри на последващото действие. В общия случай се разглеждат онези аспекти на потока, обуславящи основите на цифровия учебен процес.



Фиг. 2. Работен поток на обучаващо приложение

Построяване на дидактически модел

В настоящия труд се разглежда внедряването на обучаващото приложение в цифрово базиран учебен процес, като извън инженерната специфика този процес почива на педагогически принципи, следвайки постигането на педагогически цели, посредством дидактически подходи [2,3]. Базирайки се на горното се пристъпва към педагогическа формализация и моделиране на процеса на цифрово обучение, съответно и „имплементиране“ на получения модел в обучаваща система с цел постигане на ефикасност. За постигането на тази цел се синтезира цифрово базиран дидактически модел (фиг.3), следващ принципите на образователния процес, съобразени с водещите съвременни педагогически теории.

Фиг. 3. Дидактически модел на цифрово базиран учебен процес

4 Заключение

Настоящата публикация представя един възможен подход за моделиране на УЕБ базирано обучаващо приложение с отчитане на основните аспекти на системната разработка и имплементирането на дидактическата компонента, обуславяща постигането на поставените педагогически цели от преподавателя, включващ в инструментариума си ИКТ базирани обучаващи приложения.

Синтезираните модели и подходи предоставят принципна насока при етапите на системно моделиране и същевременно допускащи в определени граници адаптирани версии на дадени обучаващи приложения. Разглеждайки комплексността на функционалните характеристики при дадено системно моделиране, но с отчитане на образователния контекст, може да се допусне, че предложените концептуален модел, функционален модел, работен поток и дидактически модел биха могли да обезпечат съвместимост при други случаи на системна разработка на приложения, предназначени за реализиране на цифрово базиран учебен процес.

ЛИТЕРАТУРА:

[1] Фаулър, М., UML основи, Кратко ръководство за стандартния език за обектно моделиране, Издателство „СофтПрес“ ООД, 2007, ISBN 978-954-685-306-6

[2] Христов, Х., Цанков, Ц. Използване на системата e-Learning Shell в обучението по инженерните дисциплини. Научна конференция на Факултета по технически науки, Шумен, 2010, ISSN 1311-834X, с. 63-69.

[3] Atanasov, V., Ivanova, A., Student modelling in a web-based platform for learning games composing, Proceedings of the 13th International Scientific Conference "eLearning and Software for Education, Bucharest, Romania April 27 - 28, pp.272-279, 2017, ISSN 2066-026X

[4] Atanasov, V., Ivanova, A., A Framework for Measurement of Interactivity of Digital Learning Resources, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 649-654, 2019, ISSN 2623-8764

[5] Sommerville, I., Software Engineering - 9th ed. ,Addison-Wesley , 2011, ISBN-13: 978-0-13-703515-1

[6] Stahl, T., Völter, M., Model-Driven Software Development: Technology, Engineering, Management, John Wiley & Sons Ltd, 2006 ,ISBN-13: 978-0-470-02570-3

[7] Prensky, M., Digital Natives, Digital Immigrants Part 1, On the Horizon, Vol. 9 Iss: 5, 2001, ISSN: 1074-8121

[8] Prensky, M., Don`t bother me Mom, I`m learning, Paragon House Publishers, ISBN:1557788588, 2006

[9] Doll, B., Monitoring User Experience: A single page lifecycle, 2011, ,(https://blog.newrelic.com/engineering/monitoring-user-experience-a-single-page-lifecycle/)(посетен на 12.10.2019)

[10] Rinaldi, J.,,30 Eye-Opening User Experience Stats [Infographic],(https://www.impactbnd.com/blog/user-experience-stats-infographic)(посетен 12.08.2020)

Валентин Атанасов
Месторабота: Шуменски университет „Еп. Константин Преславски“
E-mail: v.atanasov@shu.bg

TECHNIQUES FOR PASSWORD CRACKING IN WIRELESS NETWORKS

LINKO G. NIKOLOV, VALENTIN T. ATANASOV

ABSTRACT: *Almost all wireless networks are vulnerable to access violation by password guessing or hashed secret key correlation. By choosing some of the famous techniques for password cracking, the possibility for network access will be tested. Some of the most popular software instruments for wireless vulnerabilities estimation are shown in this research paper. Examples of cracked passwords are shown.*

KEYWORDS: *Wi-Fi, aircrack-ng, Linux chunk, Bruteforcer, Kali Linux.*

ПОХВАТИ ЗА ПРОБИВАНЕ НА ПАРОЛИ В БЕЗЖИЧНИТЕ МРЕЖИ

ЛИНКО Г. НИКОЛОВ, ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *Почти всички безжични комуникационни мрежи могат да бъдат уязвими откъм точки за достъп, ако бъдат използвани слаби пароли. Съществуващите инструменти за изследване на сигурността на безжичните мрежи стават все по известни. В този изследователски доклад са посочени примери за използването на такива инструменти за отгатване на паролите за достъп чрез речникова атака, или чрез атака с изчисляване на пълния набор от комбинации.*

1. Осигуряване на защита в безжичните мрежи.

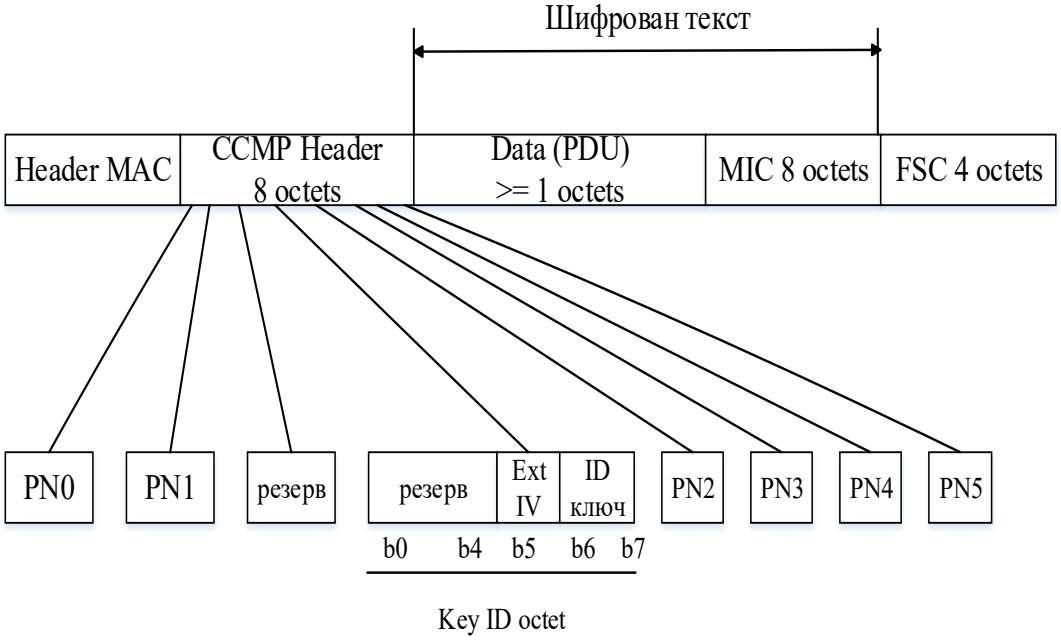
Лесното развръщане на безжична мрежа от вида Wi-Fi дефинира широкото й използване за всякакви нужди, но в същото време и много програми, които следят за активност и наличието на защита в тях. Първият протокол за защита на Wi-Fi е „WEP“. Той отдавна е компрометиран и затова не се препоръчва за използване [8]. Протоколът от следващо поколение е „Wi-Fi Protected Access“ (WPA). Но скоро след започване на употребата му се доказва, че той също е слаб от криптографска гледна точка [4] [5]. Това води до разработването на протоколът, който се използва и до днес: WPA-2. Въпреки криптографската сигурност обаче, този протокол също е уязвим на атаки, когато потребителите посочват слаби пароли. По-сложни пароли също могат да се разбиват, но това изисква повече изчислителен ресурс и налично време. За целта на това изследване ще се използва обикновен рутер, който създава точка за достъп до безжична мрежа. Ще се използва и устройство, което легитимно ще се свързва към безжичната мрежа [1]. Третият компонент от обстановката е компютър, на който е инсталирана ОС Kali Linux. С помощта на операционната система Kali Linux, инструментът Aircrack-ng^{tm}, „chunk“ и „topguw“ може да се постигне откриване на парола за достъп или отгатване на секретния ключ за криптиране на комуникационните данни, и това да е в режим извън линия (offline).

2. Речникова атака към безжична Wi-Fi мрежа.

Процесът по речниково откриване на паролата за достъп до безжичната мрежа се състои от сравняване на хеш-данните на използваната дума като парола за достъп и хеш-

данни, генерирани и организирани в речникови таблици. Сравняването става фраза по фраза и отнема изключително много време. В протокол WPA-2 има два типа обмен на ключове:

- обмен на лични данни между две устройства (режим WPA-2 personal);
- обмен на парола, контролиран от специализиран назначен сървър (WPA-2 Enterprise).



Фиг. 1 – Фрейм, криптиран чрез WPA-2 [2]

В този доклад ще се използва първия тип обмен - WPA-2 personal. Обменът на паролата за достъп се осъществява между станцията-клиент (Supplicant station/STA) и обслужващата точка за достъп (Authenticator/Access point/AP STA). В режим „WPA-2 Personal“ протоколът на първо време изпраща предварително споделен ключ, който е комбиниран с идентификатор на мрежата (SSID) и след това се създава чифт главни ключове (Pairwise Main Key, PMK). Клиентът и точката за достъп обменят данни чрез PMK и след това създават преходен ключ (Pairwise Transient Key, PTK).

Успешното декриптиране на паролата за достъп изисква откradване чрез подслушване на информацията за обмен на ключа. Тази информация може да се получи ако се уцели точния момент на иницииране от дадено крайно устройство на присъединяване към безжичната мрежа. Софтуерния инструмент „aircrack-ng“ има възможност насилствено да накара крайно устройство да се деасоциира от мрежата си чрез командата „aireplay“ [6]. И ако устройството е настроено автоматично да се асоциира към безжичната мрежа, тази команда извиква допълнителен процес на ръкостискане, който ще съдържа, макар и хеширана, стойностите на ключа и паролата за достъп.

След като се открие наличието на целева мрежа, тя ще бъде избрана за атакуване. Атакуването ще се извърши чрез серия от команди. Първата от тях е:

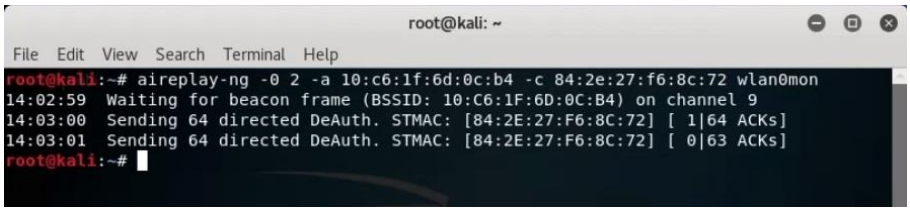
airodump-ng -c [номер на канала 9] -bssid [име на мрежата cyber_01] -w /root/Desktop [име на интерфейса в режим на следене wlan0mon]

Фиг. 2 – Следене на целева мрежа cyber_01

След като атакуващата машина е подготвена да следи активността в целевата мрежа, се използва командата за атакуващо деавтентикиране на крайното устройство:

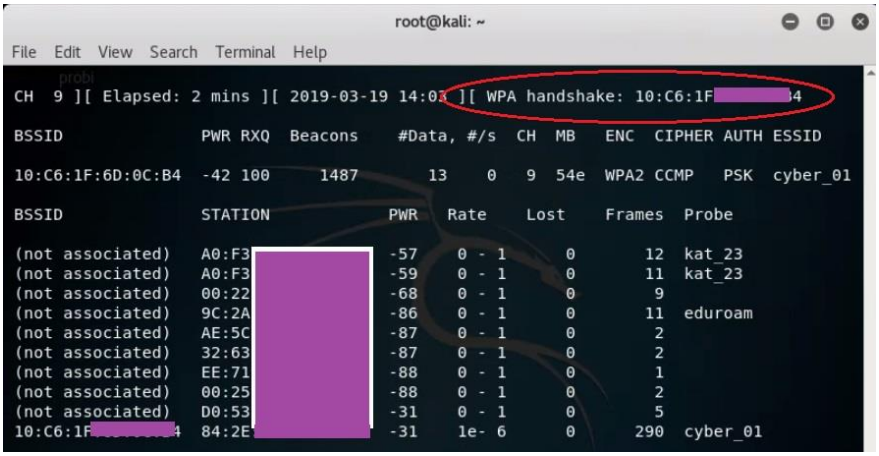
aireplay-ng -0 2 -a (router's BSSID 10:c6:1f:6d:0c:b4) -c (client's BSSID 84:2e:27:f6:8c:72) (monitor interface wlan0mon)

Чрез тази команда се изпращат деавтентикиращи пакети, които точката за достъп получава и изключва крайното устройство от мрежата. Клиентът се опитва да се присъедини отново и това е моментът, в който се събира информация, която съдържа паролата за достъп, макар и криптирана. Записва се информацията от процеса на ръкостискане.



Фиг. 3 – Команда за деавтентикация на крайното устройство

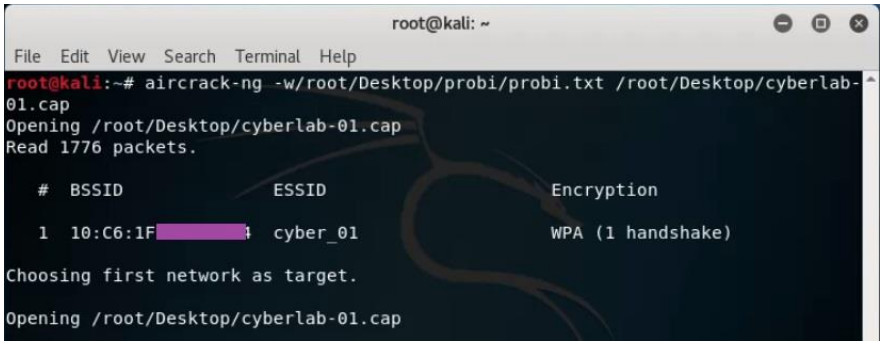
След стартирането на тази злонамерена атака, свързаната с мрежата машина-жертва (Station/STA) се изключва и автоматично се опитва да се включи отново към точката за достъп (Authenticator/AP). При това, пакетите, съдържащи ключова информация в процеса на ръкостискане, се прихващат и откраднат.



Фиг. 4 – Записване на пакети от процеса по договаряне между машините

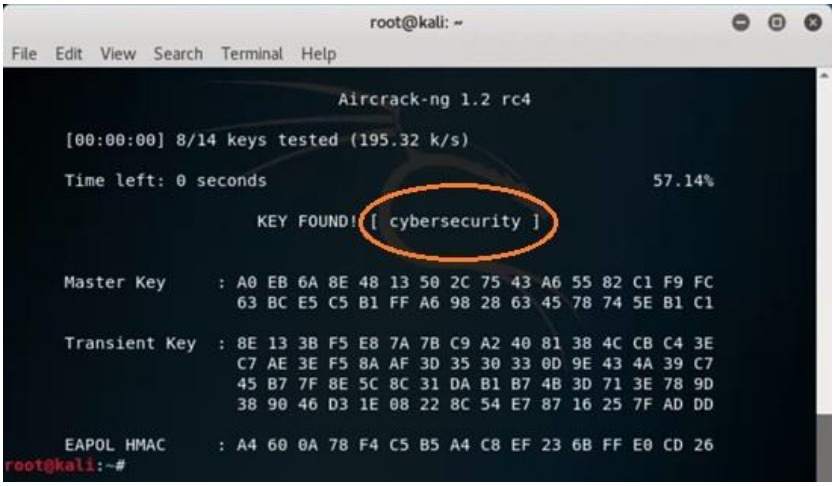
След това, атакуващия компютър използва тези прихванати пакети, записани във файл „.cap“ като ги сравнява с предварително подготвения списък с паролни фрази с цел кракване на паролата за достъп. Този процес разчита на списъкът с думи и процесорната мощност на атакуващия компютър. Командата, която се използва тук, е:

aircrack-ng -a2 -b 10:c6:1f:00:00:00 -w /root/Desktop/probi/probi.txt /root/Desktop/cyberlab_01.cap



Фиг. 5 – Команда за стартиране на речникова атака

След написване на горния команден ред, софтуерния инструмент aircrack започва корелация между базата данни, която има като речник, и прихванатия файл с разширение „*.cap“.



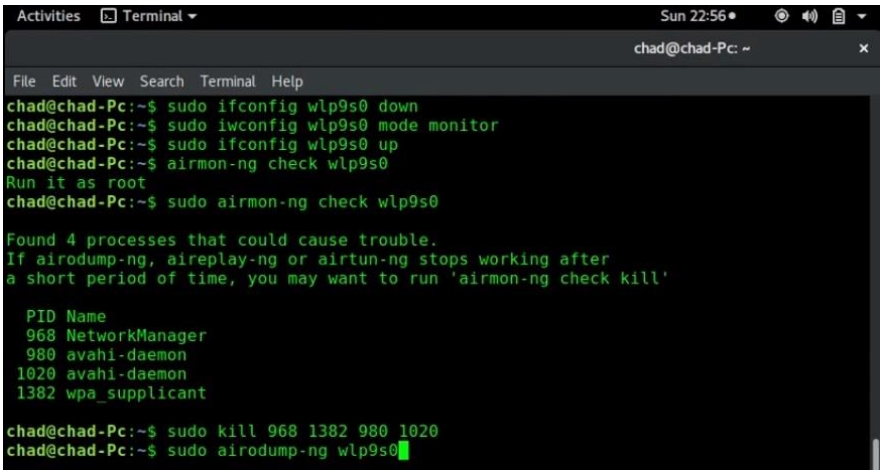
Фиг. 6 – Успешно откриване на паролата за достъп до мрежата

На фиг. 6 се вижда пример за открита парола за достъп „cybersecurity“. Уязвимостта на мрежата се определя от времето, необходимо на атакуващата система, да открие тази парола.

3. Похват за използване на „груба сила“ при отгатване на парола за достъп.

Процесът по откриване чрез груба сила на паролата за достъп до безжичната мрежа се състои в сравняване (корелация) на произволно генерирани комбинации, създаващи хеш-данни, и хеш-данните на самата парола. Криптографския алгоритъм обаче, използван в протокол WPA-2, все още е силен и чиста атака с груба сила може да отнеме изключително много време. Ето защо, при този вид атака е подходящо, при възможност, да се вмъкне

елемент на разузнаване. Чрез разузнаване може да се разбере приблизителната дължина на паролата за достъп, както и възможни символи, участващи в написването ѝ. Тази информация би допринесла за съкращаване на времената за генериране на стринговете на различни пароли. Също така, при използването на готови стрингове от пароли може да се използва логиката, генерирана от алгоритъм за размита логика, както е посочено в [3]. Похватът с предварително известна, макар и непълна информация, се използва чрез софтуерния инструмент „crunch“. Той се използва в помощ на познатия aircrack-ng, който извършва сравняване на генерираните стрингове с получените подслушвани пакети, съдържащи, макар и криптирана, паролата за достъп до мрежата. На фиг. 7 е показан командния ред за подготовка на подслушване на мрежовата карта за безжичен достъп.



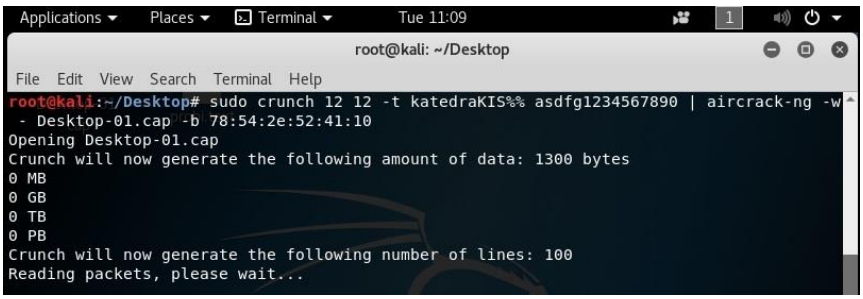
Фиг. 7 – Алтернативен ред команди при подготовка за подслушване

Командата „sudo“ се използва за изрично указване ОС да даде пълни права (super user) на текущия потребител. След командата

sudo airodump-ng wlp9s0

започва процес на следене на получаваните пакети от тази мрежова карта. След като е започнало подслушването за обмен на парола и записването на пакетите в изрично указан файл, се изчаква машината жертва да се присъедини към мрежата [7]. Ако това не става веднага, се прибягва до насилствено реасоцииране на жертвата с мрежата чрез команда „aireplay“. След получаване на пълния процес по „ръкостискане“ (WPA handshake), атаката по отгатване се инициира чрез командата „crunch“:

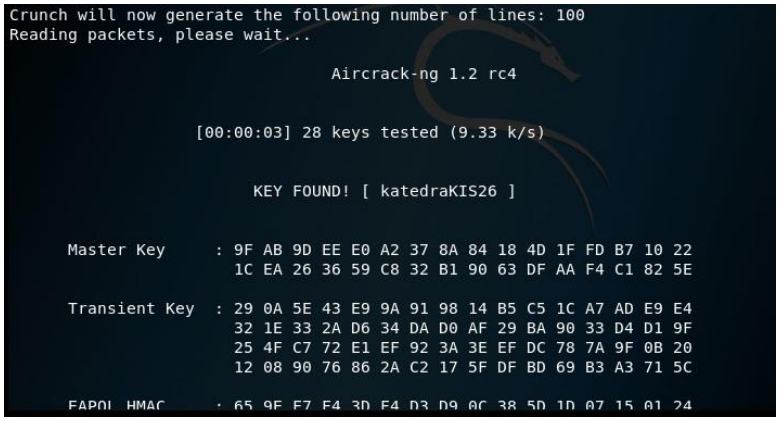
sudo crunch 12 12 –t katedraKIS%% asdfg1234567890 | aircrack-ng –w – Desktop-01.cap –b 78:54:2e:52:41:10



Фиг. 8 – Команда „crunch“ в помощ за отгатване на паролата

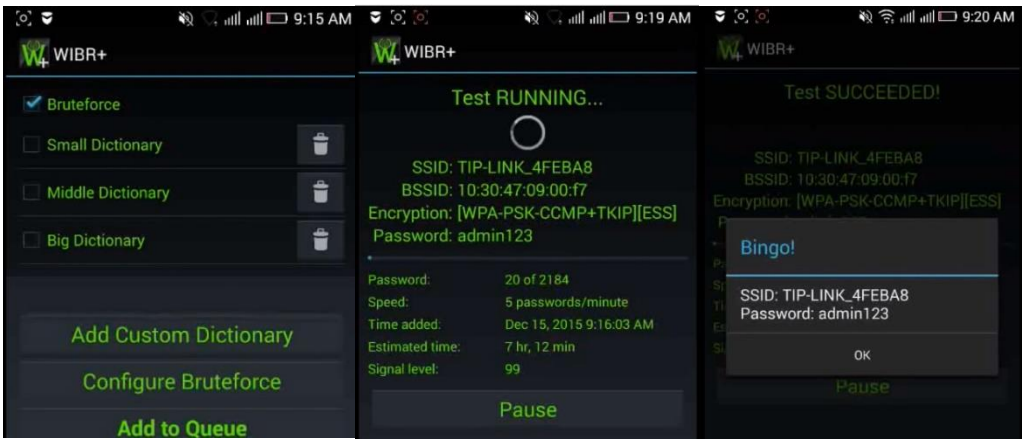
Командата crunch задава колко брой символи ще има в паролата и какви могат да бъдат те. На представения пример, след разузнаване е станало ясно, че паролата ще съдържа 12 символа и се посочва на aircrack-ng да генерира само 12-символни комбинации. Също така, с цел ясен пример, е посочено, че паролата започва с конкретния низ: „katedraKIS“. За софтуерния инструмент остава да генерира още по 2 символа в 12-символната комбинация, като изрично му се указва, че тези символи могат да са единствено „asdfg1234567890“.

На фиг. 9 е показано времето за отгатване на паролата, както и броя на проверените паролни комбинации.



Фиг. 9 – Успех при отгатването на паролата чрез „груба сила“

Друг възможен софтуерен инструмент за атакуване на безжични мрежи по метода на грубата сила е „*WIFI BRUTEFORCER*“ (фиг. 10). Успехът на програмата WIFI Bruteforcer се дължи на комбинацията на атака с груба сила, и съчетаването ѝ с речник. Важна особеност е изискването на поне 8 символа за създаването на парола и защита на безжичната мрежа. Това обаче улеснява генераторите на комбинации, тъй като им се задава по подразбиране да започват своето генериране от 8-символни комбинации нагоре.



Фиг. 10 – Действие на софтуер „WIFI BRUTEFORCER“ в ОС Andorid

4. Заключение

Уязвима точка в безжичните мрежи се оказва дължината на паролата и използваната семантика на символите в нея. Също така, сложността на генерирания ключ за криптиране,

при съвременните изчислителни мощности на атакуващите машини, може да се окаже слаба и този ключ да бъде отгатнат. С развитието на технологиите по защита на безжичните мрежи расте и популяризацията на инструментите, които я изследват. Цели операционни системи и софтуерни инструменти могат лесно и свободно да се набавят от глобалната мрежа интернет, което прави въпроса по защита на безжичните мрежи силно актуален.

ЛИТЕРАТУРА:

[1] Nikolov, L., „Network Infrastructure for Cybersecurity Analysis“, Proceedings of International Scientific Conference “Defense Technologies”, Shumen, 2018, ISSN 2367-7902, URL: http://aadcf.nvu.bg/scientific_events/dft2018

[2] Стандарт IEEE 802.1X, https://standards.ieee.org/standard/802_1X-2010.html

[3] Krasimir Slavyanov, An algorithm for object classification procedure for ISAR images, Proceedings of 12th International Symposium on Applied Informatics and Related Areas, November 9, 2017, Székesfehérvár, Hungary, 70-74, ISBN 978 - 963 - 449 - 032 - 6

[4] Boyanov, P., Identification of active hosts in the computer networks and evaluation the network security against modern types of cyber attacks, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 56, April 2019, pp. 92-98.

[5] Boyanov, P., A novel algorithm for detecting TCP/IP network attacks using hybrid firewall script applied in Linux operating system, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 57, May 2019, pp. 33-41

[6] Aaron James, “Mastering Wireless Penetration Testing for Highly Secured Environments”, PACKT, 2015, ISBN 978-1-78216-318-3

[7] Boyanov, P., Implementation of session hijacking cyber attacks against government agencies, private organizations and academic institutions, Collection of reports from Jubilee International Scientific Conference on the subject of Security and Economics in the uncertain world – Dilemmas and Challenges, ISBN 978-619-7343-24-3, December 7, 2018, Plovdiv, pp. 153-159

[8] Denev, D. R., Tsankov, Ts. S., Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018, ISSN 1311-834X.

Имена на авторите: Линко Г. Николов
E-mail: linko.nikolov@aadcf.nvu.bg
Валентин Атанасов
Месторабота: Шуменски университет „Еп. Константин Преславски“
E-mail: v.atanasov@shu.bg

Z-WAVE COMMUNICATION FOR HOME AUTOMATION

DANIEL R. DENEV

ABSTRACT: *Z-Wave is a wireless communication protocol used primarily for home automation. It allows wireless control of household appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garages with opening doors. Z-Wave can be controlled via the Internet from smartphones, tablets, or computers, as well as locally.*

KEYWORDS: *Automation, Smart home communication, Z-Wave.*

Z-WAVE КОМУНИКАЦИЯ ЗА ДОМАШНА АВТОМАТИЗАЦИЯ

ДАНИЕЛ Р. ДЕНЕВ

АБСТРАКТ: *Z-Wave е безжичен комуникационен протокол, използван предимно за домашна автоматизация. Тя позволява безжичен контрол на битови уреди и други устройства, като управление на осветлението, системи за сигурност, термостати, прозорци, брави, басейни и гаражи с отварящи се врати. Z-Wave може да се управлява чрез Интернет от смартфони, таблети или компютри, както и локално.*

Въведение

Z-Wave е безжичен комуникационен протокол, използван предимно за домашна автоматизация. Това е мрежа и затворена верига, използваща нискоенергийни радиовълни за комуникация от уред до уред. Тя позволява безжичен контрол на битови уреди и други устройства, като управление на осветлението, системи за сигурност, термостати, прозорци, брави, басейни и гаражи с отварящи се врати. Подобно на други протоколи и системи, насочени към пазара за автоматизация на дома и офиса, системата Z-Wave може да се управлява чрез Интернет от смарт телефон, таблет или компютър, както и локално чрез интелигентен високоговорител, безжичен ключодържател или монтиран на стената панел със Z-Wave шлюз или централно управляващо устройство, служещо едновременно за контролер на концентратора и като портал отвън.

Z-Wave осигурява оперативна съвместимост на приложния слой между системите за контрол на дома на различни производители. С времето нараства броят на оперативно съвместимите продукти Z-Wave – над 1700 през 2017 г. и над 2600 до 2019 г.

Протокол и развитие

Протоколът Z-Wave е разработен от Zensys, датска компания базирана в Копенхаген през 1999 г. Същата година Zensys въвежда потребителска система за управление на светлини, която се превръща в Z-Wave като собствена система с чип (SoC) и протокол за домашна автоматизация на нелицензиран честотен обхват в честотната лента от 900 *MHz*. Нейния набор от чипове от серия 100 е издаден през 2003 г., а серията 200 е пусната през май месец 2005 г., като чипът ZW0201 предлага висока производителност на ниска цена. След дълги разработки компанията пуска и чип от серията 500 по-известен като Z-Wave

Plus. Той е с четири пъти по-голяма памет, подобрен обхват на безжична връзка и подобрен живот на батерията.

Фиг 1. Z-Wave домашна автоматизирана система

Технологията Z-Wave започва да се развива в Северна Америка през 2005 г., когато пет компании, от които Danfoss, Ingersoll-Rand и Leviton Manufacturing я приемат на конгрес. Те сформират група Z-Wave Alliance, която има за цел да насърчава използването на технологията Z-Wave, като всички продукти на компаниите в Алианса (Обединението) са оперативно съвместими една с друга. През май 2006 г. предприятието Intel Capital обявява готовността си да инвестира в Zensys 16 млн. долара, точно няколко дни след като нейния основен доставчик на микропроцесорни части Intel се присъединява към Z-Wave Alliance. През 2008 г. Zensys получава също субсидийни инвестиции от Panasonic, Cisco Systems, Palamon Capital Partners и Sunstone Capital [4], [11], [12].

Z-Wave е придобита през декември 2008 г. от Sigma Designs като нов мажоритарен собственик. След придобиването, корпоративното управление на Z-Wave се премества в Фремонт, Калифорния, където е обединено със седалището на Sigma. С преместването настъпват и частични промени. Основната търговска марка Z-Wave се запазва в САЩ от Sigma Designs, а по-малките части и технологията се прехвърля на дъщерното им дружество на Aeotec Group, което става техен представител в Европа.

На 23 януари 2018 г. Sigma обявява, че планира да продаде технологията Z-Wave и бизнес активите на Silicon Labs за 240 милиона долара.

Тъй като технологиите за интелигентен дом стават все по-популярни, през 2012 г. САЩ започват да предлагат приблизително 600 продукта, използващи технологията Z-Wave. Към януари 2019 г. има над 2600 сертифицирани с операционна съвместимост Z-Wave продукти.

Оперативна съвместимост

Оперативната съвместимост на Z-Wave в приложния слой гарантира, че устройствата могат да споделят информация и позволява на целия хардуер и софтуер на Z-Wave да работи заедно. Неговата безжична мрежова технология позволява на всеки възел да разговаря със съседни възли директно или индиректно, контролирайки всички допълнителни възли.

Възлите, които са в обсега, комуникират директно един с друг. Ако те не са в обхват, те могат да се свържат с друг възел, който е в обхват както за достъп, така и за обмен на информация. През септември 2016 г. определени части от технологията са направени публично достъпни, когато тогавашният собственик Sigma Designs пуска публична версия на слоя за оперативна съвместимост, където софтуерът е добавен към библиотеката с отворен код на Z-Wave. Наличността с отворен код позволява на разработчиците на софтуер да интегрират Z-Wave в устройства с по-малко ограничения. Защитата на Z-Wave S2, Z / IP отговаря за транспортиране на сигнали през IP мрежи без загуби на информация.

Фиг 2. Контрол на домашна мрежа чрез Z-Wave

Стандарти и Z-Wave Alliance

Z-Wave Alliance е създаден през 2005 г. като консорциум от компании, които правят свързани уреди, контролирани чрез приложения на смартфони, таблети или компютри, използвайки безжична мрежова технология Z-Wave. Съюзът е формална асоциация, фокусирана както върху разширяването на Z-Wave, така и върху продължаващата оперативна съвместимост на всяко устройство, което използва Z-Wave [1], [2].

През октомври 2013 г. е обявена нова програма за сертифициране на протокол и оперативна съвместимост, наречена Z-Wave Plus, базирана на нови функции и по-високи стандарти за оперативна съвместимост, обединени и необходими за системата от серия 500 на чип (SoC), включително някои функции, които са били на разположение от 2012 г. за SoC от серия 300 и 400. Февруари 2014 г. първият продукт е сертифициран от Z-Wave Plus. Съюзът има за цел да създаде за интелигентен дом в сигурна мрежа, която да работи на различни платформи. Z-Wave е проектиран да постигне надеждна комуникация и работа между устройства и сензорни обекти от различни производители в Z-Wave Alliance, който се състои от над 700 членове. Основните членове на „Алианса“ включват ADT Corporation, Assa Abloy, Jasco, Leedarson, LG Uplus, Nortek Security & Control, Ring, Silicon Labs, SmartThings, Trane Technologies и Vivint.

През 2016 г. Алианса стартира програма за обучение на сертифицирани инсталатори за Z-Wave, за да даде на инсталаторите и интеграторите нужните инструменти за

внедряване на мрежи и устройства на Z-Wave в техните жилищни и търговски работни места. Същата година Алиансът обявява Z-Wave Certified Installer Toolkit (Z-CIT), устройство за диагностика и отстраняване на неизправности, което може да се използва по време на настройката на мрежата и устройството и може да функционира и като инструмент за дистанционна диагностика. Z-Wave Alliance поддържа програмата за сертифициране на Z-Wave. Има два компонента за сертифициране на Z-Wave:

— техническо сертифициране, управлявано чрез Silicon Labs;
— пазарно сертифициране, управлявано чрез Z-Wave Alliance.

Фиг 3. Чип Z-Wave Plus от серията 400

Радиочестоти

Z-Wave е проектиран да осигури надеждно предаване на малки пакети данни с ниска латентност при скорости на данни до 100 *kbit/s*. Пропускателната способност е 40 *kbit/s* (9,6 *kbit/s* при използване на стари чипове) и е подходяща за приложения за управление и сензори, за разлика от Wi-Fi и други базирани на стандарта на IEEE 802.11 безжични LAN системи, които са проектирани предимно за високи скорости на предаване на данни. Разстоянието за комуникация между два възела е около 30 метра (40 метра с чип от серия 500) и с възможност за прескачане до четири пъти между възлите, което осигурява достатъчно покритие за повечето жилищни къщи. Модулацията е честотно изместване (FSK) и е кодирана с Манчестърски код.

Z-Wave използва нелицензирана индустриална, научна и медицинска лента (ISM). Той работи на 868,42 *MHz* в Европа, на 908,42 *MHz* в Северна Америка и използва други честоти в други страни, в зависимост от техните разпоредби. Тази лента се конкурира с някои безжични телефони и други потребителски електронни устройства, но избягва смущения в Wi-Fi, Bluetooth и други системи, които работят в пренаселения обхват 2,4 *GHz*. Долните слоеве, MAC и PHY, са описани от ITU-T G.9959 и са напълно обратно съвместими. През 2012 г. Международният съюз ITU включи слоевете Z-Wave PHY и MAC като опция в своя стандарт G.9959 за безжични устройства под 1 *GHz*. Скоростта на предаване на данни включва 9600 *bps* и 40 *kbps*, с изходна мощност при 1 *mW* или 0 *dBm*. Приемо-предавателните чипове Z-Wave се доставят от Silicon Labs [1], [4], [5].

Таблица 1. Използвани честоти в различни части на света

Честоти в MHz	Използвани в
865.2	India
869	Russia
868.4	China, Singapore, South Africa
868.40, 868.42, 869.85	CEPT Countries (Europe and other countries in region), French Guiana
908.40, 908.42, 916	USA, Canada, Argentina, Guatemala, The Bahamas, Jamaica, Barbados, Mexico, Bermuda, Nicaragua, Bolivia, Panama,
	British Virgin Islands, Suriname, Cayman Islands, Trinidad & Tobago, Colombia, Turks & Caicos, Ecuador, Uruguay
916	Israel
919.8	Hong Kong
919.8, 921.4	Australia, New Zealand, Malaysia, Brazil, Chile, El Salvador, Peru
919–923	South Korea
920–923	Thailand
920–925	Taiwan
922–926	Japan

Настройка на мрежа, топология и маршрутизация

Z-Wave използва мрежова архитектура която е насочена към източника – мрежата. Мрежите с затворена верига са известни още като безжични ad hoc мрежи. В такива мрежи устройствата използват безжичния канал за изпращане на контролни съобщения, които след това се предават от съседни устройства по вълнообразен начин. Изходното устройство, което иска да предава, е известно като инициатор [6], [8]. Следователно, инициираното от източника устройство инициира мрежово ad hoc маршрутизиране. В началото на 90-те години са били предложени няколко протокола за маршрутизиране на мрежи, инициирани от източника. По-ранните са били:

- Ad hoc On-Demand;
- Distance Vector Routing (AODV);
- Dynamic Source Routing (DSR).

Устройствата могат да комуникират помежду си, като използват междинни възли за активно движение и заобикаляне на битови препятствия или радио вълни и мъртви точки, които могат да възникнат в многопътечната среда на дадена къща. Съобщение от възел A до възел C може да бъде доставено успешно, дори ако двата възела не са в обхвата, при условие че трети възел B може да комуникира с възли A и C. Ако предпочитаният маршрут е недостъпен, създателят на съобщение ще опита други маршрути докато се намери път до възела C. Следователно мрежата на Z-Wave може да обхваща много по-далеч от обхвата на едно радио устройство. Като малък минус може да се причислят няколко от тези скокове, но е възможно да се въведе леко забавяне между командата за управление и желания резултат. Най-простата мрежа е едно управляемо устройство и първичен контролер.

По всяко време могат да се добавят допълнителни устройства, както и вторични контролери, включително традиционни ръчни контролери, контролери за ключодържатели, контролери за стенен превключвател и компютърни приложения, предназначени за

управление и контрол на Z-Wave мрежа. Мрежата на Z-Wave може да се състои от до 232 устройства, с възможност за свързване на мрежи, ако се изискват повече устройства. Устройството трябва да бъде "включено" в мрежата на Z-Wave, преди да може да се управлява чрез Z-Wave. Този процес (известен също като „сдвояване“ и „добавяне“) обикновено се постига чрез натискане на поредица от бутони на контролера и на устройството, което се добавя към мрежата. Тази последователност трябва да се извърши само веднъж, след което устройството винаги се разпознава от контролера. Устройствата могат да бъдат премахнати от мрежата на Z-Wave по подобен процес [7], [9], [14].

Контролерът научава силата на сигнала между устройствата по време на процеса на включване, като по този начин архитектурата очаква устройствата да бъдат на предвиденото им крайно местоположение, преди да бъдат добавени към системата. Обикновено контролерът има малко вътрешно резервно копие на батерията, което позволява временно да се изключи и да се отведе на мястото на ново устройство за сдвояване. След това контролерът се връща на нормалното си местоположение и се свързва отново. Всяка мрежа на Z-Wave се идентифицира с мрежов идентификатор, а всяко устройство допълнително се идентифицира с идентификатор на даден възел. Network ID (наричан още Home ID) е общата идентификация на всички възли, принадлежащи към една логическа Z-Wave мрежа. Мрежовият идентификатор има дължина от 4 байта (32 бита) и се присвоява на всяко устройство от основния контролер, когато устройството е включено в мрежата.

Възлите с различни мрежови идентификатори не могат да комуникират помежду си. Node ID е адресът на единичен възел в мрежата. Идентификаторът на възела има дължина от 1 байт (8 бита) и трябва да бъде уникален в своята мрежа. Чипът Z-Wave е оптимизиран за устройства, захранвани от батерии, и през повечето време остава в режим на пестене на енергия, за да консумира по-малко енергия, събуждайки се само за изпълнение на своята функция. В мрежи със затворена верига Z-Wave всяко устройство в къщата отскача и изпраща безжични сигнали около къщата, водещо до ниска консумация на енергия, което позволява на устройствата да работят години наред, без да е необходимо да сменят батериите. За да могат Z-Wave да маршрутизират нежелани съобщения, те не трябва да бъдат в режим на заспиване. Следователно устройствата, работещи с батерии, не са проектирани като ретранслатори.

Сигурност

Z-Wave се основава на патентован дизайн, поддържан от Sigma Designs като негов основен доставчик на чипове, но като бизнес единица Z-Wave е придобита от Silicon Labs през 2018 г. През 2014 г. Mitsumi става лицензиран втори източник за чипове от серията Z-Wave 500. Въпреки че има редица академични и практически изследвания на сигурността на системите за домашна автоматизация, базирани на протоколи Zigbee и X10, изследванията все още са в зародиш, за да анализират слоевете на стека на протокола Z-Wave, изискващи дизайна на устройство за улавяне на радио пакети и свързания софтуер за прихващане на комуникации Z-Wave.

Ранна уязвимост е разкрита в AES-криптирани брави за вратите на Z-Wave, които могат да бъдат експлоатирани дистанционно, за отключване на врати без знанието на ключовете за криптиране. Уязвимостта не се дължи на недостатък в спецификацията на протокола Z-Wave, а е грешка при внедряването от производителя на бравата. На 17 ноември 2016 г. Z-Wave Alliance обявява по-строги стандарти за сигурност на устройства, които получават сертификат Z-Wave. Той е по известен като Security 2 (или S2), като

осигурява разширена сигурност за интелигентни домашни устройства, шлюзове и хъбове. Z-Wave утвърждава стандарти за криптиране за предавания между възли и налага нови процедури за сдвояване за всяко устройство, с уникални ПИН или QR кодове на всяко устройство. Новият слой за удостоверяване има за цел да попречи на хакерите да поемат контрола върху незащитени или лошо защитени устройства. Според Z-Wave Alliance новият стандарт за сигурност е най-модерната защита, предлагана на пазара за интелигентни домашни устройства и контролери, шлюзове и хъбове [3], [10], [13].

Фиг 4. Устройства работещи с Z-Wave

Хардуер

Чипът за Z-Wave е ZW0500, изграден около микроконтролер Intel MCS-51 с вътрешен системен часовник от 32 *MHz*. РЧ частта на чипа съдържа приемо-предавател GisFSK за избираема от софтуера честота. С захранване от 2,2-3,6 волта той консумира 23 *mA* в режим на предаване. Неговите функции включват AES-128 криптиране, 100 *kbps* безжичен канал, едновременно слушане на множество канали и USB VCP поддръжка.

Фиг 5. Чип Z-Wave ZW0500

Сравнение с други протоколи

За интелигентните домашни безжични мрежи има многобройни технологии, които се конкурират, за да се превърнат в стандарт за избор. Wi-Fi консумира много енергия, а Bluetooth е ограничен в обхвата на сигнала и броя на устройствата. Други мрежови стандарти, конкуриращи се с Z-Wave, включват Wi-Fi, HaLow, Bluetooth 5, Insteon, Thread и ZigBee. Z-Wave има дълъг работен обхват на открито от 90 метра и 24+ метра на закрито. Теоретично Insteon може да адресира голям брой устройства на 17,7 милиона (в сравнение с 65 000 на ZigBee и 232 на Z-Wave). Thread има бърза скорост на предаване на данни при 250 *kbps*. Z-Wave има по-добра оперативна съвместимост от ZigBee, но ZigBee има по-бърза скорост на предаване на данни. Thread и Zigbee работят на натоварената Wi-Fi стандартна честота от 2,4 *GHz*, докато Z-Wave работи на 908 *MHz* в САЩ, което има намален шум и по-голяма площ на покритие. Z-Wave MAC / PHY е глобално стандартизиран от Международния телекомуникационен съюз като радио ITU 9959.

Заключение

Z-Wave са уреди от ново поколение, работещи с оптимизирани протоколи и спомагащи са усъвършенстването и осъвременяването на домашната автоматизация. Очаква се през 2021 година да бъдат представени още 100 нови устройства работещи с технологията Z-Wave, които да разширят домашната автоматизация.

ЛИТЕРАТУРА:

[1] Беджев, Б., Петров, П., Трифонов, Т. Кодове за логическо разделяне на абонатите в перспективните персонални комуникационни системи. Научна сесия на НВУ „В. Левски“ – Факултет „Авиационен“, Д. Митрополия (2003).

[2] Цонев, И., Василев, Д. Постигане високи показатели на предаване на данни в мобилните комуникации. Научна конференция с международно участие „MATTEX 2014“, Шумен (2014).

[3] Цонев, И., Станев, С. Компютърни мрежи и комуникации. Университетско издателство „Епископ К. Преславски“, Шумен, ISBN 978-954-577-496-6 (2008).

[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, Bulgaria (2017).

[5] Kazakov, S., Trifonov, T., Tsonev, I. Probabilistic-temporal characteristics in a three level centralized computer structure. Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, Liepaya, Latvia (2014).

[6] Konstantinova, E., Tsankov, Ts. Analyzing security threats in smart homes technology. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, ISSN 2367-7902 (2020).

[7] Konstantinova E., Tsankov Ts. Capabilities for high-speed data transmission through the use of visible light. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, ISSN 2367-7902 (2020).

[8] Mazadzhiev, G.N., Evlogiev, S.S., Atanasov, V.T. Conceptual model of smart home mobile technological system. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2019, Collection of papers, ISSN 2367-7902 (2019).

[9] Nikolov, L. Network Infrastructure for Cybersecurity Analysis. Proceedings of International Scientific Conference “Defense Technologies”, Shumen, ISSN 2367-7902 (2018).

[10] Vasilev, D. Monitoring research in university area of the electromagnetic field in the frequency range 800 MHz – 2200 MHz. Proceedings of the 11-th Baltic – Bulgarian International Conference on BPBMMR, Riga (2016).

[11] Vasilev, D., Tsonev, I. Radio frequency requirements in acqisition, design and construction phases of sites. Journal Science Education Innovation, Vol. 5, ISSN 1314-9784 (2015).

[12] https://www.electronicdesign.com/technologies/communications/article/21796052/whats-the-difference-between-zigbee-and-zwave?fbclid=IwAR25k1dh3rvbCq3fW3trqKWexFhr8iTE2R3CW_MmoXn4jtR9V8CSFhJTdMg

[13] https://www.lifewire.com/what-is-z-wave-4588924

[14] https://www.techhive.com/article/2031180/sigma-designs-announces-next-gen-z-wave-home-control-product-family.html?fbclid=IwAR1UYdtlIMSDiALhJXi6VEGgrA-yC4hHaYOPjGuzfn8orsgeFYNNmxBURTw

Име на автора: инж. Даниел Росенов Денев
Докторант в кат. ККТ, ФТН на Шуменски университет „Епископ Константин Преславски“
E-mail: Slimshady33@abv.bg

SOLID STATE RELAYS (SSR) IN INDUSTRIAL AUTOMATION

HRISTO H. HADZHIIVANOV

ABSTRACT: *In the last few years, semiconductor relays have been increasingly used instead of electromechanical relays. This article discusses the structure, parameters and specification, advantages and disadvantages of SSR and electromechanical relays.*

KEYWORDS: *Industrial Automation SSR, Semiconductor relay, SSR, relay, SSR selection, SSR types*

ПОЛУПРОВОДНИКОВИ РЕЛЕТА (SSR) В ИНДУСТРИАЛНАТА АВТОМАТИЗАЦИЯ

ХРИСТО Х. ХАДЖИИВАНОВ

АБСТРАКТ: *В последните няколко години все повече се използват полупроводникови, вместо електромеханични релета. В настоящата статия е разгледана структурата, параметрите и спецификацията, предимствата и недостатъците на SSR и електромеханичните релета.*

1 Въведение

Индустрията има важна роля в съвременната икономика, което води до повишаване на изискванията към индустриалните контролери за управление на производствените машини и останалите периферни устройства.

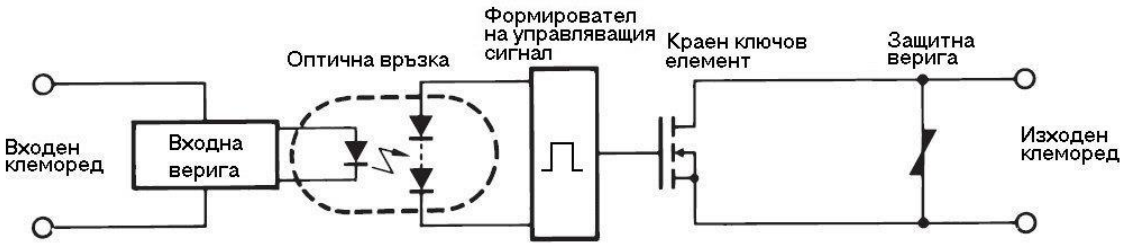
Първите PLC контролери се появяват след 1960 г., като след 1980 г. започва бурното им внедряване в производствените машини, което отваря и пътя за по лесното навлизане в употреба на полупроводникови релета на мястото на електромеханичните. Преди да започне прилагането на PLC контролерите, в релейно-контактните системи са се използвали изцяло електромеханични релета за логиката и управлението на процесите. Към настоящия момент все повече се използват SSR релета в контролерите и извън тях.

В настоящата статия ще бъде разгледана структурата и принципа на работа на SSR релетата, техни основни параметри, както и техните предимствата и недостатъци.

2 Структура, принцип на работа и характеристики

На фиг.1 е показана блоковата структура на полупроводниково реле, като на фиг.2 част от блоковете са заменени с полупроводникови елементи.

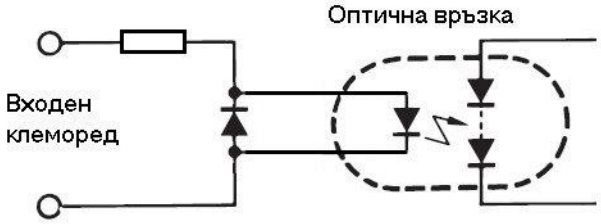
Фиг.1 Блокова схема на SSR.



Фиг.2 Функционална схема на SSR.

2.1 Входна верига

Входната верига служи за съгласуване на входния сигнал с фото диода в оптронната двойка. Известно е, че диода изисква работен ток в определени минимални и максимални граници. В случая когато има фиксирано входно работно напрежение, например 24 V_{DC} което е стандартно за автоматизацията, входната верига е опростена. Тя се състои от един резистор последователно свързване на фотодиода и защитен диод обратно свързан на фотодиода, който предпазва от обратно подаване на управляващото напрежение - Фиг.3. Когато входно напрежение е в по широки граници, например 4-32 V_{DC}, входната верига е по сложна. Входната верига представлява генератор на ток, като токът през фотодиода се подбира да е оптимален за оптрона. При SSR релетата управляващата и управляваната верига може да бъдат за прав и променлив ток.

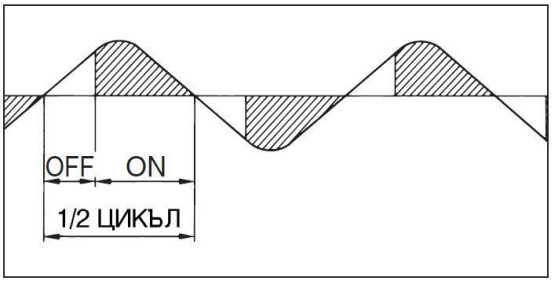


Фиг.3 Опростена входна верига.

a. Изолираща оптична връзка

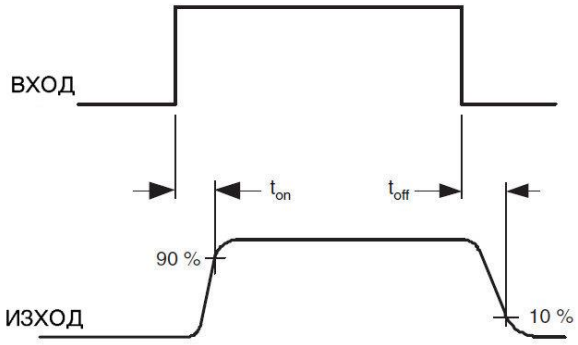
Изолиращата оптична връзка представлява оптрон с, който се постига галванично разделяне между входната и изходната верига. В зависимост от това какъв е крайният изходен ключов елемент на SSR релето, изходът на оптрона е с различно полупроводниково изпълнение.

b. Формирователь на управляващия сигнал



Фиг.4 Фазово управление.

Фиг.5 Управление през нулата.



Фиг.6 Управление при постоянен ток.

Тази схема обработва постъпилия входен сигнал и определя дали изхода трябва да е включен или не (затворена или отворена електрическата верига).

При изход за променлив ток може да има фазово управление и управление през нулата. При фазовото управление SSR изхода се включва (затваря се веригата) веднага с подаване на управляващ сигнал и се изключва след отпадане на входния сигнал и завършване на полупериода фиг.4. При управление през нулата, изходът се включва след подаване на управляващ сигнал и преминаване през нулата на управляваната верига - Фиг.5.

При изход за постоянен ток формиращата верига трябва да осигури управляващ сигнал за бързо превключване на изходната верига фиг.6.

При изход за прав и променлив ток изходът се включва веднага с подаване на управляващ сигнал и се изключва веднага след неговото отпадане.

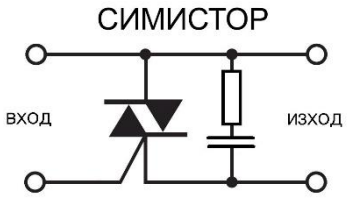
с. Краен ключов елемент

Този елемент е устройството което „затваря“ или „отваря“ изходния „контакт“ в управляваната верига. В зависимост от управлявания ток има следните варианти:

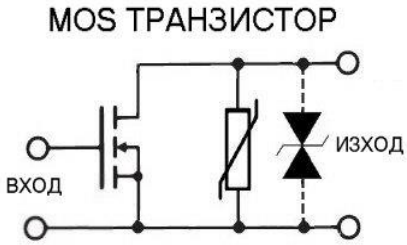
-при променлив ток се използва симистор - Фиг.7.

-при постоянен ток се използва MOS транзистор - Фиг.8, в редки случаи това е биполярен транзистор - Фиг.9.

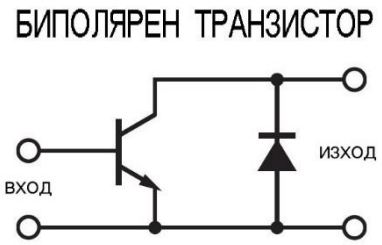
-при управление на прав и променлив ток за ниски напрежения се използват два противоположно свързани MOS транзистора - Фиг.10.



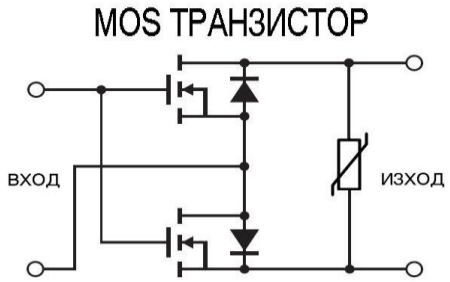
Фиг.7 Ключ за променлив ток.



Фиг.8 Ключ за постоянен ток.



Фиг.9 Ключ за постоянен ток.



Фиг.10 Ключ за постоянен и променлив ток.

d. Защитна верига

За разлика от електромеханичните релета, SSR релетата са по чувствителни от пикови и обратни напрежения. При различните управлявани напрежения (прав или променлив ток) има различно схемно решение. При управление на променлив ток се използва последователно свързани резистор и кондензатор, както е показано на фиг.7. Тази верига намалява амплитудата и стръмността на смущенията и подобрява преходните процеси при комутацията. При управление на постоянен ток или прав и променлив ток се използва варистор или трансил - Фиг.8. В този вариант се ограничава амплитудата на напреженията от самоиндукция.

e. Параметри и спецификация на SSR

Ще бъдат разгледани по-важните параметри на SSR, като част от параметрите не са точно стандартизирани и при различните производители са различни, а за някои от тях липсва информация.

От механична гледна точка SSR са два вида – релета в корпус на стандартно електромеханично реле и монолитни релета с входни и изходни клемореди.

Релетата в корпус на стандартно електромеханично реле се монтира на цокъл с клеморед за входния и изходния сигнал. С тези релета се прави лесна подмяна на старите релета, когато те са с еднакви цокли. Другият тип са монолитни с входните и изходните клемореди, които са по-неудобни за подмяна и диагностика при повреда на SSR релето или външните вериги.

В качеството на пример за SSR в корпус за монтаж на цокъл ще бъде разгледано полупроводниковото реле WAGO 788-701. Неговите основни параметри по данни от производителя са следните:

ВХОДНА ВЕРИГА

1	Номинално входно напрежение U_N	24VDC
2	Входно напрежение за логическа нула	0. . .2.5 V_{DC}
3	Входно напрежение за логическа единица	15. . .30 V_{DC}
4	Номинален входен ток при U_N	9.3 mA

ИЗХОДНА ВЕРИГА

5	Схема на свързване	двупроводна
6	Продължителен товарен ток	5 A
7	Изходно номинално напрежение	24 V_{DC}
8	Обхват на изходното напрежение	0. . .30 V_{DC}

9	Пад на напрежение при максимален товар	≤ 0.3 V_{DC}
10	Време за включване	≤ 50 μS
11	Време за изключване	≤ 600 μS
12	Честота на превключване	≤ 100 Hz

СИГНАЛИЗАЦИЯ

13	Сигнален индикатор	червен светодиод

БЕЗОПАСНОСТ И ЗАЩИТА

14	Изолация между входната и изходната верига	2,5 kVeff
15	Степен на защита	IP20
16	Температура на околната среда при работа при U_N	-40. . .70 °C
17	Температура на околната среда при съхранение	-40. . .70 °C
18	Работна температура	-25. . .50 °C

Описанието на параметрите е по групи, като първо се започва с входната верига. Първия параметър е номинално входно напрежение. Това е сигналът с който се управлява SSR релето и съответства на напрежението на бобината на електромеханичното реле, като в този случай то е за стандарт 24 V_{DC}. Със следващите параметри 2 и 3 се определя интервала в който сигналът се счита за логическа „единица“ и логическа „нула“. Аналогично на механичното реле с нормално отворен контакт има две състояния – отворен („нула“) и затворен („единица“) контакт. Параметър 4 е входния ток при номинално входно напрежение.

Следващите параметри се отнасят за изходната верига на товара – управлявана верига. Параметър 5 е схемата на свързване, в случая с два проводника. Това означава, че не е необходимо захранване, има само контакт. Продължителния товарен ток е даден в параметър 6. Номинално напрежение е 24 V_{DC} и е даден обхват на изменение 0. . .30 V_{DC}, параметри 7 и 8. Получения пада на напрежение при максимален ток е даден в параметър 9. Когато има чести превключвания са важни времената за включване и изключване (Фиг.6) и честотата на превключване които са дадени в параметри 10,11 и 12.

При повечето SSR релета има сигнализация дали е подаден управляващ сигнал, това е параметър 13.

В групата за безопасност и защита е дадена каква е изолацията между входната и изходната верига, параметър 14. , а степента на защита от околната среда е параметър 15.

Последната група е за температурите за съхранение и работа. Тези параметри са не по-маловажни от другите. Температурата за съхранение е винаги с по-голям диапазон от тази в един склад за резервни части в автоматизацията, както се вижда от параметър 17. В производствените помещения условията са тежки от температурна гледна точка, затова трябва да обърнем внимание на температурата на околната среда, дали е в границите в които ще се експлоатира SSR релето, параметър 18.

f. Предимства и недостатъци на полупроводниковите релета в сравнение с електромеханичните релета.

Предимства:

- Малка мощност (консумация) в управляващата верига
- Синхронизирано или не синхронизирано превключване

- Много ниски смущения при управление през нулата за променлив ток
- Много ниски електромагнитни смущение, поради липсата на бобина
- Много ниски смущения поради липса на искрене
- Много дълъг експлоатационен живот (няма движещи се механични части)
- Висока скорост и честота на превключване (няма движещи се механични части)
- По-добра съвместимост с цифровите устройства за управление
- Безшумна работа

Недостатъци :

- При отворен контакт имат нищожна проводимост, която има значение в някои случаи
- Изходната верига в повечето случаи се избира дали е за прав или променлив ток
- Необходимост от радиатор за по големи токове на управление
- Използват се за управление на малки мощности

3 Заключение

В настоящата статия, бяха разгледани полупроводниковите релета (SSR), които се използват в автоматизацията на производството. Съществуват и SSR релета в други приложения на техниката. Например във всяка съвременна автоматична пералня се използват SSR релета, но те обикновено са част от печатната платка и др..

В предните глави се разгледа блоковата схема, вътрешната структура на едно SSR реле, неговите основни параметри, предимства и недостатъци в сравнение с електромеханичните релета. Тази информация ни дава основни знания за полупроводникови релета (SSR) използвани в автоматизацията на технологични процеси и би била полезна при избор на SSR реле.

ЛИТЕРАТУРА:

[1] OMRON Technical Explanation for Solid-state Relays

[2] OMRON Solid-state Relays

[3] Crouzet University, Solid-State Relays Technical Manual

[4] Solid State Optronics, San, Jose, CA, 2014, Solid State Relays vs. Electromechanical Relays

[5] Сп. Инженеринг ревю - брой 9/2017 • 09.01.2018, Интегрални полупроводникови релета (SSR)

[6] Сп. Инженеринг ревю - брой 8, 2012, Полупроводникови релета (SSR)

Име на автора: Христо Хадживанов
Месторабота: Шуменски университет „Епископ Константин Преславски“
E-mail: h.hadzhiivanov@shu.bg

MAIN ISSUES IN THE PROTECTION OF INFORMATION IN THE SYSTEM OF NATIONAL AND CORPORATE SECURITY

DANIEL R. DENEV, EKATERINA M. KONSTANTINOVA

ABSTRACT: *Cryptography is involved in ensuring information security in the systems of national and corporate security. It provides processing and transformation of information in a form that is protected and not publicly available to everyone.*

KEYWORDS: *Cryptography, Information, Keys.*

ОСНОВНИ ПРОБЛЕМИ ПРИ ЗАЩИТАТА НА ИНФОРМАЦИЯТА В СИСТЕМАТА НА НАЦИОНАЛНАТА И КОРПОРАТИВНАТА СИГУРНОСТ

ДАНИЕЛ Р. ДЕНЕВ, ЕКАТЕРИНА М. КОНСТАНТИНОВА

АБСТРАКТ: *В осигуряването на информационна безопасност в системите на националната и корпоративна сигурност заляга криптографията. Чрез нея се осигурява обработка и трансформация на информацията в вид, който е защитен и не е общодостъпен за всеки.*

Въведение

В осигуряването на информационна безопасност в системите на националната и корпоративна сигурност съществуват два основни актуални проблема.

При първия, в условията на пазарната икономика, когато съществува остра и безкомпромисна конкуренция между двата пазарни субекта, възниква интерес помежду им, за тяхната работна организация (фирма).Този интерес е насочен към добиването на информация, която се отнася към сферата на комерсиалните тайни. По-конкретно, фирмите се опитват да се доберат до следните важни сведения за конкурентите си:

- същността на пазарните стратегии;
- финансовото състояние;
- клиентите;
- маркетинговите цени на стоки;
- системите от дистрибутори и доставчици.

В резултат на това възникват много проблеми със съхраняването и защитата на информацията във фирмените комуникационно-информационни системи. Това е така, защото бизнесът неразривно е свързан с получаването, натрупването, обработката и използването на разнообразни масиви информация [3], [5]. При това злонамерените лица в бизнеса преследват три основни цели:

- тайно получаване на информация, която може да повлияе върху стратегиите и тактиките на конкурентната борба;
- въвеждане на изменения в информационните потоци на конкурентите, които да доведат до тяхната дезинформация;
- унищожаване на ценни за конкурентите сведения, чертежи, масиви от данни.

При втория проблем, в началото на 90-те години на XX век настъпва нов етап във възгледите за използване на комуникационно-информационните системи. Те са необходими както за нуждите на армията ,така и за нуждите на обществото. Този нов етап е свързан с изключително нарасналата роля на компютърните и комуникационните системи

Понятието информация.

Понятието информация произхожда от латинския термин “informatio”, който означава разяснение или изложение. В най-общи позиции може да се каже, че информацията са сведенията, предавани между хората устно, писмено или по друг начин.

Изчерпателни научни определения за информацията досега не са давани, но са направени за някои тесни научни области, като например общата теория на комуникационните системи. Американският теоретик К. Шенон със своята книга „Математическа теория на свръзките“, слага началото на теорията на информацията.

Предмет на теорията на информацията е понятието информация и неговото измерване, принципите на кодиране и модулация, възприятието, предаването, представянето и преработка на информацията.

Задачата на теорията на информацията е да изучава своя предмет и на тази база да даде възможност на хората да преобразуват заобикалящата ги природна среда съобразно с техните потребности.

Теорията на информацията се състои от няколко основни клона:

- математическа теория на свръзките;
- логически основи на компютърната техника;
- теория на програмирането;
- теория на възприемането на сигналите от човека;
- теория на игрите;
- теория на управлението.

Теорията на информацията има отношение спрямо кибернетиката, тъй като освен чисто информационни обекти разглежда и обектите и целите на човешката дейност, общите технологични процеси, както и обратните връзки. В рамките на теорията на информацията се използват следните понятия:

Информация – това е съвкупност от сведения, получаването и осмислянето на които отстранява непълнотата, неточността и неопределеността в нашето познаване на някакво явление или предмет.

Съобщение – това е материалната форма на информацията.

Сигнал – в широк смисъл това е съобщение, предназначено за предаване на голямо разстояние.

Източникът на информация е: човек; някаква памет, в която са съхранени съобщения или някакъв датчик [1], [5].

Съобщенията постъпват от източника в предавателя, където се преобразуват в сигнали, които могат да преминат през канала за свръзка. Той е между източника на информация и нейния получател. Това преобразуване се нарича кодиране и много често протича на два етапа. На първия етап в кодера на източника, а на втория етап, каналният кодер. След кодиране сигналите във високочестотни сигнали, които могат да преминат през канала за свръзка. Ето защо каналният кодер се нарича още модулатор. Линията за свръзка, преодоляваща разстоянието между източника на информация и получателя на информация може да бъде кабел, вълновод, водно, въздушно или безвъздушно пространство. Към

линията за свръзка на схемата е включен източник на смущения. Математически това е некоректно, тъй като смущенията действат на сигналите във всички елементи на канала за свръзка. Идеята е в това, че от всички смущения действащи в канала, най-непредсказуеми и следователно най-опасни за цялата система за свръзка, са смущенията в линията за свръзка [2], [7].

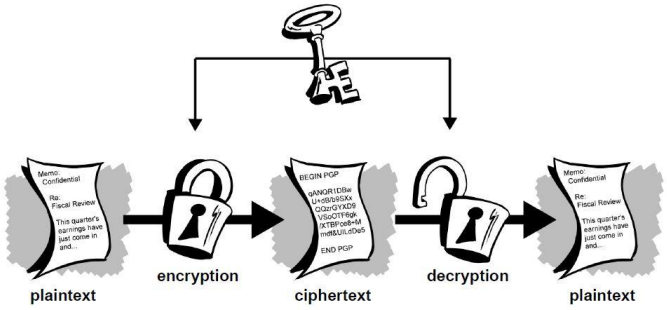
На другия канал на линията сигналът се преобразува във вид удобен за възприемане от получателя на информация. Много често това става на два етапа. На първия етап сигналът се демодулира, а на втория се представя на дисплеи.

Криптография

Възможността за комуникация винаги е била ключов момент в придобиването на знания в еволюцията на човечеството. Исторически най-голяма необходимост от сигурна комуникация е имало по време на конфликти между народите. В днешно време, където ежедневно се използват голям брой комуникационни средства, нуждата от тайна е предмет на голям брой приложения. Например софтуерните компании искат да защитят техните продукти от пиратство, банките искат да осигурят сигурни транзакции и почти всеки иска да запази своята информация в тайна. Нуждата от сигурни комуникации ражда една нова наука, наречена криптография.

Шифрираща система или криптосистема е технология, използвана за скриване на съобщенията от нежелани получатели. Криптографията е наука, която създава такива технологии, докато криптоанализът е изкуството за разкриване или разбиване на криптосистеми с цел прочитане на дадено съобщение от някой, който не е желаният получател. Терминът криптография включва криптоанализа. Той произлиза от гръцките думи – скрит и наука.

Оригиналното съобщение, което трябва се изпрати се нарича открит (явен) текст (plain text). Шифрираното съобщение се нарича шифротекст (cipher text). Шифрирането е процес на преобразуването на простия текст в шифротекст, обикновено използвайки някакъв алгоритъм и ключ (фиг. 1). Ключът е този компонент, който се предава тайно между изпращащия и получаващия съобщението и може да бъде различен във всяко едно съобщение. Ключът обикновено се нарича и криптопроменлива. Дешифрирането е процесът на преобразуване на шифротекста в явен текст. Този процес обикновено произхожда от знанието на използвания шифриращ алгоритъм и ключа.



Фиг. 1. Операция по криптиране и декриптиране

Криптографията е науката, свързана със създаването на математически методи и средства за защита на информацията, обезпечаваща конфиденциалност, цялостност, идентификация, автентификация и ред други функции [4], [8]. Въпросът за безопасността е

важна част от концепцията за внедряване на нови информационни технологии във всички сфери на живота на съвременното общество. Основни определения в криптографията са:

Шифриране – то е процесът на „маскиране“ на съобщението със способи, позволяващи скриването на неговата същност.

Шифър – това е съвкупност от обратими преобразувания на множествата на откритите данни в множествата на зашифрованите данни по зададени алгоритми за криптографски преобразувания.

Шифротекст (криптограма) се нарича зашифрованото съобщение.

Дешифрирането е процесът на преобразуването на шифротекста в открит текст.

Криптосистема – това е система, реализираща програмно, апаратно или програмно-апаратно криптографско преобразуване на информацията. Тя се състои от множествата на ключовете на откритите текстове, шифротекстовете и алгоритмите за шифриране и дешифриране.

Ключ – това е променливият елемент на шифъра, използван за шифриране на отделно съобщение, обезпечаващ избор на един вариант преобразуване от множество възможни преобразувания. Ключа определя криптоустойчивостта на системата за защита на информацията.

Устойчивостта на криптоалгоритъмът (криптоустойчивост) се заключава в способността на шифъра да противостои на атаките за неговото разшифроване. Криптоустойчивостта зависи от сложността на алгоритъма за преобразуване, дължината на ключа и обема на ключовото множество. Известни са няколко типа атаки на криптографските алгоритми:

- атака при известен шифротекст – при нея се предполага, че противника знае алгоритъма за шифриране, има набор от прехванати криптограми, но той не знае секретния ключ;
- атака при известен открит ключ – когато противника има достъп не само до шифротекста на няколко съобщения, но и до откритият текст на тези съобщения;
- проста атака с избор на открит текст – когато в противника има информация не само за шифротекста и откритият текст на няколко съобщения, но може и да избира открит текст за шифриране;
- адаптивна атака с избор на открит текст – криптоанализа има възможност да избира откритите текстове с отчитане на това, че криптограмите на всички предходни открити текстове са му известни.

Съответните криптографски алгоритми могат да се класифицират по степента на доказване на нивото на устойчивост – безусловно устойчиви и доказано устойчиви. Безусловно устойчивите криптоалгоритми гарантирано не позволяват разриването на ключа. Безопасността на доказано устойчивите криптоалгоритми се определя от сложността на решаването на добре изследвани задачи, например разлагането на числа на множители. Отличителна особеност на тези криптоалгоритми е тяхната „твърдост“.

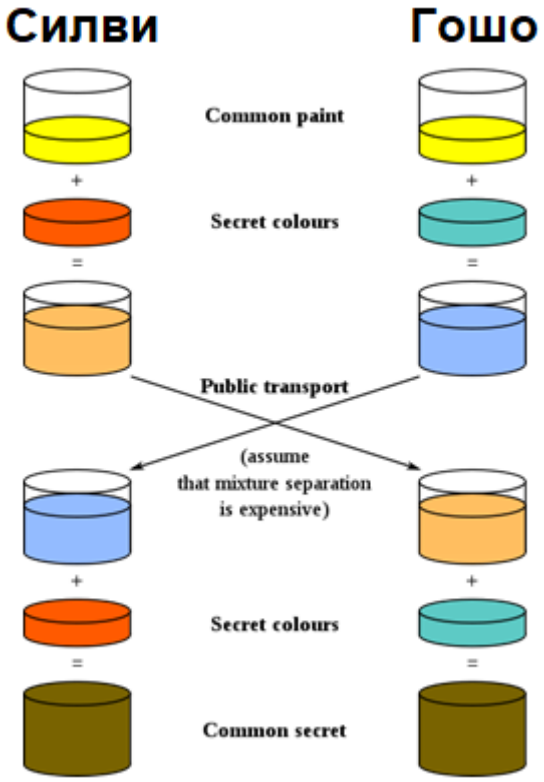
Сигурна криптирана комуникация

Традиционно сигурната криптирана комуникация се извършва между две страни, като се изисква те да си обменят ключове по сигурен физически канал [4], [6], [9]. Методът на размяната на ключове на Diffie-Hellman, позволява на две страни, които нямат предварително познание помежду си, една за друга, да създадат съвместно таен ключ по

несигурен канал. Този ключ може да бъде използван за криптиране на последващите комуникации чрез използване на симетричен шифър за ключове (фиг. 2).

Криптографско обяснение на алгоритъма чрез пример:

По най-достъпния и елементарен начин се използва мултипликативната група от цели числа mod (модул) P, където P е основен и G е примитивен корен на P. Тези две стойности се избират по този начин, за да се гарантира, че получената споделена тайна може да приеме всяка стойност от 1 до P-1. В примера ще маркираме нецелеви стойности в синьо и тайни стойности в червено.



Фиг. 2. Пример по Алгоритъма за обмен на ключове на Diffie-Hellman

ПРИМЕР:

Силви и Гошо се съгласяват да използват число **mod p = 23** и основа $g = 5$ (която е примитивен корен на 23).

Силви избира скрито цяло число $\boldsymbol{a} = 4$, тогава изпраща на Гошо $A = g^a \bmod p$

- $A = 5^4 \bmod 23 = 4$

Гошо избира скрито цяло число $\boldsymbol{b} = 3$, тогава изпраща на $B = g^b \bmod p$

- $B = 5^3 \bmod 23 = 10$

Силви computes $\boldsymbol{s} = B^a \bmod p$

- $\boldsymbol{s} = 10^4 \bmod 23 = 18$

Гошо computes $s = A^b \bmod p$

- $s = 4^3 \bmod 23 = 18$

Силви и Гошо сега споделят скритото число 18.

Извод : Силви и Гошо стигат до една и съща стойност s, защото, под mod p следва,

$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p$ и по-точно

$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$

Заключение

Основната задача в теорията на информацията е да разработва оптимални методи за кодиране и декодиране на информацията, така че информацията да достига получателя с максимална пълнота и точност.

ЛИТЕРАТУРА:

[1] Беджев, Б., Петров, П., Трифонов, Т. Кодове за логическо разделяне на абонатите в перспективните персонални комуникационни системи. Научна сесия на НВУ „В. Левски“ – Факултет „Авиационен“, Д. Митрополия (2003).

[2] Николов, Н.Р., Цанков, Ц.С., Трифонов, Т.С., Дъчева, В.А. Изследване на съставен генератор на псевдослучайни последователности, използващи хаос атрактор на Лоренц. Национална конференция с международно участие „40 години Шуменски университет 1971-2011“, Шумен, ISBN 978-954-577-620-5 (2011).

[3] Стаменова, А.В., Диманова, Д.В., Цанков, Ц.С. Новите войни на XXI век. Научна конференция MATTEX 2014, Шумен, ISSN 1314-3921 (2014).

[4] Цанков, Ц., Трифонов, Т. Алгорифм для вычисления линейной сложности сигналов. International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, Vol. 10, Liepaya, ISBN 978-9934-10-573-9 (2014).

[5] Цонев, И., Василев, Д. Постигане високи показатели на предаване на данни в мобилните комуникации. Научна конференция с международно участие „MATTEX 2014“, Шумен (2014).

[6] Kazakov, S., Trifonov, T., Tsonev, I. Probabilistic-temporal characteristics in a three level centralized computer structure. Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, Liepaya, Latvia (2014).

[7] Nikolov, L. Network Infrastructure for Cybersecurity Analysis. Proceedings of International Scientific Conference “Defense Technologies”, Shumen, ISSN 2367-7902 (2018).

[8] Vasilev, D. Monitoring research in university area of the electromagnetic field in the frequency range 800 MHz – 2200 MHz. Proceedings of the 11-th Baltic – Bulgarian International Conference on BPBMMR, Riga (2016).

[9] Vasilev, D., Tsonev, I. Radio frequency requirements in acqisition, design and construction phases of sites. Journal Science Education Innovation, Vol. 5, ISSN 1314-9784 (2015).

Име на автора: инж. Даниел Росенов Денев
Докторант в кат. ККТ, ФТН на Шуменски университет „Епископ Константин Преславски“
E-mail: Slimshady33@abv.bg

Екатерина Минкова Константинова – студент

PROGRESS AND TRENDS IN MACHINE VISION SMART CAMERAS

DANIEL R. DENEV, TSVETOSLAV S. TSANKOV

ABSTRACT: *This paper examines some of the most interesting trends in the current development of smart cameras for machine vision. It describes the partitioning of data processing between the CPU and the increasingly utilized FPGA. Attention is paid to the ongoing tendency for miniaturization, which contributes to an even wider spread of machine vision devices into the fields of robotics, self-driving cars, and healthcare. The Industry 4.0 concept also has its impact on the progress of machine vision cameras, including the need for compatibility with industry standards facilitating the communication across all major industrial protocols. Finally, a reference is made to the available software for machine vision, including proprietary algorithms and open-source products.*

KEYWORDS: *Industry 4.0, Machine vision, Robotics, Smart cameras.*

ТЕНДЕНЦИИ В РАЗВИТИЕТО НА СМАРТ КАМЕРИТЕ ЗА МАШИННО ЗРЕНИЕ

ДАНИЕЛ Р. ДЕНЕВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Настоящата работа разглежда някои от най-забележителните тенденции в развитието на смарт камерите за машинно зрение към момента. Описано е поделянето на функциите по обработка на данни между централния процесор и FPGA. Представена е продължаващата тенденция за миниатюризация, способстваща още по-широкото навлизане на устройства за машинно зрение в роботиката, самоуправляемите автомобили и здравеопазването. Индустрия 4.0 също налага редица изисквания, в т.ч. съвместимост с промишлени мрежови стандарти с цел комуникация по всички индустриални протоколи. Накрая са представени тенденциите в наличния софтуер, включително патентовани алгоритми и отворени продукти.*

Въведение

В производствената индустрия има силен стремеж за контролиране на протичащите процеси във всичките им проявления. Това обикновено се реализира с измерване на променливите преди и след процеса. Широко използван метод за получаване на тези данни е чрез системи за машинно зрение. Те могат да заснемат изображения, да правят измервания и проверки чрез анализ на тези изображения. Възможностите на такава система зависят преди всичко от използвания хардуер и софтуер за осъществяване на анализа. Това което прави тази технология толкова мощна, е че вместо локални измервания например с лазерен или физически сензор тя може едновременно да извършва множество измервания върху само едно изображение.

Широко се използват два типа реализации на машинно зрение: смарт камери и системи с персонален компютър (ПК). Първите обикновено се състоят от лещи, сензор, интегриран модул за обработка на данни, памет, съдържаща софтуера за обработка и входно-изходни канали, реализиращи определени интерфейси. При системите с ПК камерата предава заснетите изображения чрез специален протокол към външен компютър, където се извършва обработването им [3], [4].

Използването на смарт камери започва през 80-те години на миналия век. Първоначално в тях се включват нископроизводителни процесори и се предлагат за приложения само с една конкретна цел – например четене на баркодове, локализирано вземане на решения за успех/неуспех, оптично разпознаване на символи или броене, което не изисква програмиране. Трудното управление на алгоритми за разпознаване с еталон на клас по това време означава, че сложните изображения или операции, изискващи бърз анализ, остават извън възможностите им. И все пак производителите постепенно изявяват желание да жертват производителността и гъвкавостта на системите с ПК за сметка на лекотата при работа и компактната структура на смарт камерите.

С подобряването на обработката смарт камерите започват да конкурират системите с ПК при различни приложения, включително проверка на сглобяването, инспекция чрез 1D и 2D баркодове и насочване на роботи. Те се възползват и от развитието в технологията на сензорите CMOS, в резултат на което понастоящем на пазара има голямо разнообразие от продукти с големи изчислителни възможности и резолюции. Макар вече да си проправят път към здравеопазването, охранителната и развлекателната индустрия, те основно се използват в производствения сектор, където употребата им продължава да расте – особено при необходимост от независимо инспектиране в няколко области от производствената линия, напр. в автомобилната промишленост [1], [7].

Освен все по-ниската им цена основното предимство на смарт камерите е наличието на вградени изчислителни възможности за независимо решаване на задачи за разпознаване на образи без връзка с персонален компютър. Компактният форм фактор позволява на смарт камерите да се побират в малки пространства или с тях да бъдат преоборудвани съществуващи процеси. Тъй като имат малък брой подвижни части и не генерират високи температури, разходите за поддръжката им остават ниски.

Многопроцесорна архитектура

Съвременните смарт камери могат да осигуряват скорости до 300 кадъра в секунда (*fps*) при пълна 12-мегапикселова резолюция в 10-битов режим или 140 *fps* в 12-битов режим – характеристики, които само допреди няколко години са били непостижими. Намаляването на ROI прозореца от изображението и следователно количеството данни в изображението може допълнително да увеличи скоростта.

Като елемент или модул за обработване на данни обикновено се използва централен процесор с общо предназначение (central processing unit, CPU), графичен процесор (graphics processing unit, GPU), микропроцесор за цифрова обработка на сигнали (digital signal processor, DSP) или програмируема логическа матрица (field-programmable gate array, FPGA) (фиг. 1).

Важна тенденция в развитието на смарт камерите е използването едновременно на няколко елемента за обработване на данните. Многопроцесорните архитектури са полезни за осигуряване на висока производителност при обработката на изображения, необходима в приложенията на машинното зрение, тъй като при нея дейностите може да се разпределят между отделните процесори. Например точковата обработка и подобни на нея дейности, като изравняване на хистограмите и филтриране, най-ефективно се изпълняват от FPGA, докато задачите по статистическо разпознаване с еталон на клас могат най-добре да се реализират на микропроцесор с общо предназначение.

Въпреки че архитектурата е различна при отделните смарт камери, един от дизайните, доказали високата си ефективност, включва ARM процесор, комбиниран с FPGA. Логическата матрица се справя ефикасно с предварителната обработка и

комуникационните интерфейси, за да осигури управление в реално време и нулево закъснение. Добавянето на FPGA за предварително обработване от ниско ниво е важна стъпка, тъй като освобождава процесора от тези задачи и той може да се съсредоточи върху високото ниво на обработване, което на свой ред намалява времето за изпълнение и латентността [10], [12].

Фиг. 1. Архитектура на смарт камерите

Съвременните FPGA, използвани в смарт камерите, може да се персонализират за специални целеви приложения и са предпочитана алтернатива на x86 процесорите. FPGA може вече да управлява видео преобразувателя и входно-изходните комуникации, което чувствително подобрява работата със заснетите изображения и намалява натоварването на процесора. За разлика от сложните матрици, използвани в по-старите камери, модернизираните FPGA лесно могат да бъдат програмирани с езиците VHDL, Verilog и библиотеки като OpenCL. Потребителите са свободни директно да реализират патентовани алгоритми с цел намаляване на натоварването върху процесора, така че основната му задача да остане анализирането на данните, екстраполирани от FPGA.

Разпределени мрежи

Стратегията за изграждане на мрежи от смарт камери, реализиращи разпределени алгоритми, също се доказва като ключов компонент за системите с вградено машинно зрение, който дава възможност за използване на технологии, насочени към облачни изчисления, интернет на нещата и много бъдещи приложения.

Разпределените алгоритми са предназначени да се изпълняват на хардуер, съставен от взаимно-свързани процесори и се прилагат в различни области като телекомуникации, изчислителни науки, разпределена информационна обработка и управление на процеси в реално време. Всеки от тези процесори, представляващи възли в мрежата, няма пряка информация за състоянието на останалите възли. Един възел може да извлече състоянието на друг само след получаване на съобщение от него. Предаването на съобщения в разпределените системи има нетривиална стойност, затова разпределените алгоритми целят минимизиране на броя съобщения, необходими за завършване на алгоритъма.

Разпределените смарт камери представляват реалновремеви децентрализирани мрежи от вградени системи, които изпълняват сложни задачи с машинно зрение чрез няколко (или много) камери. Този подход възниква благодарение на обединяването на едновременни постижения в четири ключови дисциплини: компютърно зрение, видео преобразуватели, вградени системи и сензорни мрежи. Разпределянето помага да се намали комуникационното натоварване в мрежата от камери и да се увеличи надеждността и

мащабируемостта на многокамерните приложения. То също така олицетворява тенденцията в сензорните мрежи за вътремрежово обработване. Всяка смарт камера, която е част от мрежата, извършва огромен брой изчисления, за да компресира данните за изображението в по-абстрактна форма, което намалява необходимата честотна лента за предаването им. Тези мрежи се възползват от основните техники в организирането на ad hoc сензорни мрежи, но освен това се нуждаят от допълнителни слоеве за управление на локалното и нелокалното обработване.

Системите от смарт камери може да се разглеждат като форма на сензорни мрежи с по-различни характеристики: по-малко възли и повече изчислителни, комуникационни и енергийни ресурси във всеки възел. Специфичните характеристики на разпределените камери като сензорни мрежи водят до някои важни проблеми. Повишената скорост на изчисление и комуникация извиква нужда от по-усъвършенствани услуги за разпределени изчисления, например мигриране на задачите и балансиране на натоварването. Тези услуги са особено важни при приложения с повишена сигурност. Необходимо е точно калибриране на мрежите от камери, както в пространството, така и във времето. Когато към системата се добави и звукова информация, времевото калибриране става дори още по-важно [9], [11].

Смарт камерите може да се комбинират с данни от сензори на други свързани устройства и по този начин да се добие представа за това, как всяка стъпка и променлива влияе върху крайния продукт. Всички приложения на разпределените смарт камери изискват сливане на данните от изображения с цел интерпретиране на сцената. Тъй като обектите на интерес имат сложни геометрични отношения помежду си, за анализирането им може да е необходимо взаимодействие между различни групи от камери. Поради движението на обектите е възможно групите от взаимодействащи си камери да се променят бързо. Предаването на цялото видео съдържание от голям брой камери към централен сървър изисква много ресурси и по своята същност е немащабируемо. Комбинацията от много на брой възли, голямо бързодействие и постоянно променящи се връзки между камерите носи редица предимства пред сървърните архитектури, а алгоритмите за разпределени изчисления осигуряват реалистичен подход към създаване на големи децентрализирани системи от смарт камери.

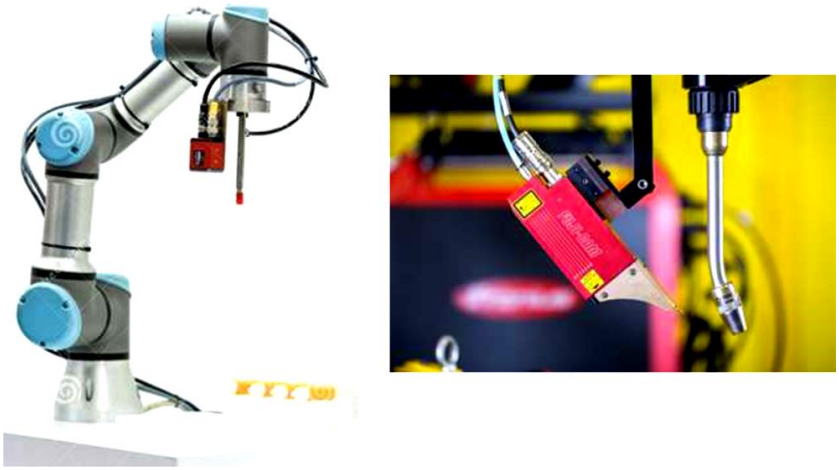
Миниатюризация

Вградените приложения на смарт камери и двигатели в последните години бележат сериозен ръст в роботиката, автомобилостроенето, производството на медицински изделия и лабораторната автоматика. Това основно се дължи на изключително малкия размер на смарт камерите, както и на факта, че те съдържат всички необходими елементи за осветяване, увеличаване, обработване и комуникиране в един завършен сензорен модул. Много ключови компании в сферата на медицинската образна диагностика предоставят решения, реализирани с вградена образна технология. Тези малки, ефективни и „умни“ камери обикновено се монтират неподвижно или към малки роботи във вътрешността на автоматичното оборудване (фиг. 2).

Това им помага да извършват действия като идентифициране на проби и реагенти, измерване на нивото на запълване, следене за наличие и отсъствие, качествени (напр. цветово) и количествени измервания на линейни и обемни величини, както и много други дейности с цел проследяване на правилното протичане на процесите.

Новата вълна от смарт камери е стимулирана от тенденцията за все по-широко използване на миниатюрни, нискоенергийни технологии, много от които са заимствани от потребителските видеоустройства. Инженерите пренасят ARM процесорите, CMOS

сензорите и други компоненти, типично използвани в устройства като смартфони, за да разработват още по-малки и „умни“ камери, удовлетворяващи все по-строгите изисквания за надеждност, гъвкавост и възпроизводимост, присъщи на машинното зрение. В резултат на това, новото поколение смарт камери се приема все по-мащабно в роботиката, наблюдението, самоуправляемите автомобили, здравеопазването, както и в традиционните приложения на машинно зрение като например автоматичното производство.



Фиг. 2. Вляво е индустриален робот на Microscan със смарт камера Vision HAWK, вдясно – лазерно насочвана смарт камера за заваряващи роботи на Fanuc

В електрониката и здравеопазването има особено силна нужда от използване на миниатюрни баркодове. Когато става въпрос за приложението на смарт камерите за разчитане на баркодове, тенденцията за миниатюризация в електрониката, както и изискванията на системите за присвояване на уникални идентификатори към медицинските изделия (напр. UDI), при производството им и в лабораторната автоматика, увеличават значението на способността за надеждно и съгласувано разчитане на такива малки кодове, които в някои случаи дори са невидими за човешкото око. Наблюдава се и тенденция за заемане на технологии от смарт камерите за машинно зрение и оползотворяването им в потребителските камери, най-вече в развлекателната индустрия. Компанията Google например представя през 2018 г. продукта си Clips – нова камера, която използва машинно обучение, за да прави автоматично снимки на хора, домашни любимци и други неща, които намери за интересни. Също така много смартфони вече използват разпознаване на лицето за отключване [1], [2].

Индустрия 4.0

С наименованието Индустрия 4.0 се означава съвременната тенденция за автоматизиране и обмен на данни в производствените технологии. Тя включва киберфизични системи, интернет на нещата, облачни и когнитивни изчисления. Често се нарича „четвъртата индустриална революция“. В условията на Индустрия 4.0 устройствата се свързват с други компоненти и системи, участващи в създаването на индустриална стойност, с вътрешните локални индустриални мрежи и с интернет. Смарт камерите се свързват чрез локални мрежи (най-често Ethernet) към автоматични устройства, които реагират на подаваната информация, което незабавно води до желаното действие без

никаква човешка намеса. От обикновен реактивен инструмент за откриване на дефекти днешните смарт камери се превръщат в извличащ инструмент, който използва техники от науката за данните и статистически методи в стила на големите данни (big data) за извличане на информация от изображения и прилагането ѝ в цялото предприятие.

Смарт камерите се вписват подходящо в концепцията за „умна фабрика“, тъй като предлагат резолюция от много мегапиксели и скорост, сравнима с тази на система с ПК, но без размерите, отделяната топлина и енергийната консумация, присъщи на масивните процесори и сензори. Освен това, тъй като свързаността е ключов фактор, определящ успешната програма в Индустрия 4.0, много смарт камери са изградени така, че да поддържат широко установени стандарти в машинното зрение, като Camera Link, GigE Vision, CoaXPress или USB 3.

С помощта на смарт камери и анализ на данни например ръководителят на завода може да определи кога даден елемент от оборудването ще се повреди, преди екипът по поддръжката да забележи, че има проблем. Системите улавят предупредителни признаци, използват данни за създаване на график за поддръжка и проактивно обслужват оборудването, преди проблемът да настъпи.

Друг пример е употребата на смарт камери за получаване на изображения на формовани детайли на всяка стъпка от производствения процес, започвайки от местоположението на доставчиците. Събраните изображения на детайлите може да бъдат сравнявани с хиляди други, съхранени в облак, за установяване на корелации и тенденции. Производителите на смарт камери се стремят да поддържат гама от промишлени мрежови стандарти, използвани в автоматиката, така че продуктите им да са способни да комуникират по всички индустриални протоколи и в рамките на стандартни дискретни входно-изходни интерфейси. В наши дни фабричните протоколи могат директно да се интегрират в някои камери, но други протоколи като Ethernet/IP и PROFINET може да изискват конвертори на трети страни.

Тенденции в софтуера

Не по-малко важна от архитектурата на смарт камерите е и лекотата на употребата им, както и възможността за програмиране с цел изпълнение на конкретни задачи с необходимата скорост. Освен че тези камери се предлагат в разнообразни конфигурации от типове на видео преобразуватели, процесори, входове, изходи и осветителни функции, производителите може да предоставят и продукти за реализиране на специфични задачи, като например прочитане на бар-кодове. По-старите смарт камери използват затворени софтуерни платформи, което означава, че на тях може да се разполагат само софтуерни продукти от същия производител. Този подход е в пряко противоречие с целите на модерната автоматика, която се стреми към персонализиране, гъвкавост и мащабируемост. Отварянето на платформата обаче предоставя възможност за максимално оползотворяване на производителността на камерата за машинно зрение при по-ниска цена [5], [8], [14].

Много системни интегратори търсят смарт камери, които имат възможности за изпълнение на разнообразни операции по обработка на изображения – например подобряване на изображението, локализиране на характеристики, измерване на обекти, откриване на наличие/отсъствие. В такъв случай програмистът е изправен пред няколко варианта. За удовлетворяване на подобни нужди много производители предлагат смарт камерите си със собствен софтуер и среда за разработка с графичен потребителски интерфейс. Макар употребата на такива камери да е ограничена само до фирмения софтуер, системният интегратор може да разчита на това, че производителят познава отблизо както

камерата, така и софтуера за анализ и разпознаване на образи, който тя използва. Някои производители – особено онези с традиции в разработването на софтуер за машинно зрение – осъзнават появата на смарт камери от трети страни, подобни на предлагания от тях продукт. Вместо да пренебрегват тази възможност, много традиционни доставчици вече позволяват внедряването на софтуера им в продукти от трети страни. Предлаганите образни средства от по-малко реномираните производители често имат по-ограничена поддръжка, но благодарение на това отворено взаимодействие опитните системни интегратори могат да използват готови софтуерни пакети и камери от трети страни за разработване на най-ефикасното и ефективно решение за задачите си по машинно зрение.

В наши дни много компании осъзнават, че основното прочитане или проверка на целостта на данни от баркодове например трябва да бъде допълнено със системи и софтуер за наблюдение в реално време. Системата Explorer RTM на Cognex може да интерпретира данни за изображения от четци на баркодове, за да осигури информация за работата им и по този начин – за състоянието на периферните устройства в индустриалната мрежа (фиг. 3).

Чрез внедряване на подобни мрежови системи ръководителите на заводи могат да установяват и класифицират всички грешки при четене и проверка, да визуализират данни за причините – например: неизправен принтер за баркодове и по този начин да увеличат дела на правилно прочетените кодове, да подобрят ефикасността на машините в продуктовата линия и да намалят загубите.

Фиг. 3. Explorer RTM на Cognex

Компаниите с дълга история в производството на софтуер за машинно зрение разработват опростени потребителски интерфейси, използващи алгоритми за обработка на изображения, които в миналото са предлагани само като функции за езика C. По този начин системните разработчици не е необходимо да извършват сложно софтуерно програмиране и получават свобода да се съсредоточат върху конкретната задача за инспекция.

Докато много патентовани смарт камери са насочени към дейности като четене на баркодове, програмируемите устройства позволяват осъществяване на разнообразни задачи от машинното зрение. Вместо да избират смарт камера от фирма, която произвежда както хардуера, така и софтуера, системните интегратори могат да избират камери на трети страни. Тъй като много от тях са базирани на процесори Intel или AMD, разработчиците могат да използват софтуера на производителите на смарт камери, както и такъв за компютърно базирани системи.

Редица производители на смарт камери поддържат също софтуерни пакети за машинно зрение от трети страни. Системите, използващи софтуерен интерфейс въз основа на поток от данни например, може да се програмират за различни задачи като калибриране на камерата, четене на баркодове, 1D и 2D измервания и съвпадение с еталон на клас.

Заключение

Стремежът към все по-голяма производителност и по-високо качество стимулира развитието на ново поколение усъвършенствани смарт камери за машинно зрение. Те комбинират високи резолюции и скорости, сравними със системите с ПК, без да наследяват недостатъците им, свързани с големи размери, топлоотделяне и енергийна консумация. Важна тенденция в развитието на промишлените смарт камерит е увеличаването на бързодействието им чрез поделяне на изчислителните задачи между няколко обработващи елемента – най-често централен процесор и програмируема логическа матрица.

Благодарение на вградените си микропроцесори и автономната си работа, смарт камерите са особено подходящи за включване в децентрализирани образни мрежи. Обработката на данни чрез разпределени алгоритми има сериозни предимства пред централизирания подход, тъй като не налага предаване на големите количества информация, получена при изпълнение на дейностите по машинно зрение [4], [6], [13].

Развитието в електрониката като цяло способства и за създаване на все по-малки смарт камери. Продължава успешното им внедряване в много промишлени отрасли, където пространството е ограничено от други машини или е необходимо вграждането им в по-малки устройства, като например мобилни и специализирани роботи.

„Умните“ фабрики, концептуализирани от четвъртата индустриална революция, налагат изисквания за свързаност, автономност и взаимодействие между всички устройства, участващи в технологичния процес. Смарт камерите за машинно зрение играят изключително важна роля в реализирането на тази постановка и способстват вземането на самостоятелни решения без участие на човека.

Системните разработчици, целящи внедряване на смарт камери в производствените си съоръжения, разполагат с няколко различни опции: избор на специализирани устройства с фиксирани функции, програмируеми камери от традиционно установени производители на хардуер и софтуер или камери с отворен код от по-малко реномирани производители. Тук може би по-съществено значение от съотношението цена-производителност имат функционалностите и нивата на софтуерна поддръжка, предлагани от всеки производител.

Много компании възприемат подхода за предоставяне на софтуерни инструменти за конфигуриране на произвежданите от тях камери, вкл. създаване на потребителски алгоритми, чрез лесен за използване интерфейс, което намалява нуждата от конвенционално програмиране. Макар че към настоящия момент съществуват различни мнения относно справянето с предизвикателствата, наложени от автоматиката, всички се обединяват около факта, че смарт камерите за машинно зрение играят решаваща роля в цялостното ѝ развитие и практическо осъществяване.

ЛИТЕРАТУРА:

[1] Арабаджиева-Калчева, Н., Николов, Н. Класифициране на мнения от потребителски коментари на английски език чрез алгоритми на машинното обучение. V-та научна конференция с международно участие "Компютърни науки и технологии", Списание Компютърни науки и технологии, ISSN 1312 -3335 (2018).

[2] Арабаджиева-Калчева, Н., Николов, Н. Сравнителен анализ между наивния бейсов класификатор и метода на опорните вектори използващ оптимизация при класификация на български текст в машинното обучение. Списание Компютърни науки и технологии, ISSN 1312-3335 (2017).

[3] Беджев, Б., Петров, П., Трифонов, Т. Кодове за логическо разделяне на абонатите в перспективните персонални комуникационни системи. Научна сесия на НВУ „В. Левски“ – Факултет „Авиационен“, Д. Митрополия (2003).

[4] Цонев, И., Василев, Д. Постигане високи показатели на предаване на данни в мобилните комуникации. Научна конференция с международно участие „MATTEX 2014“, Шумен (2014).

[5] Цонев, И., Станев, С. Компютърни мрежи и комуникации. Университетско издателство „Епископ К. Преславски“, Шумен, ISBN 978-954-577-496-6 (2008).

[6] Arabadzieva-Kalcheva, N. Comparative Analysis of Algorithms for Classification of Text in the Bulgarian Language in Machine Learning, International Conference “Applied Computer Technologies” ACT 2018 – Ohrid, Macedonia, ISBN 978-608-66225-0-3 (2018).

[7] 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, Bulgaria (2017).

[8] Kazakov, S., Trifonov, T., Tsonev, I. Probabilistic-temporal characteristics in a three level centralized computer structure. Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, Liepaya, Latvia (2014).

[9] Nikolov, L. Error rate analysis in ricean channel and complex radio environment. International scientific conference - Defence technology forum – Shumen, Collection of papers, Факултет, ISSN: 2367-7902 (2016).

[10] Nikolov, L. Network Infrastructure for Cybersecurity Analysis. Proceedings of International Scientific Conference “Defense Technologies”, Shumen, ISSN 2367-7902 (2018).

[11] Vasilev, D. Monitoring research in university area of the electromagnetic field in the frequency range 800 MHz – 2200 MHz. Proceedings of the 11-th Baltic – Bulgarian International Conference on BPBMMR, Riga (2016).

[12] Vasilev, D., Tsonev, I. Radio frequency requirements in acqisition, design and construction phases of sites. Journal Science Education Innovation, Vol. 5, ISSN 1314-9784 (2015).

[13] https://www.qualitymag.com/articles/94806-fast-evolving-smart-cameras-are-transforming-machine-vision

[14] https://www.vision-systems.com/articles/print/volume-22/issue-8/features/smart-cameras-challenge-host-based-systems-in-industrial-applications.html

Имена на авторите: инж. Даниел Росенов Денев
Докторант в кат. ККТ, ФТН на Шуменски университет „Епископ Константин Преславски“
E-mail: Slimshady33@abv.bg

доц. д-р инж. Цветослав Станиславов Цанков,
Месторабота: Шуменски университет „Епископ Константин Преславски“
E-mail: c.cankov@shu.bg

PREREQUISITES FOR TECHNOLOGY IMPLEMENTATION IN THE FIELD OF CYBERSECURITY

VALENTIN T. ATANASOV, ALEKSANDER P. MILEV

ABSTRACT: *This publication examines aspects related to the current issues in the field of cybersecurity and the questions raised about the need for implementation cybersecurity technologies in an human activity or the transformation of implemented technologies for this purpose. A formalized apparatus for studying the probability of an event in the domain of "cybersecurity" is presented and a paradigm of cybersecurity is synthesized, which logically constructs the concept of cybersecurity. The presented thesis could give an answer or at least guidelines for answering the main question - Is it necessary to implement such technologies in our business?.*

KEYWORDS: *Cybersecurity, cyber, cyberattack, business security, small business security, ICT security, cybercrime, cybertechnology.*

ПРЕДПОСТАВКИ ЗА ВНЕДРЯВАНЕ НА ТЕХНОЛОГИИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

ВАЛЕНТИН Т. АТАНАСОВ, АЛЕКСАНДЪР П. МИЛЕВ

АБСТРАКТ: *Настоящата публикация разглежда аспекти, свързани с актуалната проблематика в сферата на киберсигурността и поставяните въпроси за необходимостта от внедряване на технологии от областта на киберсигурността в дадена дейност или трансформация на внедрени технологии за тази цел. Представен е формализиран апарат за изследване на вероятност от събитие в домейна на „киберсигурността“ и е синтезирана парадигма на киберсигурността, която логически конструира концепцията за киберсигурност. Представената теза би могла да даде отговор или поне насоки за отговор на основния въпрос – Необходимо ли е внедряване на такива технологии в нашата дейност?*

1 Въведение

За да бъде изследван даден феномен, процес или обект е необходимо да бъде налична достатъчна информация за неговото функциониране, модел, зависимости и др. данни, пряко свързани с него. Описващата го дефиниционна област следва да бъде основана на недвусмисленост, доказуемост и достатъчност. Обектът на настоящото изследване е разглеждан в значителен интервал от време, но са налице данни, че именно дефиниционната му област не предполага добавянето на аксиоматична характеристика в нейния състав.

Поради известна неяснота на произхода на термина „киберсигурност“ и неговото имплементиране в области на човешката дейност, се установява, че към настоящата дата на това изследване продължават дискусионните процеси [1,2,3] в семантичен аспект. Като съществена констатация може да бъде приета, че в обхвата на киберсигурността са предимно държавни институции, национални правителствени институции, образователни институции и определени крупни субекти в частната област (банкови институции, развойни центрове и изследователски компании). Но когато се разглеждат в по-широк кръг, обхващащ бизнес организациите в среден и малък клас, се забелязва или незаинтересованост или липса на приоритизация в тази област [2,5,7,8, 10].

Основна цел на публикацията е представяне на някои ключови аспекти на киберсигурността, чието познаване от страна на слабо заинтересованите страни би довело

до стъпки към внедряване на определени технологии в областта на киберсигурността, или класифицирането на внедрени вече технологии, чиито основни характеристики, съвпадат с тези на технологиите в киберсигурността. Разглежданите аспекти са основавани на натрупан теоретичен обем, представящ формализиращ апарат и обуславящ решенията за необходимостта от разискваното по-горе внедряване [6].

2 Дефиниционна област и парадигма на киберсигурността

За определянето на дефиниционната област на киберсигурността се обобщават следните характеристики на домейна „киберсигурност“:

- *Доминантност* $\boldsymbol{D}$ – не може да бъде определена област на човешката дейност към която да не бъде съотнесена киберсигурността;
- *Висока технологизираност* $\boldsymbol{Q}$ – всяко технологично решение, произтичащо от IV-тата индустриална революция предполага събитие от домейна „киберсигурност“;
- *Дуалност* $\boldsymbol{V}$– операциите, реализиращи събития от домейна „киберсигурност“ имат човешки или машинен характер;
- *Времева независимост* $\boldsymbol{I}$ – операциите, реализиращи събития от домейна „киберсигурност“ имат стохастичен характер;
- *Неопределеност на изхода* $\boldsymbol{C}$ – последствията от реализираните операции имат стохастичен изходящ резултат.

В настоящото изследване се прави допускането, че киберсигурността $\boldsymbol{S}$ може да бъде обвързана с показател на производителността на човешката дейност. Приема се за отправна теоретична база законът на Амдал [4] за оценка производителността на компютърната система. И в този случай факторите, влияещи върху показателя за производителност на човешка дейност $\boldsymbol{A_i}$ са два:

1. Частта от времето за изпълнение на човешка дейност $\boldsymbol{A_i}$, която първоначално е без използване на ИКТ, и която може да бъде преобразувана, за да бъде отчетено подобрението при $\boldsymbol{A_i}$. Тази част се обозначава като $\boldsymbol{ThAction_{enchanced}}$ и винаги е по-малка или равна на 1.
2. Подобрението при $\boldsymbol{A_i}$, получено с използване на ИКТ в режим на изпълнение на $\boldsymbol{A_i}$, т.е. $\boldsymbol{speedUpThA_{enchanced}}$. Неговата стойност винаги е по-голяма от 1.

Времето за изпълнение на дейността $\boldsymbol{A_i}$ с възможности за използване на ИКТ ще бъде сумарна стойност на времето за изпълнение на частта без ИКТ режим и времето за изпълнение на частта с ИКТ режим . На основа на горното може да се приеме изразът:

$$\boldsymbol{\_humanActTime_{new}} = \boldsymbol{\_humanActTime_{old}} \cdot \left((\mathbf{1} - \boldsymbol{ThAct_{enchanced}}) + \frac{\boldsymbol{ThAct_{enchanced}}}{\boldsymbol{speedUpThA_{enchanced}}} \right) \quad (1)$$

където:

$\boldsymbol{\_humanActTime_{new}}$ – време за изпълнение на цялостната дейност $\boldsymbol{A_i}$ с използване на ИКТ режим.

$\boldsymbol{\_humanActTime_{old}}$ – време за изпълнение на цялостната дейност $\boldsymbol{A_i}$ без използване на ИКТ режим.

$\boldsymbol{ThAct_{enchanced}}$ – период на изпълнение на част от човешката дейност $\boldsymbol{A_i}$ с използване на ИКТ режим

$\boldsymbol{speedUpThA_{enchanced}}$ – ускорението при изпълнението на частта от човешката дейност $\boldsymbol{A_i}$ с използване на ИКТ режим.

Цялостното ускорение в този случай се определя от израза:

$$\boldsymbol{speedUpThA_{overall}} = \left(\frac{\boldsymbol{\_humanActTime_{old}}}{\boldsymbol{\_humanActTime_{new}}}\right) \tag{2}$$

или

$$\boldsymbol{speedUpThA_{overall}} = \frac{\mathbf{1}}{\left((\mathbf{1} - \boldsymbol{ThAct_{enchanced}}) + \frac{\boldsymbol{ThAct_{enchanced}}}{\boldsymbol{speedUpThA_{enchanced}}}\right)} \tag{3}$$

Ако се положи $\sigma = \left(\boldsymbol{speedUpThA_{overall}} - \mathbf{1}\right)$, то на основата на горното може да се приеме изразът:

$$\sigma \rightarrow \boldsymbol{P(cyberEvent)} \; \forall \; (\sigma_i : \sigma) \; > \mathbf{0} \tag{4}$$

Показаният израз формулира вероятността за възникване на събитие от домейна „киберсигурност“, функционална зависима от приложението на ИКТ режим на изпълнение в сферата на дейности на всеки субект в т.ч. и стопански субект (предприятие).

Освен формализацията на предпоставките за внедряване на технологии от областта на киберсигурността е необходимо да бъдат дефинирани по-ясно логическите структурни компоненти на киберсигурността. В настоящата статия се приема, че киберсигурността е процес а не състояние. Опирайки се на горното и на основата на дефиницията на „киберсигурност“ се приема установената в [2, 9] теоретична постановка, която формира следните ключови компоненти:

- *Инициатор* на събитието от домейна „киберсигурност“;
- *Цел* на събитието в домейна „киберсигурност“;
- *Признак* от домейна „киберсигурност“;
- *Предмет* на събитието от домейна „киберсигурност“;
- *Обект* на събитието от домейна „киберсигурност“;
- *Последствие* от събитието от домейна „киберсигурност“.

Инициаторът е активната съставка при генерирането на събитие от домейна на „киберсигурността“. Следва да бъде отбелязано, че няма имплицитно равенство между заинтересована страна и инициатор. Инициаторът стои на по-ниско йерархично ниво от заинтересованата страна.

Целта е мотивирано очертание на достижение при реализиране на определена последователност от действия.

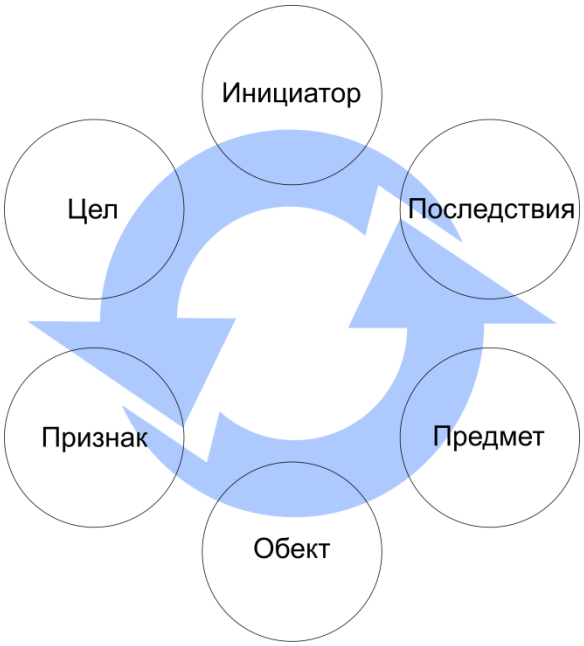
Признакът е единичен елемент от логически свързан и ограничен набор от признаци, пряко или непряко свързани с предоставената функционалност на системата по които може да бъде реализирано определено събитие от домейна на „киберсигурността“ .

Предметът на събитието е програмно базиран инструмент чрез който ще бъде осъществено генерирането на събитието от домейна на „киберсигурността“.

Обектът на събитието е специфициран от системата елемент или група елементи, който концентрира върху себе си предмета на събитието.

Последствието е състояние в което системата е установена след приключване на генерираното от инициатора събитие от домейна на „киберсигурността“.

Ако за дадена функционираща система е валиден изразът (4), то за да се обуслови събитие от домейна „киберсигурност“ следва да бъде изградена логическа конструкция в съответствие с парадигмата на киберсигурността дадена на фиг. 1.



Фиг.1. Парадигма на киберсигурността.

На базата на представения парадигматичен модел и подчиненост на израз(4) може да бъде изградена постановка за всяка човешка дейност, в релация с домейна на „киберсигурността“.

3 Заключение

Настоящата теоретична теза предоставя един по-ясен механизъм за изграждане на разбиране или концепция за отговор на основния въпрос – *Необходимо ли е внедряване на технология от областта на киберсигурността при дадена дейност*?

Отговорът на този въпрос е апроксимиран в определена дейност - производствена, административна, логистична, финансова или друга дейност, която е в обхвата на предложената парадигма на киберсигурността и формализирания израз (4). Въпреки, че отговорът има дихотомна характеристика, той все пак поставя фокуса върху сигурността при функционирането на дадена система.

ЛИТЕРАТУРА:

[1] Kulev, N., Analysis of definition set formed by given definitions of term cybersecurity, JDST vol.2, no.1, pp. 3-10, 2020, e-ISSN 2534-9813, https://doi.org/10.46713/jdst.002.01;

[2] Etzioni, A., International Engagement on Cyber IV: “The Private Sector: A Reluctant Partner in Cybersecurity.”, Georgetown Journal of International Affairs, 2014, pp. 69-78, ISSN 15260054, www.jstor.org/stable/43773650;

[3] Challenges to effective EU cybersecurity policy, Briefing Paper, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf;

[4] Hennessy, J., L., David A. Patterson, D., A., Computer Architecture A Quantitative Approach Sixth Edition, 2019,ISBN: 978-0-12-811905-1;

[5] Николов, Н.Р., Беджев, Б.Й., Цанков, Ц.С. Приложение на изкуствените имунни системи при синтеза на сигнали с оптимални автокорелационни свойства. Научна конференция MATTEX 2016, Шумен, ISSN 1314-3921 (2016).

[6] Трифонов, Т.С., Цанков, Ц.С., Николов, Н.Р., Велчев, С.П. Хардуерна реализация на съставен генератор на псевдослучайна последователност използващ неразложими полиноми в полета GF(2) и GF(5) и програмно управление на обратните връзки. Втора международна юбилейна научна конференция „50 години от полета на Юрий Гагарин“, Шумен, ISBN 978-954-8557-11-5 (2011).

[7] Iliev, M.P., Nikolov, N.R., Tsankov, Ts.S. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Journal "Electrotechnica & Electronica", Vol. 46, No 7-8/2011, ISSN 0861-4717.

[8] K. Ciglic, Cybersecurity Policy Framework: “A practical guide to the development of national cybersecurity policy”, https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-framework, (Посетен на 01.06.2020);

[9] Runia, Rinia, Private companies and cyber risk : A chat with Deloitte Private cyber leader Don MacPherson, https://www2.deloitte.com/ca/en/pages/deloitte-private/articles/private-companies-and-cyber-risk.html, (Посетен на 01.06.2020)

[10] Консултативен съвет по киберсигурност се създава към БСК, 2019, https://www.bia-bg.com/news/view/26156/, (Посетен на 01.06.2020)

Валентин Атанасов
Месторабота: Шуменски университет „Еп. Константин Преславски“
E-mail: v.atanasov@shu.bg
Александър Милев
Месторабота: Шуменски университет „Еп. Константин Преславски“
E-mail: al.milev@shu.bg

HISTORICAL OVERVIEW IN THE DEVELOPMENT OF RISK THEORY

DONIKA V. DIMANOVA

Abstract: *Although the word "risk" is spreading in Europe since the XIV century, people have known the phenomenon since ancient times and were aware of their dependence on the natural and social forces. Interaction with nature and other people, dealing with the many dangers and threats were the main source of uncertainty,which connects man as a social being with the collective way of life. You could say that risk is at the heart of the boldest political, military, technical and scientific projects. The development of a general theory of risk is impossible without assessing the past - how the different ideas originated and flowed, how they are historically related and logically and how they have proven themselves in practice.*

Keywords: *risk theory, historical risk development, institutionalization and philosophy of risk management, international standards*

ИСТОРИЧЕСКО РАЗВИТИЕ НА ТЕОРИЯТА НА РИСКА

ДОНИКА В. ДИМАНОВА

АБСТРАКТ: *Макар че думата „риск“ се разпространява в Европа след XIV век, още от древността хората са познавали явлението и са осъзнавали своята зависимост от природните и обществените сили. Взаимодействието с природата и останалите хора, справянето с многобройните опасности и заплахи са били основният източник на неопределеност, който свързва човека като социално същество с колективният начин на живот. Може да се каже, че рискът е в основата на най-дръзките политически, военни, технически и научни проекти. Изработването на обща теория на риска е невъзможна без да се оцени миналото – как са възникнали и протекли различните идеи, как са свързани исторически и логически и как са се доказали в практиката.*

Keywords: *теория на риска, историческо развитие на риска, институционализиране и философия на управлението на риска, международни стандарти.*

1 Въведение

Рискът е случайно явление, което динамично се развива с еволюцията на човека, технологиите, техниката, обществото и природата. Понятието „риск“ идва от арабското „risq“ – нещо, което е дадено на човека от Бог и от което той може да извлече печалба. Преминава през латинското „risicum“ - предизвикателство, което бариерните рифове поставят пред мореплавателите. В древен Китай думата има аналогично значение, като китайците за първи път разпределят риска помежду си. В гръцкия език „risikon“ се определя като случайно настъпване на някакъв резултат, а в английският език „risk“ има определено негативен смисъл – възможност за загуба, неблагоприятен резултат или изход, разрушаване. В италианския „risicare“ означава: дръзвам, решавам се, осмелявам се. Във френския език дума „risqué“ носи главно негативен смисъл, но не изключва напълно възможността за положителен резултат. В българския език понятието „риск“ навлиза от френски и има три значения: възможна опасност; възможна загуба от търговска сделка във валута или от кредитни операции; действие наслука, с надежда за успех.

В съвременното общество хората все по-често се сблъскват с нови несъществуващи доскоро явления. Като такива може да се определят [2]:

- задълбочаване на разрива между държавите, слоевете на обществото и отделните лица по отношение усвояването и използването на нови технологични решения;
- нарастващият синергизъм на въздействие на различни нововъведения върху личността, обществото и човечеството;
- усилващата се глобализация на икономиката и пазарните интереси, при които рисковете в една страна бързо стават трансгранична заплаха за много други страни.

Носител на риска може да бъдат природата, обществото, техниката, технологиите и човека [8]. Изработването на обща теория на риска е невъзможна без да се оцени миналото – как са възникнали и протекли различните идеи, как са свързани исторически и логически и как са се доказали в практиката [7].

В тази връзка целта на изложението е да разкрие същността на риска и причините за възникването му, като се направи исторически преглед в развитието на теорията на риска.

2 Изложение

Откритието на нови морски пътища, вносът на суровини и тъкани от Индия, потокът от злато и сребро от Америка предизвикват бурното развитие на търговията, финансите и банкерството. Подем преживяват селското стопанство и навигацията, развива се военното дело. Движеща сила за това развитие става застраховането – система, която изцяло зависи от способността да се изчислява вероятността.

Предвестник на концепцията за риска през средните векове е новото разбиране за лихварството, с което се въвеждат относителни критерии при оценка на справедливостта на лихвените проценти. По-сериозното изучаване на риска започва през XVI век, когато терминът „риск“ става обект на множество теоретични изследвания, свързани със статистическото разглеждане на рисковите калкулации в застраховането и хазарта. Според О. Рамстед [6] формалната рационалност на решенията вземани в застраховането и хазарта, която произлиза от способността за пресмятане на печалби, поставя началото на процеса на изграждане на понятието „риск“.

Резултатите от тези изследвания полагат основите на теорията на вероятностите, която става математическа основа на теория на риска. Те се свързват със забележителни открития и имена като Блез Паскал, Пиер Ферма, Якоб Бернули, Пиер Симон Лаплас, Томас Бейс и др.

Според някои изследователи [5] до началото на XVII век са открити по-голяма част от всички инструменти, които днес се използват при измерване и управление на риска, при анализа на решенията и избора на поведение в системите на теорията на игрите и теорията на хаоса.

На по-късен етап рискът започва да се изследва в икономическата дейност, а в техническите науки се прилага основно при определяне на надеждността на различни системи и устройства.

Като по-значимите могат да се отбележат следните открития и факти, на базата на които се основава теорията на риска [2]:

- Поставената задача през 1654 г. от Шевалие да Маре пред Блез Паскал и Пиер Ферма за разделянето на банката в хазартна игра между двама играчи.

През 1665 г. френският аристократ Шевалие да Маре, който е любител математик и запален играч на зарове, се обръща към младия Блез Паскал да реши следната задачата: Как да раздели банката между двама играчи на прекъснатата по средата игра на зарове, ако един от тях в момента печели? Паскал и неговият колега Пиер Ферма дават следния отговор:

Парите в банката следва да се разделят на основата на вероятността да спечели всеки играч. В този отговор за пръв път математически се обосновава теорията на вероятностите.

- Публикуваните данни за раждаемостта и смъртността в Лондон през 1662 г. от английския търговец Дж. Граунд, които са получени на база метода на статистическата извадка.
- Публикуването на „Регистъра Лойд“ (от Е. Лойд) за набиране на статистически данни за корабоплаването и морското застраховане.
- Изчисляване стойността на застрахователното обезщетение от английския математик и астроном Е. Хелий през 1696 г. Изчисленията се основават на данни за очакваната продължителност на живота и възрастта на застрахования.
- Продаването от британското правителство на права на пожизнена рента през 1725 г. на база очакваната продължителност на живот, която се изчислява чрез специално съставени таблици от математици.
- Публикувания труд през 1713 г. на швейцарския математик Якоб Бернули „Закон за големите числа“, който позволява при ограничен набор от данни да се изчисли вероятността и статистическата значимост.
- Тезата на швейцарския математик Даниел Бернули през 1738 г. за процеса за избор и вземане на решения, която е основа за изследване на риска в икономическата сфера и по-точно при управление на инвестициите.

Според Бернули „ползата от неголямото нарастване на богатството е обратно пропорционална на величината на вече наличното (първоначално) богатство“. Бернули обогатява теорията на вероятностите с формулираното понятие „полезност“. Той открива възможност при застраховането на търговските кораби да намали застрахователната премия за сметка на повече клиенти.

- Издаването на труда на Томас Бейс, озаглавен „Есе за решаване на проблемите в теорията на случайните събития“ през 1763 г.
- „Теорията на хазарта“ на Пиер Симон Лаплас през 1816 г.

Лаплас изследва риска не от гледна точка на математиката и теорията на вероятностите, а в съдържанието, взето от морското застраховане – съществен елемент на риска е надеждата, свързана с утрешния ден (очакването). В неговата теория се смята за рационално поддържането на равновесие между очакваните печалби и вероятните загуби. Той разглежда и въпроса, свързан с персоналната отговорност при възникване на неблагоприятни последици в резултат от вземането на рисково решение.

- Морското търговско застраховане в края на XVII и началото на XVIII век.
- Откритието през 1885 г. от Ф. Гълтън за явлението „регресия“.
- Издадената през 1921 г. книга на Франк Найт „Риск, неопределеност и печалба“;
- Завършената през 1944 г. книга „Теория на игрите и икономическо поведение“ на Джон фон Нойман и Оскар Моргенщайн.
- Теорията на портфейла на Хари Марковиц през 1952 г.
- Теорията на хаоса на американския метеоролог Едуард Лоренц от 1963 г. и фракталната геометрия като неразделна част от теорията на хаоса, формулирана от Беноа Манделброт през 1982 г.
- Математически модел на Ф. Блек и М. Шоулз за изчисляване на опция от 1970 г.
- Теорията на перспективата на Даниел Канеман и Еймъс Тверски през 1979 г.
- Хипотеза на У. Шарп през 1990г., според която изменението на богатството също влияе върху степента на неприемане на риска и като следствие от това увеличението на богатството води до усилване на апетитите към риска, а загубите го отслабват.

- Изследвания на генетичните алгоритми и невронните мрежи.

Интересът към темата за риска не спира до тук. Изследванията продължават и като резултат са установени редица модерни теории и приложни аспекти на математиката, кибернетиката, физиката, информатиката и информационните технологии.

В резултат на научно-техническата революция през 50-те години на XX век се появяват нови направления в науката, нови технологии и производства. С бързи темпове се развива строителството, машиностроенето, автомобилната промишленост, химическата промишленост, енергетиката, производството на битова техника и др. С това развитие възникват и нови рискове – икономически, финансови и технически, осигуряването на които ангажира вниманието на научната общност и се превръща в проблем с важно значение.

В големите западни компании се появяват нови длъжности: risk-adviser – консултант по нестандартни ситуации и risk-manager – служител, който разкрива, анализира и контролира риска. Целта на тези длъжности е да предотвратяват всякакви произшествия в сферата им на действие.

За първи път през 1955 г. професорът по застраховане Уейн Снайдър от Темплския университет (САЩ), предлага понятието „риск мениджмънт“, а една година по-късно Ръсел Галахар в „Харвард бизнес ревю“ дава описание на професията „риск мениджър“. През 1973 г. в САЩ за пръв път се дава професионална квалификация по риск мениджмънт.

Следва разширяване на концепцията за управление на риска със създаването на десетки неправителствени национални и международни организации като: Risk and Insurance Management Society (RIMS, 1950 г.) – Общество по управление на риска и застраховането, International Federation of Risk and Insurance Management Association (IFRIMA, 1984г.) – Международна федерация по управление на риска и застраховане, Global Association of Risk Professionals (GARP, 1996г.) – Глобална асоциация на риск професионалистите и др.

Популяризирането на управлението на риска във всички области от живота става толкова голямо, че се стига до важни законодателни промени в САЩ, които постепенно се разпространяват по целия свят. Като такъв пример може да се посочи приносът на Уилям Ръкенхаус, който налага управлението на риска в екологията, политиката и управлението на държавата.

През 1982 г. страните от Европейския съюз приемат известната Директива „Севезо“, насочена към предотвратяване на крупни промишлени катастрофи и аварии. Съгласно нея предприятията са задължени да изготвят оценка на рисковете, да предприемат мерки за предотвратяване на авариите и да осъществят план за управление на риска. На основа на принципите, залегнали в директивата, са разработени нов подход и конкретни препоръки, които са съобразени със законодателствата на много страни [3].

В края на 80-те години на XX век започва институционализирането на управлението на риска в нефинансовите корпорации, предимно в атомната енергетика, транспорта, разработването на нефтени находища и полети в космоса. В този период фокусът на вниманието е насочен към политическият риск.

В началото на 90-те години на XX век в световен мащаб избухват поредица от големи пожари на паметници на културата, които причиняват огромни загуби. Това са Историческият център (Шиадо) на Лисабон през 1988 г., Историческата библиотека на Националния технически университет в Атина през 1991 г., Редойтензале на двореца Хофбург във Виена през 1992 г. и кралският замък Уиндзор в Англия през 1992 г.

Резултатите от изследванията на тези обекти са показали ниската ефективност на системата за защита от пожари, регламентирани в държавното регулиране. Анализите са установили, че мероприятията за защита много често не са приложими от гледна точка нарушаване на целостта на стенописите, фреските и архитектурните детайли на сградите. Поради това правителството на Англия препоръчва за всяка историческа сграда да се прилага система за съхранението ѝ, включваща три основни положения:

- да бъде изготвена политика за сигурност;
- да бъде направена оценка на риска;
- да се въведат модерни и съвременни технологически системи за ранно диагностициране на аварийни ситуации, известяване и реагиране за недопускане и ограничаване на вредни последици.

Така в средата на 90-те години на XX век се формира промяна във философията на управлението на риска. Като отправна точка вече не се приема минимизиране на вредата, която ще понесе организацията в резултат на външна опасност, а се търсят такива управленски решения, които да не водят до неочаквани последици. Тези промени във философията предизвикват институционални промени. Управлението на риска започва да осъществява метеорологическото ръководство на отделите по човешки ресурси, безопасността на труда, охранителната дейност, пожарната безопасност, вътрешния одит, охраната на природната среда и др. [1].

Стига се до такова развитие на философията, че днешните риск мениджъри имат право на все по-малко грешки при вземането на решения.

В управлението на риска започва нов етап, след като процесният подход и риск мениджмънтът се налагат като базова платформа при разработването на серия международни стандарти (ISO) на системи за управление на околната среда, сигурността на информацията и изискванията към управлението на риска. Тези стандарти съдържат указания, принципи и правила по прилагане управлението на риска. През 2009 г. Международната организация по стандартизация (International Organization for Standardization) утвърждава пакет от документи, регламентиращи управлението на риска. Съществен е стандартът ISO 31000:2009, който е предназначен за унифициране на практиката по управление на риска. В негова подкрепа са приети стандартът ISO Guide 73 „Ръководство с термини и определения по управление на риска“ и стандарта ISO 31010:2009, съдържащ насоки за подбор и прилагане на техники за оценка на риска. Новият стандарт ISO 31000:2018 опростява управлението на риска като помага при управлението на несигурността.

Внедряването на управлението на риска се утвърждава като образец на добра практика в управлението на публичния и непубличния сектор. По този начин концепцията за риска се институционализира и се утвърждава с претенциите и перспективите да получи първостепенно място и значение в управлението на съвременната държава. Може да се каже, че няма европейски закон, в който да не е вложена концепцията на риска като задължителна правна норма. В България тази тенденция съвпада с периода на синхронизиране на законодателството ни с европейското, преди приемането на страната ни за член на ЕС [1].

Заключение

Изработването на обща теория на риска е невъзможна, без да се оцени миналото. По-сериозното изучаване на риска започва през XVI век, когато терминът „риск“ става обект на множество теоретични изследвания, свързани със статистическото разглеждане на

рисковите калкулации в застраховането и хазарта. Резултатите от тези изследвания полагат основите на теорията на вероятностите, която става математическа основа на теорията на риска. Рискът се определя като случайно явление, което динамично се развива с еволюцията на човека, технологиите, техниката, обществото и природата. В съвременното общество хората все по-често се сблъскват с нови несъществуващи доскоро явления, резултат на тази еволюция.

ЛИТЕРАТУРА:

[1] Георгиев, Ю. Управление на риска в сигурността. Изток – Запад, София (2012), с.18.

[2] Диманова, Д., Управление на риска. УИ Епископ Константин Преславски, Шумен (2016).

[3] Попчев, И. Рискът в новата парадигма// Мениджмънт и лидерство. София (2008).

[4] Христов, П. Метатеория на риска. Парадигма и подходи. София (2010).

[5] P. L. Bernstein. Again the Gods. The remarkable story of risk. John Wiley and Sons, Inc., N.Y. (1996).

[6] Rammstedt, O. Wieviel Unsicherheit vertragt der Mensch? Vorwarts 52, (1980).

[7] Solakov, T. Theoretical aspects of national security. International Scientific Refereed Online Journal With Impact Factor, Issue 68, April 2020, ISSN 2367-5721, www.sociobrains.com, pp.154-164.

[8] Христов, Х., Андреев, А., Управление на риска от кризи, породени от бедствия чрез използване на геоинформационни системи, International Scientific Conference “Defense Technologies”, Collection of Papers, 6-7 октомври 2016, ISSN 2367-7902, 2016, стр. 81-90.

Име на автора: Доника Величкова Диманова
Месторабота: ШУ „Епископ К. Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“
e-mail: d.dimanova@shu.bg

ORGANIZATION OF THE MANAGEMENT SYSTEM IN THE MINISTRY OF INTERIOR WHEN PARTICIPATING IN DISASTER PROTECTION MEASURES IN THE COUNTRY

LYUBOMIR K. DUCHEV

ABSTRACT: *Organization of the management system in the Ministry of Interior of the Republic of Bulgaria when participating in disaster protection operations in the country, based on the existing legal framework in Bulgaria.*

KEYWORDS: *Command, Management, Interaction, Ministry of Interior, Disaster*

ОРГАНИЗАЦИЯ НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ В МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ ПРИ УЧАСТИЕ В МЕРОПРИЯТИЯ ЗА ЗАЩИТА ПРИ БЕДСТВИЯ В СТРАНАТА

ЛЮБОМИР К. ДУЧЕВ

АБСТРАКТ: *Организация на системата за управление в Министерството на вътрешните работи на Република България при участие в мероприятия за защита при бедствия, съгласно правната уредба в страната*

Въведение

В зависимост от различните аспекти на обществения живот националната сигурност се разглежда като съвкупност от различни сфери за сигурност: политическа, икономическа, военна, социална, екологична и т.н., които по своята същност се явяват комплексно явление зависещо от различни фактори, свързани с националната сигурност пораждащи се от самата системност и интегралност на обществото. Тя е свързана с разглеждането на непрекъснато протичащи процеси на взаимодействия и конфликти в една многопластова функционална система, които засягат жизнено важните интереси на личността, обществото и държавата. В резултат се решават задачи, посочени Конституцията, законите, „Стратегията за национална сигурност“, свързани с функциониране на системата [19], в която политиката на държавата, свързана с бедствията и авариите е една от основните ѝ цели.

В съответствие с Конституцията на Република България държавната политика в областта на защитата при бедствия се формира и осъществява от Министерски съвет, който:

- осъществява общото ръководство на защитата при бедствия;
- приема Национална стратегия за намаляване на риска от бедствия;
- приема Национална програма за намаляване на риска от бедствия и годишни планове за защита от бедствия;
- приема Национален план за защита при бедствия;
- въвежда Национална система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия;
- планира финансови средства за защита при бедствия.

При сегашния управленски модел в страната има четири нива за защита при бедствия: Национално; Областно; Общинско; Обектово (за обекти от критичната инфраструктура).

Дейностите за защитата на населението при опасност или възникване на бедствия са:

предупреждение; изпълнение на неотложни мерки за намаляване на въздействието; оповестяване; спасителни операции; оказване на медицинска помощ при спешни състояния; оказване на първа психологична помощ на пострадалите и на спасителните екипи; овладяване и ликвидиране на екологични инциденти; защита срещу взривни вещества и боеприпаси; операции по издирване и спасяване; радиационна, химическа и биологична защита при инциденти и аварии с опасни вещества и материали и срещу ядрени, химически и биологични оръжия; ограничаване и ликвидиране на пожари; временно извеждане, евакуация, укриване и предоставяне на индивидуални средства за защита; извършване на неотложни аварийно-възстановителни работи; ограничаване на разпространението и ликвидиране на възникнали епидемични взривове, епидемии и епизоотии от заразни и паразитни болести; други операции, свързани със защитата. [1]

Основният нормативен акт, който урежда обществените отношения свързани с осигуряването на защитата на живота и здравето на населението, опазването на околната среда и имуществото при бедствия в Република България се явява Закона за защита при бедствия. В чл.2 на закона е дадена дефиниция на термина „бедствие“, която обуславя осъществяването на реални оперативни дейности по защита при бедствия. Със Закона за защита при бедствия е въведена Единна спасителна система (ЕСС) в Република България, в която се включват структури на министерства и ведомства, общини, търговски дружества и еднолични търговци, центрове за спешна медицинска помощ, други лечебни и здравни заведения, юридически лица с нестопанска цел, включително доброволни формирования и въоръжените сили.

Основни съставни части на ЕСС са Главна дирекция „Пожарна безопасност и защита на населението“ и областните дирекции на Министерството на вътрешните работи, както и центровете за спешна медицинска помощ. Тези организации имат водеща роля в дейността по защита при бедствия. Те са съставни части на ЕСС, като запазват институционалната или организационната си принадлежност и определените им функции или предмет на дейност. Координацията на съставните части на ЕСС се осъществява чрез оперативните центрове на Главна дирекция „Пожарна безопасност и защита на населението“ в Министерството на вътрешните работи (ГДПБЗН).

В изпълнение на Закона за защита при бедствия е изготвен национален план за защита при бедствия в Република България. Основната цел на плана е извършване на анализи и оценки за риска от възникване на бедствия на територията на страната и набелязване на превантивни мерки за намаляване на неблагоприятните последици в резултат от бедствията, организиране и координиране на действията за предотвратяване или намаляване на последиците от бедствия. Основните задачи на плана са: анализиране на възможните бедствия и прогнозиране на последиците от тях; планиране на мерки за предотвратяване или намаляване на последиците от бедствията; разпределение на задълженията и отговорностите между органите на изпълнителната власт за изпълнение на планираните мерки; осигуряване на средствата и ресурсите, предвидени за ликвидиране на последиците от бедствия; определяне на начина на взаимодействие между органите на изпълнителната власт; определяне на реда за навременното уведомяване на органите на изпълнителната власт и населението при заплаха или възникване на бедствие. [12]

За изпълнение на националния план за защита при бедствия със заповед на министър-председателя на Република България се създава национален щаб с поименно определени ръководител и членове: министри, заместник-министри, ръководители на ведомства или техни заместници и други, представляващи институции, които имат задължения за изпълнението на Националния план за защита при бедствия. Дейността на Националния щаб се осигурява логистично, комуникационно и административно от ГДПБЗН, както и от

компетентните с оглед характера на бедствието министерства, ведомства и институции.

Взаимодействието и координацията между частите на ЕСС, участващи в изпълнението на дейности в района на бедствието, се извършва от ръководител на операциите, който се определя със заповед на министър-председателя на Република България, на съответния областен управител или кмет на община в зависимост от обхвата на бедствието. Ръководителят на операциите организира и контролира изпълнението на одобрените решения на щабовете за изпълнение на плановете за защита при бедствия.

Изложение

Съгласно националния план за защита при бедствия министърът на вътрешните работи [12]:

- провежда държавната политика по защита при бедствия;
- осъществява взаимодействието между органите на изпълнителната власт, юридическите лица и неправителствени организации при бедствия;
- организира събирането, анализирането, оценката на информацията и прогнозира рисковете от бедствия;
- организира разработването на Националния план за защита при бедствия;
- поддържа в готовност сили и средства и осигурява участието на подчинените си структури, като съставна част на единната спасителна система;
- организира и контролира извършването на превантивни дейности за недопускане или ограничаване въздействието на рисковите фактори, предизвикващи бедствия;
- организира функционирането и експлоатацията на Националната система за ранно предупреждение и оповестяване при бедствия;
- организира провеждането на спасителни и неотложни аварийно-възстановителни дейности при бедствия;
- осигурява опазването на обществения ред, пожарната безопасност и извършване на пожарогасителна и аварийно - спасителна дейности при бедствия;
- оказва съдействие на областната и общинска администрация по организацията на движението, безопасността на населението при евакуация, издирване на пострадали и идентификация на починали граждани;
- подпомага дейността на правителствени и неправителствени организации при дейността им по оказване хуманитарна помощ на населението;
- организира обучението на населението за начините на поведение и действие при бедствия и прилагане на необходимите защитни мерки;
- организира информирането на населението чрез средствата за масово осведомяване за възникнали бедствия, предприетите мерки за овладяване на обстановката и за правилата за действие и поведение;
- осигурява и актуализира информацията за екипите и средствата на министерството като част от ЕСС, техните задачи и възможности за провеждане на спасителни и неотложни аварийно-възстановителни дейности.

При осъществяване на своите правомощия министърът на вътрешните работи се подпомага от заместник-министри и главен секретар на министерството на вътрешните работи (МВР), както и административен секретар на МВР. При отсъствие министърът на вътрешните работи се замества от определен от него заместник-министър. За изпълнение на функциите си министърът на вътрешните работи се подпомага от политически кабинет, който се създава и функционира съгласно Закона за администрацията.

Основните структури в Министерството на вътрешните работи са: главни дирекции; областни дирекции; дирекции; специализиран отряд за борба с тероризма; дирекция

„Вътрешна сигурност“; дирекция „Миграция“; дирекция „Международно оперативно сътрудничество“; дирекциите от общата и специализираната администрация; Академия на МВР; Медицински институт на МВР; научноизследователски и научно-приложни институти. [5]

Главните дирекции на МВР се ръководят от директори, които осъществяват общото и непосредственото ръководство, като ръководят, планират, организират и отговарят за дейността на главните дирекции. Директорите изпълняват заповедите на министъра на вътрешните работи, заместник-министрите и на главния секретар на МВР и се отчитат пред тях.

Областните дирекции на МВР се ръководят от директори, които осъществяват общото и непосредственото ръководство, като ръководят, планират, организират и отговарят за дейността им. Директорите организират изпълнението на заповедите, поставени от горестоящите им органи, като се отчитат за цялостната си дейност пред министъра на вътрешните работи, заместник-министрите и главния секретар на МВР, както и пред директора на Главна дирекция „Национална полиция“ в МВР по направление на дейност.

Съществено значение за регулиране на обществените отношения, свързани със защитата при бедствия, след Закона за защита при бедствия, има Закона за министерството на вътрешните работи. Съгласно Закона за министерството на вътрешните работи, една от основните дейности на МВР е осигуряване на пожарна безопасност и защитата при пожари, бедствия и извънредни ситуации. Тази дейност се осъществява от органите по пожарна безопасност и защита на населението в ГДПБЗН при условия и по ред определени в Закона за министерството на вътрешните работи и на Закона за защита при бедствия чрез:

- превантивна дейност;
- 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 контролна дейност на продукти за пожарогасене;
- неотложни аварийно-възстановителни работи, оперативна защита при наводнения и операции по издирване и спасяване, и химическа, биологическа и радиационна защита;
- ранно предупреждение и оповестяване при бедствия и при въздушна опасност на органите на изпълнителната власт и населението;
- изследване на причините и условията за възникване и разпространение на пожари и извършването на експертизи и експертни справки;
- подпомагане на дейностите по анализ, оценка и картографиране на рисковете от бедствия;
- подпомагане на координацията на дейностите по установяване на критичните инфраструктури и обектите им и оценката на риска за тях;
- методическа и експертна помощ на териториалните органи на изпълнителната власт по отношение на защитата при бедствия и при организиране дейността на доброволните формирования, като води регистър на тези формирования;
- осъществяване координацията на съставните части на ЕСС, чрез оперативните си центрове;
- определяне на пожарните характеристики на продукти и техническите и експлоатационните показатели на пожаротехническо оборудване и продукти за пожарогасене;
- професионално обучение на органи за пожарна безопасност и защита на

населението, спасители и доброволци за осъществяване на пожарогасителна и спасителна дейност и неотложни аварийно-възстановителни работи;

- оперативно сътрудничество със структурите на Европейския съюз, Организацията на Северноатлантическия договор (НАТО) и други международни организации в областта на пожарната безопасност и защитата на населението, хуманитарната помощ и гражданско-военното аварийно планиране.

Обхватът и съдържанието на отделните дейности са определени с правилник за устройството и дейността на министерството на вътрешните работи, Наредба за осъществяване на превантивна дейност от органите за пожарна безопасност и защита на населението на министерството на вътрешните работи, Наредба за реда за осъществяване на държавен противопожарен контрол и Наредба за реда за осъществяване на пожарогасителната и спасителната дейност от органите за пожарна безопасност и защита на населението на министерството на вътрешните работи. [7, 8, 9, 16]

Основните структури на ГДПБЗН са дирекция „Оперативни дейности“, дирекция „Държавен контрол и превантивна дейност“ и регионални дирекции „Пожарна безопасност и защита на населението“ (РДПБЗН) във всички областни центрове в страната, които се ръководят от директора на главната дирекция, като не се включват в структурата на областните дирекции на министерството на вътрешните работи.

В ГДПБЗН се създават дирекции, отдели, сектори и други звена от по-нисък ранг в зависимост от функциите и дейността, а в РДПБЗН има сектори, групи и участъци „Пожарна безопасност и защита на населението“. Районите на действие на РДПБЗН се определят със заповед на министъра на вътрешните работи по предложение на директора на ГДПБЗН.

Органи за пожарна безопасност и защита на населението са служителите на ГДПБЗН, които пряко осъществяват дейностите по осигуряване на пожарна безопасност и защита при пожари, бедствия и извънредни ситуации, контролна и превантивна дейност, както и тези в обекти по сключени договори между МВР и заинтересовани лица за осъществяване на пожарогасителна и спасителна дейност и държавен противопожарен контрол. Органите за пожарна безопасност и защита на населението осъществяват дейността си в екипи от минимум трима служители, като се допуска в населени места с население до 5000 души да се осъществява в екипи от двама служители.

Дирекция „Оперативни дейности“ осъществява методическо ръководство, помощ и контрол на РДПБЗН, по направление на пожарогасителна и спасителна дейност, неотложни аварийно-възстановителни работи, оперативна защита при наводнения и операции по издирване и спасяване и химическа, биологическа и радиационна защита, ранно предупреждение и оповестяване при бедствия и при въздушна опасност на органите на изпълнителната власт и населението, както и за дейностите по осъществяване на координацията на съставните части на ЕСС чрез оперативните центрове и водене на регистър на доброволните формирования. [16] Регистърът се води съгласно 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, издадена от министъра на вътрешните работи. [10]

Дирекция „Държавен контрол и превантивна дейност“ осъществява методическо ръководство, помощ и контрол на регионалните дирекции „Пожарна безопасност и защита на населението“, по направление на превантивната дейност. [16]

Превантивната дейност на ГДПБЗН включва:

- информиране на обществеността относно опасностите и риска от пожари, бедствия и извънредни ситуации;

● подпомагане на обучението и практическата подготовка на централните и териториалните органи на изпълнителната власт, силите за реагиране и населението;

● подпомагане на обучението по защита при бедствия в системата на предучилищното и училищното образование и в системата на висшето образование;

● подпомагане на съвета за намаляване на риска от бедствия към Министерския съвет, областните съвети за намаляване на риска от бедствия и общинските съвети за намаляване на риска от бедствия;

● подпомагане планирането на защитата при бедствия.

За осъществяване на пожарогасителната и спасителната дейност се поддържа постоянна готовност на личния състав, пожарната и спасителната техника за незабавно изпращане на сили и средства при съобщение за пожар, бедствия и извънредни ситуации за ограничаване и ликвидиране на пожара, спасяване или евакуация на хора и оказване на долекарска помощ на пострадалите и транспортирането им до лечебните заведения.

Органите за пожарна безопасност и защита на населението могат да извършват пожарогасителни и спасителни дейности и неотложни аварийно-възстановителни работи в служебни и жилищни помещения и превозни средства на чуждестранните представителства и на физическите лица, които се ползват с имунитет, по постъпило тяхно искане. Когато непосредствено са застрашени други сгради и съоръжения, със съгласието на ръководителя на чуждестранното представителство или на чуждестранното физическо лице, ползващо се с имунитет, органите за пожарна безопасност и защита на населението извършват пожарогасителни и спасителни дейности и неотложни аварийно-възстановителни работи и в техните служебни и жилищни помещения.

Организацията за осъществяване на аварийно-възстановителните дейности е определена с Инструкция на министъра на вътрешните работи за условията и реда за осъществяване на аварийно-възстановителни дейности. [6] Неотложните аварийно-възстановителни работи и оперативната защита при наводнения включват дейности за ограничаване на въздействието и подпомагане възстановяването на обекти на техническата инфраструктура при бедствия и извънредни ситуации.

Операциите по издирване и спасяване включват разузнаване, оказване на помощ и евакуация на хора, изложени на опасност, при разрушаване на строежи или на части от тях, движения на маси (срутища, свлачища, кално-каменни порои, изкопни работи и др.) и при инциденти в повърхностни води с изключение на дейностите по защита при бедствия в морските пространства на Република България.

Химическата, биологическата и радиационната защита включват дейности за подпомагане ограничаването на последствията при бедствия и инциденти с опасни химични вещества и смеси, опасни биологични агенти или радиоактивни вещества и материали.

Ранното предупреждение и оповестяването при бедствия и при въздушна опасност на органите на изпълнителната власт и на населението осъществявани от ГДПБЗН обхващат:

● предоставяне на информация за приближаваща или непосредствена заплаха от възникване на бедствие или въздушна опасност на органите на изпълнителната власт и силите за реагиране на ЕСС, с цел повишаване на готовността им за реагиране и предприемане на необходимите мерки;

● оповестяване с акустични сигнали и гласова информация на големи групи хора на определена територия за предстоящо или настъпило бедствие или въздушна опасност и излъчване на указания за необходимите предпазни мерки и действия.

● При изпълнение на дейността си органите за пожарна безопасност и защита на населението от ГДПБЗН имат право:

● да влизат в жилищни, производствени и други сгради и помещения на физически и

юридически лица;

- да разрушават сгради или части от тях, да разглобяват конструкции, да отстраняват, унищожават или повреждат имущество или насаждения, когато няма друг начин за извършването на дейността;
- да използват спасителни, пожарогасителни, транспортни, съобщителни и други технически средства - собственост на физически или юридически лица;
- да привличат длъжностни лица, участници в доброволни формирования и граждани за оказване на съдействие;
- да изменят реда за движение и да ограничават достъпа на външни лица в района, където се извършват дейностите, до пристигането на съответните компетентни органи;
- да използват безвъзмездно водоизточници и водопроводни мрежи за осигуряване на необходимите количества вода при бедствия, за гасене на пожари и при извънредни ситуации;
- да извършват евакуация на хора и движимо имущество в района, където се извършват дейностите.

Дейностите на органите за пожарна безопасност и защита на населението се организират и осъществяват самостоятелно или съвместно със специализираните сили и средства на органите на изпълнителната власт, организациите, юридическите лица и гражданите [17]. Координацията и ръководството на действията при извършване на съвместни дейности се осъществяват от органите по пожарна безопасност и защита на населението от ГДПБЗН/РДПБЗН.

Координацията на съставните части на ЕСС се осъществява чрез оперативни комуникационно-информационни центрове [2] в ГДПБЗН, които:

- приемат и оценяват информация за възникнали бедствия;
- уведомяват компетентните съставни части на ЕСС и координират по-нататъшната дейност на основата на стандартни оперативни процедури, разработени от главния секретар на МВР;
- извършват ранно предупреждение и оповестяване на органите на изпълнителната власт, съставните части на ЕСС и населението при бедствия;
- по искане на ръководителя на операциите организират включване на предвидените в плановете за защита при бедствия съставни части на ЕСС, както и на допълнителни сили и средства.

При бедствия, пожари и извънредни ситуации органите на държавната власт, на местното самоуправление, юридическите лица и гражданите са длъжни при поискване да предоставят на органите за пожарна безопасност и защита на населението собствени спасителни, пожарогасителни, превозни, съобщителни и други технически средства. При използването на такива средства, на собствениците се заплаща обезщетение съгласно Правилник за организацията и дейността на междуведомствената комисия за възстановяване и подпомагане към министерския съвет във връзка с чл. 54, ал. 6 от Закона за защита при бедствия. [15]

Органите за пожарна безопасност и защита на населението от ГДПБЗН/РДПБЗН оказват методическа и експертна помощ на териториалните органи на изпълнителната власт по отношение на защитата при бедствия, включваща подпомагане на щабовете за защита при бедствия при изпълнение на функциите им и разработването на програми и проекти за намаляване на риска от бедствия.

Заключение

Анализът на нормативната уредба в Република България показва, че в страната има сравнително добра правна уредба на обществените отношения, свързани със защитата при бедствия. Законът за защита при бедствия създава организационна архитектура за реагиране при бедствия с водеща роля на Главна дирекция „Пожарна безопасност и защита на населението“ в Министерството на вътрешните работи.

В Закона за министерството на вътрешните работи и подзаконовите му актове ясно са дефинирани функциите, задачите и правомощията на органите от Главна дирекция „Пожарна безопасност и защита на населението“, като изрично е прогласена ръководната и координационна роля на органите за пожарна безопасност и защита на населението при бедствия. Регламентирана е и контролната дейност на органите за пожарна безопасност и защита на населението, включително да извършват проверки за спазване на изискванията за защита при бедствия с цел готовност за използване на всички способи и средства за защита на населението и националното стопанство и провеждане на предварителни мероприятия за недопускане и намаляване на вредното въздействие и предотвратяване на възможните последствия за населението при възникване на бедствия.

ЛИТЕРАТУРА:

[1] Диманова, Д. Защита при бедствия, аварии и катастрофи. УИ на ШУ „Епископ Константин Преславски“. Шумен. 2016. ISBN 978-619-201-098-0.

[2] Диманова Д, Кузманов З, Национална система за спешни повиквания. НК МАТТЕХ 2016. ШУ „Епископ Константин Преславски“ 11-13 ноември 2016, Шумен, ISSN: 1314-3921. pp. 77-83.

[3] Закон за администрацията, Обн., ДВ, бр. 130 от 5.11.1998 г., в сила от 6.12.1998 г.; посл. изм. и доп., бр. 7 от 19.01.2018 г.

[4] Закон за защита при бедствия, Обн., ДВ, бр. 102 от 19.12.2006 г., посл. изм. и доп., бр. 77 от 18.09.2018г., в сила от 1.01.2019 г.

[5] Закон за министерството на вътрешните работи, Обн., ДВ, бр. 53 от 27.06.2014 г., посл. изм. и доп., бр. 34 от 23.04.2019 г.

[6] Инструкция на министъра на вътрешните работи № 8121з-914 от 1 декември 2014 г. за условията и реда за осъществяване на неотложни аварийно-възстановителни работи, Обн. ДВ. бр.101 от 9 Декември 2014г. в сила от 09.12.2014 г.

[7] Наредба № 8121з-1006 от 24 август 2015 г. за реда за осъществяване на пожарогасителната и спасителната дейност от органите за пожарна безопасност и защита на населението на министерството на вътрешните работи, Обн. ДВ. бр.67 от 1 Септември 2015г., в сила от 01.09.2015 г.

[8] Наредба № 8121з-758 от 22 октомври 2014 г. за осъществяване на превантивна дейност от органите за пожарна безопасност и защита на населението на министерството на вътрешните работи, Обн. ДВ, бр. 90/30.10.2014 г.

[9] Наредба № 8121з-882 от 25 ноември 2014 г. за реда за осъществяване на държавен противопожарен контрол от органите за пожарна безопасност и защита на населението на министерството на вътрешните работи, Обн. ДВ. бр. 100 от 5 Декември 2014 г., посл. изм. и доп., бр. 78 от 4 Септември 2020 г.

[10] 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, издадена от министъра на вътрешните работи, Обн., ДВ, бр. 50 от 3.07.2012 г., посл. изм. и доп., бр. 94 от 24.11.2017 г., в сила от 24.11.2017 г.

[11] Наредба за условията и реда за функциониране на Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване за въздушна опасност, обн., ДВ, бр. 20 от 9.03.2012 г., посл. изм. и доп., бр.61 от 2 август 2019г.

[12] Национален план за защита от бедствия, РМС № 973 от 29 декември 2010 г.

[13] Национална програма за защита при бедствия 2014 - 2018 г.

[14] Национална стратегия за намаляване на риска от бедствия 2018-2030г., РМС № 505 от 19 юли 2018г.

[15] Правилник за организацията и дейността на междуведомствената комисия за възстановяване и подпомагане към министерския съвет, обн. ДВ. бр.28 от 13 април 2010г., изм. и доп., бр.37 от 7 май 2019г.

[16] Правилник за устройството и дейността на министерството на вътрешните работи, Обн., ДВ. бр.60 от 22 Юли 2014г., посл. изм. и доп., бр.48 от 26 Май 2020г.

[17] Христов, Х., Андреев, А., Аспекти на системата за сигурност при бедствие – наводнения, International Scientific Conference „Defense Technologies“, Collection of Papers, 6-7 октомври 2016, ISSN 2367-7902, 2016

[18] Hristov, H., Military counterintelligence in the intelligence community of England, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 53, January 2019, Bulgaria, 2019, pp. 108-116.

[19] Solakov T., „Theoretical aspects of national security“, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas – Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 68, April 2020, pp. 154-164

Любомир Кирилов Дучев,
Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
E-mail: l_duchev_2012@abv.bg

A LOOK AT THE MANAGEMENT OF SECURITY SERVICES IN THE REPUBLIC OF BULGARIA

ILIN A. SAVOV

ABSTRACT: *The report assesses management as multispectral phenomenon that can be seen from different sides. The management can be examined like a multiphase. In management stand such phases as: leadership, planning, organization, control and regulation.*

KEYWORDS: *management, security services, State Agency "Technical operations", State Agency "National Security", Law of Special Intelligence Means.*

ЕДИН ПОГЛЕД ВЪРХУ УПРАВЛЕНИЕТО НА СЛУЖБИТЕ ЗА СИГУРНОСТ В РЕПУБЛИКА БЪЛГАРИЯ

ИЛИН А. САВОВ

АБСТРАКТ: *Докладът оценява управлението като многоспектрален феномен, който може да се погледне от различни страни. Управлението може да се разглежда като многофазно. В управлението стоят такива фази като: лидерство, планиране, организация, контрол и регулиране.*

Въведение

Още от древността сигурността като родово понятие се разбира като невъзможност да се нанесе вреда, като защита на всеки човек и обкръжаващата го среда от извънредна опасност. Някои автори я определят като комплексно понятие, съдържащо "отсъствие на опасност", увереност на индивида, обществото и държавата, че са защитени от възможни опасности. Други автори я свързват с общност на политически цели, стратегии и методи, които служат за предотвратяването на война при запазване способността за политическо самоопределение.

Прието е да се счита, че мисията на службите за сигурност е свързана с постигането на основната цел, отнасяща се до осигуряване и гарантиране на надеждна защита на националната сигурност, интересите, правата и свободите на гражданите и демократичното функциониране на държавните институции с оглед осигуряване на устойчиво икономическо развитие и просперитет на страната.

Ето защо в подкрепа на успешната й реализация обществените очаквания са свързани с извършване на така необходимата реформа в сектора на управлението на службите за сигурност на Република България с оглед оптимизирането им, за даване на адекватен отговор и отпор на предизвикателствата, касаещи пряко или латентно засягането на сигурността на отделни области от обществения живот чрез замисляни, подготвяни или провеждани посегателства и престъпления.

В настоящият доклад сме направили преглед на състоянието на управлението на службите за сигурност в Република България, както и необходимостта от реформиране и оценка върху бъдещите заплахи и опасности в средата за сигурност.

Изложение

Управлението на службите за сигурност в днешно време се разглежда като целенасочена интелектуална дейност между битието на субективните фактори /съвкупността от службите за сигурност/ и обективните обстоятелства /чужди специални служби, организирани престъпни групи или високо подготвени престъпници и тяхната дейност в средата за сигурност/. В тази връзка посегателствата и престъпните прояви, създаващи реална заплаха от увреждащо въздействие за сигурността на държавата могат да се избегнат или посрещнат организирано в зависимост от нивото на познание за тях. След това идва умението да се формират подходящи управленски механизми за реакция със силите и ресурсите на организацията на специализираните структури и на осъществяването на техните мерки и инициативи.

От подготвеността и достигането до високи нива на организационна и управленска култура, зависи и какви ще са равнищата на професионална и интелектуална компетентност на ръководителите и изпълнителите в службите за сигурност, за да може качествено да се отговори на въпроса: „Как да се извършва начертаното и планираното желано бъдещо състояние?”

Ежедневното изпълнение на сложните и трудоемки функции и дейности от специално оправомощените от държавата служби за сигурност и опазване на обществения ред за гарантиране на надеждната защита на националната сигурност и обществената безопасност и спокойствието на гражданите протича при трудни и постоянно изменящи се условия. Те са свързани с динамичността на развиващите се събития и явления, имащи пряко или косвено отношение с посегателски прояви или престъпни действия, създаващи заплаха за националната сигурност. Също така в работата на специализираните държавни органи за защита на националната сигурност и обществения ред в страната се забелязва типичната и присъща характерна особеност, свързана с недостига на качествена и навременна информация за случващото се или случилото се престъпление. Следва да се отбележи и при повечето от случаите се разполага и с недостатъчното количество време /бюджет за оперативно реагиране/ сили, средства и ресурси. За обхващането, предотвратяването, превенцията, и пресичането на посегателства, като и за разкриването на авторите на престъпления, засягащи националната сигурност и други правонарушения се изискват и законосъобразни реакции, адекватни решения от съответните оправомощени ръководни органи. Ето очакванията на народа за превенция и противодействие на престъпността и другите тайни посегателства, изискванията, които поставя обществото и партньорските държави от ЕС пред службите за сигурност в съвременните условия са оправдани в значителна степен.

Според науката за управление управлението се разкрива като многоспектърно явление, което може да бъде разглеждано от различни страни. Управлението може да се изследва като многофазен процес, в който се различават отделно обособени етапи. В управлението разглеждано като процес се открояват такива фази последователно през които се преминава като: ръководене, планиране, организиране, контрол и регулиране. Управлението в същото време се разглежда като последователност от изпълнени решения. Поради тази причина редица автори определят изработването на решения като най-важната управленска функция.

Много от авторите определят функциите на управлението като дейност, разбират управлението като специфичен вид работи, осигуряващи постигането на някаква цел независимо от това каква е тя. По-конкретно те влагат в съдържанието на този термин разбирането, че функцията е дейност, която в своята съвкупност обхваща обективно необходими, устойчиво повтарящи се отделни действия, обединени с оглед крайните цели.

По такъв начин функциите на управление се отъждествяват със стадиите на управленския цикъл. /НОРД, анализ и оценка, вземане на управленско решение, изпълнение на управленско решение-планиране, координация и взаимодействие, контрол/. От друга страна, функциите, възприемани като основни задачи /задължения/ се използват за определяне на даден отрасъл или вид работи, представляващи съвкупност от решения, действия или процеси, обединени от общността на обекта и решаваните задачи от субекта на управлението.

Управлението се разглежда като понятие, което е характерно и присъщо само и единствено на системата, системността и съдържанието на системния подход в теорията на системите. То се съдържа иманентно в конфигурирането на структурата й, в нейната организация и функциониране. Ето защо поставено извън системата управлението е мъртво и няма никакви живителни сили и потенциал. С пълна сила тази теза е валидна и се отнася и за значението и особеностите на управлението на социалните системи в това число и за управленската дейност в системата на службите за сигурност.

От гледна точка на разделението на труда - вертикално и хоризонтално, управлението може да се разглежда като процес, който има свой стадий или степен на осъществяване, в този смисъл функциите биха съвпаднали с етапите. Ръководителят като субект на управление, от една страна подготвя и взема решение, а от друга организира чрез своя апарат изпълнението на взетите решения. Така изглеждат функциите на управление от позициите на ръководителя, на субекта на управлението, т.е. съществува очевидното съвпадение между задачите и действията. Но от позициите на обекта на управлението нещата са по-сложни, защото изпълнението на задачите, на решението, най-често придобива характера на предварително разпределени задачи между изпълнителите. В крайна сметка достигнахме до правилния извод, че:

За управляващият субект решението представлява резултат от дейност или самата дейност /решаването/, т.е. негова функция, но същото това решение за управлявания обект е задача за изпълнение, т.е. функция-задача.

Следователно могат да бъдат различени функциите на системата за управление, на управляващата я подсистема, както и различно биха изглеждали функциите на управление една спрямо друга в отделна система и подсистема.

Най-общо в системата за управление в службите за сигурност като цяло има две групи функции-ръководни и изпълнителски. Такива функции има във всяка подсистема, разглеждана като относително цяло, т.е. като система. Всяка една от посочените функции може да се раздели на отделни под функции, респективно на задачи и подзадачи или на дейности и части, детайли от тях.

Функциите на системата за управление са и функции на нейния субект. Всички задачи, поставени пред една от службите за сигурност в Република България са задачи и на нейния ръководител като субект на управлението. Що се отнася до изпълнителите, то техните функции-задачи са само част от общите функции задачи на системата като цяло. Ръководителите на отдели, сектори или звена в службите за сигурност например изпълняват само част от общите задачи в системата за сигурност. Разпределението на отделните задачи между отделните звена е предварително установено съобразно разписаните функции и компетенциите на всяка служба, разглеждана като самостоятелна подсистема.

В системата на службите за сигурност всяко ръководство на отделната структура защитава своята жизненост, чрез настъпателни действия, чрез активността на целия личен състав. Тази активност от правна гледна точка е заповядана отвън, предизвикана от системата на изпълнително-разпоредителната власт. Множеството нормативни документи, предписания, критерии и показатели обаче, характеризират система за управление с

прекален централизъм. В съвременните условия в системата за управление на службите за сигурност стремежа на законодателите е да се съчетават централизма с децентрализма на поставяне на разпореждания и изпълнението на поставените задачи от състава. За да се превърнат целите и задачите в задължения за изпълнение, са необходими подходящи ресурси – кадри, средства и време, като и добре разпознати начини за изпълнение, които се реализират чрез функцията планиране. Тук от съществено значение е подбора на онези кадри, които разполагат с най-голямото количество информираност, и способности за прилагане на иновативните практики, чрез които ще се постигне качествено изпълнение. Проблемът с подготвеността на кадрите е от съществено значение за степента на изпълнение.

Различаваме различни видове управленски решения на базата на изведени критерии: Според предмета на дейност - постъпващи в организацията, инвестирането на капитални вложения, формирането развитието на персонала, оперативното ръководство на процесите, организацията на производствения процес, проучването на средата за сигурност и определяне на целите и промените и др. Според характера на решенията - рутинни или програмирани, нерутинни или непрограмирани. Според начина на вземане на решения- интуитивни, логически и рационални. Според броя на участниците- индивидуални, колективни /екипни/.

Сложността и многообразието на проблемите, функциите и задачите, които възникват и се поставят в процеса на управление на службите за сигурност изискват вземането на най-разнообразни управленски решения. Те могат да се класифицират според:

а/ вида на субекта, който взема решение - еднолични и колективни;

б/ значимостта във времето - стратегически, оперативни и тактически;

в/ организационно-йерархическото равнище на субекта – централно /общодържавно/, регионално /областно, териториално/;

г/ характера на задачите, за които се отнасят - правни, икономически, културни, спортни, финансови, кадрови и др.;

д/ правния статут на субекта- държавноправни, административно правни, публично правни, частни решения;

е/ обхвата на проблемите - общи и частни;

ж/ своята категоричност при изпълнението на целта- императивни /задължителни/, препоръчителни, указващи и уведомяващи;

з/ времетраенето в процеса, за който се отнасят - дългосрочни, средносрочни и краткосрочни;

и/ мястото си в достигането на общата цел - първоначални, междинни и крайни;

й/ характера на процеса на решаване- творчески /евристични/, нетрадиционни /иновативни/, рутинни, и смесени и др.

Когато говорим за системата на службите за сигурност имаме в предвид всички онези специализирани държавни органи, които по Конституция и на основата на устройствени и функционални закони и подзаконови нормативни актове са оторизирани да извършват дейности по защита на националната сигурност, противодействие на тайни посегателства и престъпления, създаващи заплаха за националната сигурност, чрез законосъобразни и регламентирани правомощия да използват в своята дейност специални форми, методи и средства на работа. Това са съвкупността от служби за сигурност на Република България, изчерпателно изброени в преходните и допълнителни разпоредби на ЗЗКИ: Държавна агенция „Разузнаване“, Националната служба за охрана, Държавна агенция „Национална сигурност”, Главна дирекция „Борба с организираната престъпност” на Министерство на

вътрешните работи, служба „Военно Разузнаване” на Министерството на отбраната и Държавна агенция „Технически операции”.

Службите за сигурност в публичното пространство и в теорията на управлението са припознати като „специални” служби. Понятието „специални” служби е по-широко от разузнавателните, контраразузнавателните и оперативно-издирвателните структури към Президента на страната или към изпълнителната власт. Има чисто разузнавателни дейности и полицейски или други /военни, научно- технически и научно-експертни/ дейности, свързани също с разузнаване. Ето защо в широкото тълкуване на специалните служби могат да се приобщят и военната полиция, жандармерията, граничната охрана и др. Специални са предоставените законови правомощия за прибягване до тайни негласни форми и методи на използване конспиративно на човешки и технически ресурси.

Съгласно нормативната уредба, също в ЗЗКИ са визирани и специализираните служби за обществен ред: Това са Главна дирекция „Национална полиция”, Главна дирекция „Гранична полиция”, Главна дирекция „Пожарна безопасност и защита на населението”, областните дирекции на МВР и дирекция „Вътрешна сигурност” на МВР.

Дирекция "Митническо разузнаване и разследване" към Агенция "Митници" при Министерството на финансите. На тази дирекция с последните промени в Закона за митниците през 2014-2015 г. им се вмениха функции по разследване на митнически престъпления и нарушения на митническия режим. Това са по същество полицейски ангажименти свързани с оперативно-издирвателни мероприятия.

Към тях трябва да се присъединят и частните охранителни дружества, осъществяващи охранителни и издирвателни действия в частния сектор. Засега нерегламентирано функционират и така нар. „детективски агенции”, които използват някои методи на оперативно-издирвателната дейност, скрито и маскирано фото и видео заснемане, външно проследяване и негласно наблюдение на лица и обекти, главно за разкриване на изневери на членове на семейството и нерегламентирани контакти на бизнес контрагенти.

Според множество изследователи управлението може да се разглежда като многофазен процес, в който се открояват различни стадии и етапи при които се наблюдава последователност, паралелност и цикличност. Това важи с пълна сила и за управлението на службите за сигурност на Република България в съвременните условия.

В управлението на службите за сигурност ръководителят е оторизираният от най-висшето равнище на законодателната или изпълнителната власт служител. Съгласно приетата нормативна уредба, Народното събрание избира председателите на ДАНС и ДАТО.

Съгласно чл. 19в от ЗСРС Държавна агенция "Технически операции" се ръководи от председател, който се назначава с указ на президента на републиката по предложение на Министерския съвет.

Държавна агенция "Национална сигурност" се ръководи от председател, който се назначава с указ на президента на републиката по предложение на Министерския съвет за срок 5 години.

Въз основа на разпоредбите, визирани в българската конституция Президентът на републиката е и върховен главнокомандващ въоръжените сили и има правото да издава укази и назначава директорите на ДАР, НСО и Служба „Военно разузнаване” , които също са му препоръчани от ръководителя на министерския съвет.

Министерският съвет съгласно Конституцията осигурява обществения ред и националната сигурност и осъществява общото ръководство на държавната администрация и на въоръжените сили. Министър-председателят на който е вменена по конституция функцията да ръководи и координира общата политика на правителството и носи

отговорност за нея, в това число и изпълнението на държавната политика за защита на националната сигурност има правомощията да назначава висшите оперативни ръководители на службите за сигурност и главния секретар на МВР.

На основата на приетите разпоредби в устройствените закони/ ЗДАНС, ЗМВР, ЗСРС, ЗОВС/ всеки ръководител на служба от своя страна избира по свое усмотрение и назначава ръководителите на дирекции, отдели и сектори в подчинената му организация. По този механизъм се устройва управленското проектиране и инженеринг на ръководните равнища в системата на службите за сигурност на Република България в днешно време.

Необходимо е ръководителят, независимо на каква позиция е разположен в управленската йерархия в системата на службите за сигурност да притежава способности, професионални и интелектуални компетентности и управленска култура, които биха допринесли за:

- ограничаване броя на допусканите грешки с помощта на използване неизчерпателните възможности на комплексния и интегриран подходи;
- правилно формулиране на личните междинни и стратегически цели и обезпечаване на тяхното изпълнение;
- задълбочено изследване на състоянието на различните системи, бързо изучаване и разкриване на техните основни елементи;
- ефективно управление на управляваната подсистема- обект на управление;
- способност за прогнозиране и предвиждане на събитията в средата за сигурност;
- правилно разработване на нови системи от съвременен тип;
- повишаване на качеството на експертизата и съкращаване на времето за вземане на адекватни управленски решения;
- умения за обединяване на знанията от различни науки за постигане на синергитичен ефект в културата и компетентността;
- правилна преценка на развиващите се събития, обстоятелства и процеси, както и за състоянието на уязвимост на обектите, определени за стратегическа и жизненоважна защита пред службите за сигурност.

Заключение

Бурният ръст на появата и развитие на новите форми на престъпност, свързани с прането на пари, фалшифицирането на парични и други банкови инструменти, нетрадиционни корупционни практики и разнообразни изяви на организирана и транснационална престъпност, предизвикват пристъпването към организационно развитие на системата на службите за сигурност. Необходимостта от задоволяването на тази актуална за гражданското общество потребност се свързва с даване на адекватен отговор на тези нетрадиционни престъпни прояви, които вече отправят своите ужилвания и спрямо интересите на други страни в международен план. Наложително е предприемане на неотложни стъпки на непосредствено преустройство и организационно развитие на системата в структурно, психологическо и функционално направления.

Организационното развитие ще доведе до положителни резултати в процеса на извършване на така дългоочакваната реформа в сектора на сигурност. Ще се постигне излизане от вътрешно служебните недоразумения, преодоляване на дублирането на функции и правомощия, недопускане на междуличностни конфликти на ръководителите на отделните служби за сигурност и обществен ред.

ЛИТЕРАТУРА:

[1] Закона за защита на класифицираната информация - Обн. ДВ. бр.45 от 30 Април 2002г., попр. ДВ. бр.5 от 17 Януари 2003г., изм. ДВ. бр.31 от 4 Април 2003г., изм. ДВ. бр.52 от 18 Юни 2004г., …..изм. и доп. ДВ. бр.60 от 7 Юли 2020г., изм. ДВ. бр.69 от 4 Август 2020г.

[2] Закон за специалните разузнавателни средства-ДВ, бр. 70 от 2013 г., в сила от 09.08.2013 г.) (1) (Изм. - ДВ, бр. 14 от 2015 г.).. изм. и доп. ДВ. бр.7 от 19 Януари 2018г., доп. ДВ. бр.56 от 6 Юли 2018г., изм. ДВ. бр.17 от 26 Февруари 2019г., доп. ДВ. бр.37 от 7 Май 2019г., изм. ДВ. бр.69 от 4 Август 2020г.

[3] Закон за Държавна агенция „Национална сигурност“ - в сила от 01.01.2008 г., …доп. ДВ. бр.94 от 29 Ноември 2019г., изм. ДВ. бр.99 от 17 Декември 2019г., доп. ДВ. бр.51 от 5 Юни 2020г.

[4] Закон за митниците - Обн. ДВ. бр.15 от 6 Февруари 1998г., изм. ДВ. бр.89 от 3 Август 1998г.,..изм. и доп. ДВ. бр.102 от 31 Декември 2019г., изм. ДВ. бр.14 от 18 Февруари 2020г.

Име на автора: проф. д-р Илин Александров Савов
Месторабота: Академия на Министерство на вътрешните работи, София, Факултет „Полиция“
E-mail: ilin_savov@abv.bg

ROLE AND PLACE OF THE MILITARY COUNTERINTELLIGENCE IN THE INTELLIGENCE COMMUNITY OF THE REPUBLIC OF BULGARIA

HRISTO A. HRISTOV

ABSTRACT: ***The recent security environment is characterized by dynamic changes and the tasks of the military counterintelligence bodies are not only at the national level, but must also comply with the common counterintelligence policy regulated by the relevant NATO counterintelligence documents. With this respect it is appropriate to analyze the role and place of the Bulgarian counterintelligence bodies in the intelligence community, their organization and tasks in comparison with the similar services of our coalition partners.***

KEYWORDS: ***Security services, Military counterintelligence, intelligence community, national security, national security protection system.***

РОЛЯ И МЯСТО НА ВОЕННОТО КОНТРАРАЗУЗНАВАНЕ (ВКР) В РАЗУЗНАВАТЕЛНАТА ОБЩНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

ХРИСТО А. ХРИСТОВ

АБСТРАКТ: *Съвременната среда за сигурност се характеризира с динамични промени и задачите на органите за ВКР са не само на национално ниво, но и трябва да съответстват на общата контраразузнавателна политика, регламентирана от съответните документи на НАТО за контраразузнаване. В този аспект е целесъобразно да се направи анализ на ролята и мястото на българските органи на ВКР в разузнавателната общност и тяхната организация и задачи в сравнение с аналогичните служби на коалиционните ни партньори.*

Key words: *Служби за сигурност, Военноконтраразузнаване, разузнавателна общност, национална сигурност, система за защита на националната сигурност.*

Високата степен на възможността на държавата самостоятелно да компенсира, неутрализира или управлява различните видове заплахи и надеждно да защитава гражданските, обществени и държавни интереси, които в съвкупност съставляват националните интереси, независимо от намеренията, действията и позицията на други страни, етнически, икономически, религиозни и други образувания се явява критерий за гарантиране на националната сигурност [9]. Имайки предвид предходното и анализа на процеса на трансформация на разузнавателните служби в развитите демократични европейски държави и посткомунистическите страни показва, че няма общ модел, а също така няма прости и ясни отговори на въпросите, свързани с този процес.

В света няма държава със съвършена система на функциониране на националната сигурност, с универсален модел на взаимодействие на разделените власти в сигурността, който може да бъде наложен като матрица върху всяко демократично общество. Хронологично, към настояще време, са създадени второ поколение, а за някои системи – и трето поколение закони в системата на националната сигурност, чиято основна цел е била оптимизирането на системата. Но това оптимизиране е продължителен процес. На настоящия етап системата за национална сигурност не е добре балансирана с възможности тя да бъде използвана за тяснопартийни интереси.

Създаването през 2008 г. на Държавната агенция „Национална сигурност“ е първият пробив в извеждането на специалните служби от мегаминистерството на вътрешните работи и създаването на модерна система на контраразузнаване.

На базата на анализа на ролята и мястото на ВКР в СЗНС на чужди държави и на база на доктрината за Разузнаване и Контраразузнаване на НАТО, изхождайки от променливата и динамично променяща се среда за сигурност в Балканския регион, е наложителна промяна в структурата и задачите на ВС на РБ. Налага се изводът, че е необходима нова концепция за позиционирането на ВКР в СЗНС на Р България.

Концепцията трябва да отразява еволюцията на възгледите относно контраразузнавателните дейности, в които е необходимо участието на всички държавни служби и институции. Тя трябва да отчита, че контраразузнаването трябва да отразява посегателствата не само на чуждестранни разузнавателни служби и техните агенти, но и на терористи, транснационални престъпни групи, кибернетични шпиони, злонамерени вътрешни лица, както и на международни промишлени конкуренти, свързани или подозирани във връзки с тези структури.

Разработването на подробен модел на дейността на военното контраразузнаване в Българските въоръжени сили е сериозен изследователски процес, който трябва да се базира на нов архитектурен модел на управление и функциониране на цялата разузнавателна общност у нас. Сега съществуващият такъв има редица пропуски [9].

В доклада са предложени базови принципи за концепция за военното контраразузнаване, препоръки на базата на опита на автора и анализ на съществуващите документи за дейността на войсковото контраразузнаване, като се започне отдолу нагоре. Винаги трябва да се има предвид обстоятелството, че войсковото контраразузнаване на ниво бригада, батальон, контингент, формирование в мисия, трябва да работи във взаимодействие с аналогичните служби на коалиционните партньори (съюзната доктрина AJP2A) [1].

Авторът се придържа към мнението, че основното във войсковото контраразузнаване е дейността по идентифициране и неутрализиране на заплахите за сигурността, произтичащи от неприятелски разузнавателни служби или организации или от лица, занимаващи се с шпионаж, саботаж, подривна дейност, тероризъм и новата заплаха, породена от кибератаки на компютърните системи. Под подривна дейност следва да се разбират пропаганда и агитация, разпространение на агитационни материали, демонстрации, вербоване на поддръжници за противникови идеи, използване на организации под прикритие за истинска дейност, създаване на климат на недоверие към командирите, разпространение на слухове или дезинформация. AJP2A [1].

На база на получени резултати от направения преглед и изложената научна експертиза е целесъобразно у нас всички военни служби за сигурност и разузнаване да имат единно военнополитическо ръководство, което да има три нива на управление:

- Стратегическо ниво на управление на ВКР;
- Оперативно ниво на управление на ВКР;
- Тактическо (войсково-полево) ниво на управление на ВКР (вж. фиг. 1.).

Стратегическото ниво на управление е задача на нова Агенция „Военно разузнаване и сигурност“, подчинена директно на министъра на отбраната, в състава на която да влизат три служби: Служба „Военна информация“ (СВИ), Служба „Военно контраразузнаване“ (СВКР) и служба „Военна полиция“ (СВП). Задачите на агенцията могат да се формулират така:

- добиване на военнополитическа, военнопромишлена и военна информация, която улеснява процеса на вземане на решения на правителството, както и събиране на всички

необходими данни за стратегическо-оперативното и информационно планиране на МО и Щаба по отбрана;

- откриване и предотвратяване на усилията на чуждестранните тайни служби, засягащи суверенитета и отбранителните интереси на Р България;
- откриване и предотвратяване в своята област на отговорност на всички тайни усилия, насочени към нарушаване или промяна на конституционния ред на Р България чрез използване на различни средства;
- събиране на информация за терористични организации, заплашващи националната сигурност, откриване и предотвратяване на усилията на чуждестранни сили, организации или лица за извършване на терористични актове срещу организации на МО или въоръжените сили;
- събиране на информация за организации, групи и лица, които биха се поддали на влиянието на различни религиозни движения, в това число и забранени, в резултат на което биха се ангажирали с антиконституционни, политически екстремистки, сепаратистки и дори терористични прояви [6] в Министерство на отбраната и Българската армия.
- събиране в рамките на нейната компетентност, възложени с нормативни актове за националната сигурност, на информация за организирана престъпност, засягаща нейното функциониране, за престъпни деяния, застрашаващи МО и въоръжените сили при изпълнение на техните задачи, както и за всяка кибернетична дейност, която нарушава интересите на отбраната на страната ни и на всички усилия и опити, насочени срещу български части и войски, разгърнати в операции;
- събиране на информация за религиозни деноминации, чийто непосредствени цели са финансово-икономически (за получава полезна информация за конкурентите или икономическите възможности) и шпионство (набиране на информация от областта на отбраната и сигурността, финансите и икономиката, социалната сфера) [5] в полза на чужди разузнавателни служби.
- изпълнение на съответните задачи, свързани с националната сигурност, във връзка с всякакви промишлени, научноизследователски и развойни дейности, производство и свързани с търговията дейности за отбраната, на компетентните органи на Министерството на отбраната или въоръжените сили и предприемане на необходимите мерки, от една страна, за откриване, предотвратяване или възпрепятстване на незаконната търговия на международно контролирани продукти, технологии, отбранително оборудване и услуги, а от друга страна, контролиране на тяхната законна търговия;
- осигуряване на сигурност и защита на стратегически военни обекти и инсталации, както и на правителствените и военни съоръжения за контрол и управление;
- изготвяне на всички квалификации, разрешения за достъп и задачи, свързани с личната защита на лица, заемащи важни и поверителни длъжности, както и на икономически организации, специални поръчки, военни събития и учения.
- предотвратяване и разкриване на криминални престъпления в рамките на подчинените на МО организации и формирования;
- опазване на войсковия ред във военните формирования и военните гарнизони.

Военното разузнаване, което е наследник на сегашната служба ВИ, трябва да реализира всички видове разузнавания посочени в AJP2A [4].

В предлагания модел на интегриране на разузнавателните, контраразузнавателните и полицейските дейности на общо подчинение на министъра на отбраната отпада необходимостта от наличие на Специализирана дирекция „ВКР“ в ДАНС. Освен това моделът изисква всички служители от СВКР да имат завършено висше военно образование, да получават военни звания и имат задължението да носят военна униформа при работата

си във военните формирования. Естествено това би ликвидирало и аномалията – в органите по сигурност да има служители на ВКР без военно образование и служба. Това несъмнено ще повиши авторитета на ОВКР пред командирите и военнослужещите от формированията, които обслужват.

Моделът ще се отрази благоприятно на вербовъчния процес и на работата със секретните сътрудници на ОВКР, както и ще гарантира ефективността на КРР при осигуряване на национални военни контингенти при участие в международни мисии зад граница.

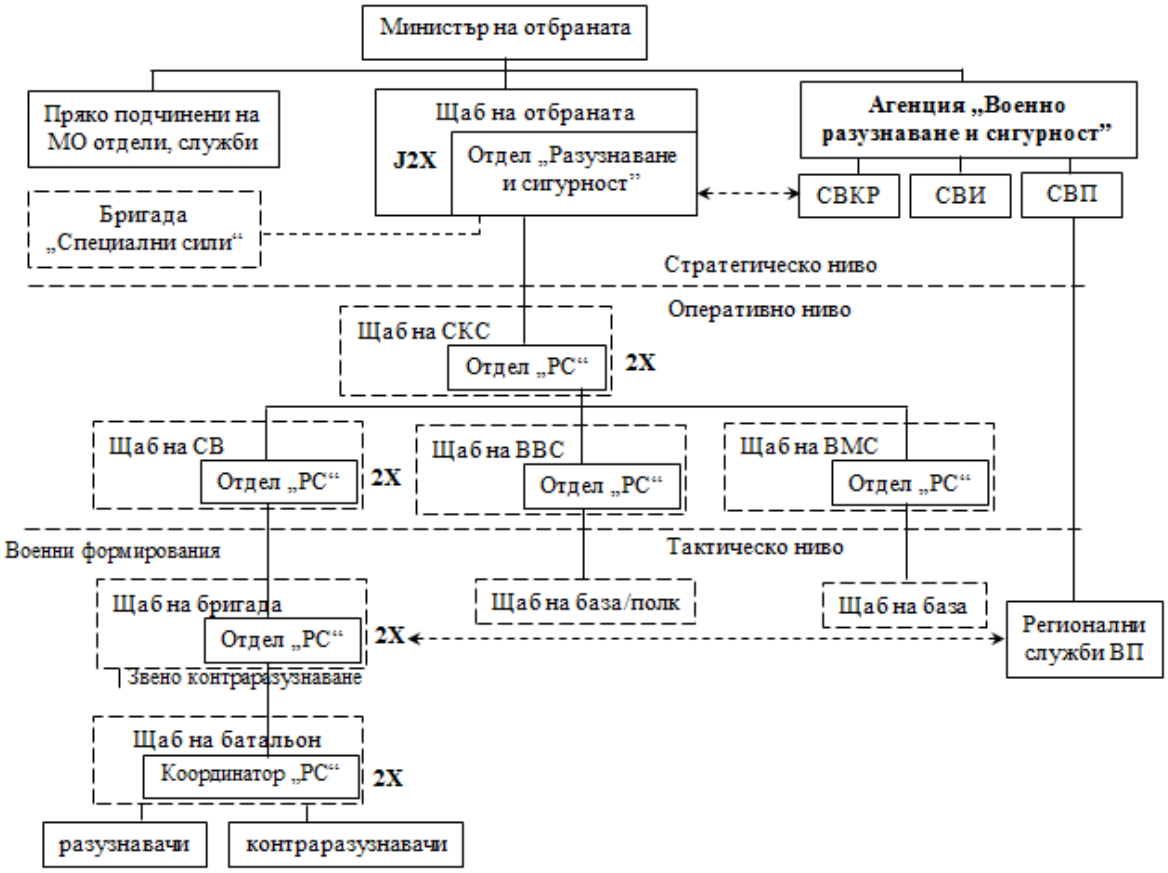
Сигурността на всички войскови нива се ръководи от командването, затова към всеки щаб трябва да се формира отдел, сектор или звено по разузнаване и сигурност, наричани по-нататък „щабове по сигурността“ аналогично на съюзните структури 2Х в командната верига, които да дават препоръки на командването по въпросите за сигурността и да ръководят цялата дейност по нейното осигуряване. Създаването на контраразузнавателен орган в щабовете на военните формирования осигурява на командването контраразузнавателни способности, с каквито към момента те не разполагат.

Показаните елементи за разузнаване и сигурност в щабовете комбинират контраразузнаването и войсковото агентурно разузнаване (HUMINT) под ръководството на офицер – координатор по разузнаване и контраразузнаване в щаба по сигурността на съответното ниво. В рамките на щаба контраразузнавателните звена отговарят за координиране на контраразузнавателната дейност. Щабове по сигурността има във всяко военно формирование, приравнено на бригада и батальон.

Основните отговорности на тези щабни структури, показани на трите нива на контраразузнаване на фигура 1 са [1]:

1. Информиране на командира за всички заплахи за сигурността на повереното му военно формирование (шпионаж, тероризъм, саботаж, подривна дейност, организирана престъпност или кибератаки срещу автоматизираните системи и мрежи).
2. Управление и поддръжка на операциите за противодействие на заплахите за сигурността (оценка на заплахите, мерки за сигурност на личния състав, физически мерки за сигурност, оперативни мерки за сигурност, мерки по информационна сигурност).
3. Събиране, обработка и споделяне на информация, относима към контраразузнавателните изисквания и изготвяне и разпространение на информация за текущите заплахи за сигурността.
4. Принос към процеса за оперативна сигурност (вкл. планиране, координация и прилагане на мерки за защита и сигурност за цялото формирование).
5. Създаване и поддържане на връзки с „цивилните“ правоприлагащи и контраразузнавателни органи.

Контраразузнавателните органи трябва да контролират стриктното спазване на фундаменталния принцип на сигурността – „необходимо да се знае“ от военнослужещите за достъп до класифицирана информация. Един от важните принципи на операциите по сигурността е тяхното координиране с щаба на разузнаването и всички разузнавателни усилия. Тъй като начинът, по който е организирано контраразузнаването в страните от НАТО не е еднакъв, контраразузнавателните структури при коалиционни операции трябва да държат връзка с пункта за контакт в щаба по отбраната и други структури.



Фиг. 1. Модел на нива на управление на ВКР (концепция)

На фигура 2 е показан модел на контраразузнавателния процес, анлогичен на другите разузнавателни процеси въз основа на разузнавателния цикъл [6] със следните етапи:

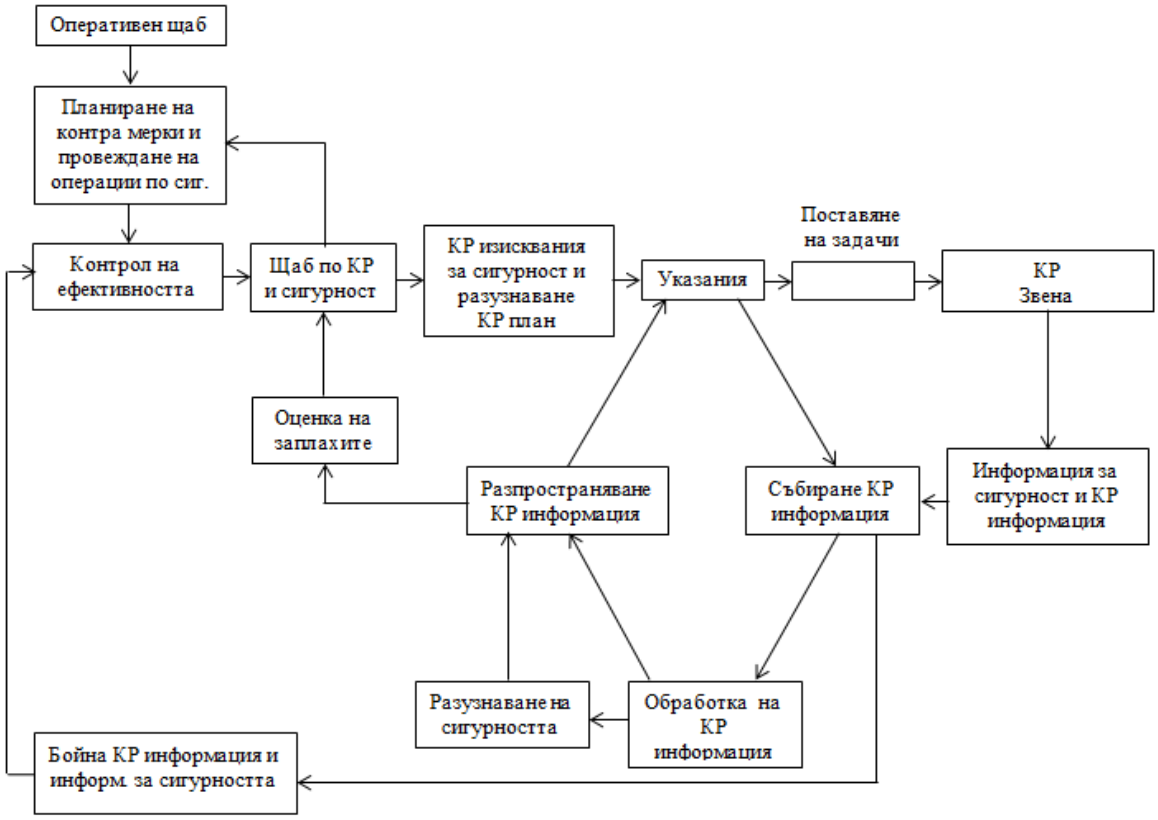
1. Указания;
2. Събиране на информация;
3. Обработка на контраразузнавателната информация;
4. Разпределение на контраразузнавателната информация.

За успеха на контраразузнавателните (КР) операции има значение добрият КР план, в който освен заплахите за формированието трябва да се посочват и контрамерките за защита. Командирите, в чиито отговорности влиза и контраразузнаването, имат нужда от КР информация, отразена на фигурата като КР изисквания, която по реда на приоритеност включва:

- информация за разузнавателните служби на държави, които не са членове на НАТО и организации, занимаващи се с подривна дейност;
- своевременна текуща КР информация, допълваща горната информация, а така също и своевременна информация за терористични и престъпни групировки;
- спешна информация, изискваща вземането на незабавни контрамерки от формированията на НАТО.

Контраразузнавателната оценка на заплахите е препоръчително да обхваща следните раздели: Шпионски действия; Саботажи; Подривни действия; Терористични действия; Действия на организираната престъпност; Компютърна мрежова атака и Обща оценка.

Най-ниското контраразузнавателно изпълнително звено в предлагания модел на СВ работи в тясна връзка с офицера от щаба по разузнаването и координира работата си с поддържаното подразделение 2Х. Препоръчително е да се състои от 4 души – офицери от контраразузнаването. Контраразузнавателното звено извършва контраразузнавателните разследвания и операции (разпити, операции с източници, поддържане на връзка, проверки), контраразузнавателен анализ и техническа поддръжка, за да защити частта, която поддържа, от дейността на противниковото разузнаване. Моделът на щаб по сигурността е до бригада, на ниво батальон е един офицер – 2Х.



Фиг.2. Модел на контраразузнавателен (КР) процес

В предлагания модел на нова структура на армейското контраразузнаване офицерите трябва да са назначени и обучени да провеждат разследвания и операции за контраразузнаване в армията, да разполагат с правомощия за арест и юрисдикция при разследването на престъпления, свързани с националната сигурност, като измяна, шпионаж, подбудителство, подривна дейност, саботаж с намерение да се навреди на националната отбрана и за подкрепа за международния тероризъм, докато другите наказателни дела се разследват от военната полиция.

Структурата на звената за контраразузнаване във ВВС и ВМС трябва да са съобразени и да отчитат спецификата на двата вида въоръжени сили.

Операциите за сигурност трябва да се провеждат съгласно следните принципи:

- Командирите на всички нива са отговорни за сигурността;
- Политиката за сигурност трябва да присъства на всяко ниво от командването;
- Трябва да се създават екипи по сигурността, за да работят по заплахите и да предоставят съвети по въпроси за сигурността на командирите на всяко ниво на командване;

- Информация за заплахата трябва да се изготвя от разузнавателния персонал и този по сигурността – предупреждения, оценки на заплахата и становища за нивото на заплахата;
- Събирането на информация, свързана със сигурността трябва да бъде координирано на всяко ниво на командване и интегрирано с усилията за цялостно събиране на разузнавателна информация.

Сигурност по защитата се дефинира като организирана система от отбранителни мерки, въведени и поддържани на всички нива на командване с цел постигане и поддържане на сигурност. Това е защита на силите и средствата, в това число и личния състав, от нежелано събитие или от компрометиране. Съществуват 4 категории мерки по защита на сигурността: Сигурност на личния състав, Физическа сигурност, Сигурност на операциите, Информационна сигурност (INFOSEC).

Процедурите за защита на сигурността включват: Разработване на оценка на заплахата; Мерки за сигурност; Физически мерки за сигурност; Оперативни мерки за сигурност; Мерки по информационна сигурност.

Контраразузнавателните звена в щабовете по сигурността изпълняват контрамерки в целия спектър на контраразузнаването и сигурността и имат следните цели:

Възпиране – дейностите по провеждане на явни мерки за ефективно възпиране на потенциалния нападател.

Недопускане – дейностите за предотвратяване на достъпа на противника до защитена и чувствителна информация, предотвратяване на неблагоприятно влияние върху личния състав и проникване зад преградите на физическата ни сигурност.

Разкриване – разобличаването и неутрализирането на дейността на противника за извършване на посегателства срещу сигурността на ВС.

Дезинформация – дейността, която се използва за въвеждане на противника в заблуждение за способностите и намеренията на приятелските сили, целите, задачите и възможностите на военните формирования.

Предложеният модел за интегрирана Агенция „Военно разузнаване и сигурност“ може да се приложи и при осигуряване на сигурността на български военнослужещи, участващи в мисия зад граница, като допринася за оперативността за добиване на пълна и достоверна информация относно средата за сигурност, военнополитическата обстановка, както и предприемане на своевременни мерки за защита на сигурността на военнослужещите от контингента и българските граждани, пребиваващи на територията на дадената държава.

Опитът на автора от участие в мисия на ЕС „Алтея“ в Босна и Херцеговина показва, че при състав на войсковия контингент с ранг на рота (140 и повече военнослужещи), с цел максимално ефектив и надеждно осигуряване на разузнавателни и контраразузнавателни способности на контингента е необходимо в щаба на ротата да има звено – тим по сигурността (ТС) на интегрираната Агенция „Военно разузнаване и сигурност“, което да се състои от минимум 5 военнослужещи, както следва:

- Началник (ръководител) на звеното – старши офицер от агенцията с натрупан опит от участие в мисии зад граница, осигуряващ разузнавателните и контраразузнавателните способности на българския войскови контингент с основни функции да ръководи дейността на тима и да координира взаимодействието със сродни и партньорски служби за сигурност на местно, национално и международно ниво;
- Член на ТС – офицер от военното разузнаване, осигуряващ разузнавателните способности на български войскови контингент с основни функции работа с доброволни сътрудници и източници на информация от местното население и население от страните в конфликта;

- Член на ТС – офицер от ВКР, осигуряващ контраразузнавателните способности на български войскови контингент с основни функции работа с доброволни сътрудници и източници на информация сред личния състав на контингента;
- Член на ТС – офицер от ВП, осигуряващ противодействието на криминални прояви на личния състав на контингента и войсковия и вътрешния ред на българските военнослужещи в базата;
- Член на ТС – завеждащ регистратурата за класифицирана информация и с функция шофьор на звеното.

За гарантирането на надеждно разузнавателно и контраразузнавателно осигуряване и повишаване на сигурността на контингента по време на участието му в операция и/или мисия зад граница, ТС на Агенцията „Военно разузнаване и сигурност“, следва да изпълнява задачи, свързани с:

1. Анализ и оценка на оперативната обстановка в контингента, средата за сигурност по линиите и направленията на работа на АВРС, спецификата и особеностите на военнополитическата обстановка, спецификата и особеностите на местността (релеф, климат) в зоната на операцията, тенденции относно рисковете и заплахите за сигурността на участниците в мисията и др.

2. Разкриване на интересите на чуждите специални служби, подпомагащите ги организации и лица, насочени към българския военен контингент, коалиционните партньори и интересите на Р България.

3. Контрол на терористичната активност и долавяне на преки и косвени признаци за намерения, подготовка и организация за извършване на терористични атаки срещу личните състави на българския контингент, войските от коалицията и базите на дислокация от страна на паравоенни формирования, терористични групи и организирани престъпни организации.

4. Подпомагане на дейността на командванията на военните контингенти по защита на сигурността на военнослужещите, както и българските граждани и коалиционните партньори в театъра на бойни действия.

При определяне на модела на структурата и функциите на звеното на Агенция „ВРС“, което да гарантира надеждното осигуряване на разузнавателни и контраразузнавателни способности на български войскови контингенти зад граница с ранг на батальон, е необходимо да се вземе предвид мнението на експерти от военното разузнаване, контраразузнаване и военна полиция, участвали в операции по подържане на мира и се отчете спецификата на конкретната задгранична мисия.

Заключение

Направеният в монографията анализ на развитието на органите за сигурност във войските на развитите държави показва, че военното контраразузнаване присъства като неизменна част в системите за защита на националната им сигурност. Ролята и мястото на тези служби в тези системи се определят от характерните за даден период външни и вътрешни заплахи за националната сигурност, целите на функциониране на органите в системата за сигурност и основните задачи за защита на националната сигурност, които се възлагат от националните законодателства и коалиционни доктрини.

Предложената концепция и модел за ново по-ефективно позициониране на ОВКР в разузнавателната общност на Р България може да бъде принос на научната общност в сложния и продължителен процес на реформиране на системата за защита на националната сигурност.

ЛИТЕРАТУРА

[1] Алипиев, И. Необходимост от изграждането на нов архитектурен модел за управление на разузнавателната ни общност. CSDM Views 8, Център за мениджмънт на сигурността и отбраната, София. 2012. ISSN 1314-5622.

[2] Алипиев, И. Позициониране на разузнавателната общност в националния сектор за сигурност. CSDM Views 3. ISSN 1314-5622 https://it4sec.org/system/files/views_003.pdf?download=1.

[3] Бакалов, Й. Теоретичен модел на политика за сигурност и граждански контрол в Р България. НБУ, София. 2011. ISBN 978-954-535-689-6.

[4] Солаков Т., Дестриктивните религиозни организации и техните цели в държавата, публикувано в Сборник Научни трудове международна Научна конференция „Широка сигурност“, Том 2, Кибер сигурност. Икономическа, социална и културна сигурност, ISSN 978-619-7383-19-5, София, 2020. стр. 548-555.

[5] Солаков Т., Религиозните секти като заплаха за националната сигурност, Сборник доклади от годишна университетска научна конференция 27-28 юни 2019г., Издателски комплекс на НВУ „Васил Левски”, ISSN 2367-7481, стр. 551-559.

[6] Съюзна доктрина на НАТО за разузнаване, контраразузнаване и сигурност. AJP 2.0 (A). 2014.

[7] Христов, Х. Сигурност на фирмата и противодействие на посегателствата срещу нея. Университетско издателство „Еп. Константин Преславски“, Шумен. 2014. 328 с. ISBN 978-954-577-981-7.

[8] Official site of Információs Hivatal. http://www.ih.gov.hu/.

[9] Solakov T., „Theoretical aspects of national security”, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas – Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 68, April 2020, pp. 154-164.

Христо Атанасов Христов
Шуменски университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
E-mail: h.a.hristov@shu.bg

RETURN ON INVESTMENT IN SECURITY CULTURE

VLADIMIR V. YANKOV

ABSTRACT: *Some organizations still view security as a predominantly technical issue and pay little attention to the beliefs, attitudes, and other cultural factors that characterize the security system. It is therefore important to consider the financial costs and actual benefits of a well-developed security culture in organizations in order to determine cost-effectiveness. In other words, what will this cost in terms of financial and other resources and what benefits will the organizations receive as a result.*

Due to the preventive and protective nature of security, it is not easy to define reliable criteria for return on investment, and developing a meaningful cost-effectiveness ratio for a security culture is an even greater challenge because culture is based primarily on intangible beliefs, attitudes and values. Its effects are long-term and are often combined with other factors, which makes their assessment quite variable.

Keywords: *Security, Security culture, Return on investment*

ВЪЗВРЪЩАЕМОСТ НА ИНВЕСТИЦИЯТА В КУЛТУРАТА НА СИГУРНОСТ

ВЛАДИМИР В. ЯНКОВ

АБСТРАКТ: *Някои организации все още гледат на сигурността като на предимно технически въпрос и почти не обръщат внимание на убежденията, отношенията и други културни фактори, които са характерни за системата на сигурност. Затова е важно да се разгледат финансовите разходи и действителната полза от добре развита култура на сигурност в организациите, за да се определи ценовата ефективност. С други думи, какво ще струва това по отношение на финансови и други ресурси и какви ползи ще получат като резултат организациите.*

Поради превантивния и защитен характер на сигурността не е лесно да се определят надеждни критерии за възвращаемост на инвестициите, а разработването на смислено съотношение разходи / ефективност за културата на сигурност е дори още по-голямо предизвикателство, защото културата се основава преди всичко на нематериални вярвания, нагласи и ценности. Нейните ефекти са дългосрочни и често се комбинират с други фактори, което прави оценката им доста променлива.

1. Въведение

Терористичните атаки през изминалите години в редица европейски държави очертават тенденция на увеличаващ се риск от терористична дейност. Няма съмнение, че това се отнася в еднаква степен и за България, която не е изолирана. Поради значимоста на корпоративния сектор за националната сигурност, заплахите за сигурността на търговските дружества следват в голяма степен тенденциите на заплахите в глобален план, включвайки заплахи от радикализация, терористични действия, организирана престъпност и кибертероризъм.

Предотвратяването и неутрализирането на тези заплахи само чрез звена за охрана, фирмена и информационна сигурност, става все по трудно в аспекта на увеличаващата се хибридност на тези заплахи в световен мащаб. Противодействието на такива комплексни и дори все още невъзникнали заплахи, изисква определени ценности и нагласи, споделяни от всички в дружествата, които определят подхода и разбирането на ръководителите и служителите към сигурността.

2. Изложение

Човешкият фактор като цяло е допринесъл за всички инциденти свързани със сигурността. Те включват умишлени злонамерени действия, неумишлени грешки на персонала, въпроси свързани с проектирането и оформлението на софтуера и хардуера, неадекватни организационни процедури и процеси, както и грешки в управлението. Повечето пропуски в сигурността са резултат на човешки слабости и недостатъци като ниска мотивация, грешни преценки или злонамереност.

Колкото по-сложни са технологиите и мерките за сигурност, толкова по важни са хората, които ги проектират, оперират с тях, поддържат и подобряват материалната част. Дори добре проектирана система може да стане неефективна, ако необходимите процедури за експлоатация и поддържане са непълни или ако операторите не умеят да следват процедурите. В крайна сметка, целият режим на сигурност издържа или се проваля заради хората, които са включени в него.

В действителност, нарушенията сред персонала по отношение на сигурността, както неумишлени, така и преднамерени, не се осъществяват в изолирана среда. В повечето случаи те са резултат на нарушена организационна култура.

Организационната култура определя начина на поведение в организацията. Тази култура се състои от споделени вярвания и ценности, установени от лидерите и след това комуникирани и подсилени чрез различни методи, в крайна сметка оформящи възприятията, поведението и разбирането на служителите. Организационната култура задава контекста за всичко, което се прави в една организация. Понастоящем недвусмислено е доказано и признато, че организационната култура представлява значим фактор в работата, производителността, безопасността, съответствието с изискванията и дисциплината на персонала.

Характеристиките на организационната култура, които са съотносими към сигурността, формират културата на сигурност. Така културата на сигурност може да се определи като споделени вярвания и ценности в организацията, които определят как хората се очаква да мислят и да подхождат към сигурността.

Някои организации все още гледат на сигурността като на предимно технически въпрос и почти не обръщат внимание на убежденията, отношенията и други културни фактори, които са характерни за системата на сигурност. Затова е важно да се разгледат финансовите разходи и действителната полза от добре развита култура на сигурност в организациите, за да се определи ценовата ефективност. С други думи, какво ще струва това по отношение на финансови и други ресурси и какви ползи ще получат като резултат организациите.

Поради превантивния и защитен характер на сигурността не е лесно да се определят надеждни критерии за възвращаемост на инвестициите, а разработването на смислено съотношение разходи / ефективност за културата на сигурност е дори още по-голямо предизвикателство, защото културата се основава преди всичко на нематериални вярвания, нагласи и ценности. Нейните ефекти са дългосрочни и често се комбинират с други фактори, което прави оценката им доста променлива.

Възвръщаемост на инвестицията (ROI – Return on investment) е най-обичайната мярка за ефективност, използвана за оценка на ефективността на инвестицията или сравняване на ефективността на различни инвестиции. Този опростен класически финансов подход оценява възвръщаемостта на инвестицията чрез сравняване на паричната стойност на инвестицията с паричната стойност на печалбата, получена от тази инвестиция. За да се изчисли възвръщаемостта на инвестицията, печалбата от инвестиция се разделя на цената на инвестицията и резултатът се изразява като процент или съотношение.

$$ROI = \frac{\text{Печалба от инвестицията - Цена на инвестицията}}{\text{Разходи за инвестиция}}$$

Сигурността обикновено не е инвестиция, която води до печалба. Сигурността е по-скоро намаляване на риска за активите на фирмата, или с други думи, печалбата може да бъде изразена чрез измерване на това колко загуби се избягват поради инвестицията в сигурността. Съотношението възвръщаемост на инвестициите в сигурността (ROSI – Return on security investment) е дадено по-долу:

$$ROSI = \frac{\text{Намаляване на загубите - Разходи за инвестиция}}{\text{Разходи за инвестиция}}$$

При формулирането на съотношението за възвръщаемост на инвестицията за културата на сигурност трябва да се вземе под внимание и това, че инвестицията в култура на сигурност гарантира чрез човешкия фактор, че системите за сигурност ще бъдат толкова ефективни, колкото са проектирани. Дори и най-скъпата система за сигурност би се провалила без подходяща култура на сигурност. Т.е. инвестицията в културата на сигурност гарантира ефективността на инвестицията в системите за сигурност.

Така съотношението възвръщаемост на инвестицията в култура на сигурност (ROSCI – Return on security culture investment) ще отчете доколко културата на сигурност се повишава поради инвестицията и ще добави стойност към инвестицията в системи за сигурност:

$$ROSCI = \frac{\text{Подобряване на културата на сигурност} + \text{Инвестиции в системи за сигурност} - \text{Разходи за инвестиции в култура на сигурност}}{\text{Разходи за инвестиция в култура на сигурност}}$$

Тъй като подобряването на културата на сигурност води до повишаване на сигурността, можем да я заменим с намаляване на риска за активите на организацията и така уравнението ще стане:

$$ROSCI = \frac{\text{Намаляване на риска за активите на организацията} + \text{Инвестиране в системи за сигурност} - \text{Разходи за инвестиция в култура на сигурност}}{\text{Разходи за инвестиция в култура на сигурност}}$$

За да се определи дали съотношението е положително, т.е. инвестицията е ефективна, трябва да разберем какви биха били хипотетичните разходи за инвестиция в културата на сигурност за една организация. Ефективната култура на сигурност зависи от правилното планиране, обучение, осведоменост, експлоатация и поддръжка, както и зависи от хората, които планират, управляват и поддържат системи за сигурност. Най-съществена

роля в развитието на културата на сигурност имат ръководителите в организациите, затова основните разходи ще са за развитие на лидерски умения в ръководителите. От голямо значение също така са индивидуалното разбиране и ангажимент на персонала към ролята и отговорностите за сигурността, както и ангажимента за непрекъснато усъвършенстване, които се развиват чрез обучение и мотивация.

Обикновено тези разходи не надхвърлят инвестицията в системите за сигурност, откъдето веднага може да се заключи, че инвестицията в развитие на култура на сигурност само по този показател ще има положителна възвръщаемост. Допълнително, правилното изграждане на културата на сигурност в организацията ще помогне за развитието на съзнателна работна сила и ще насърчи желаното поведение по отношение на сигурността, което се иска от персонала. Крайната цел на развитието на културата на сигурност е да се изградят желаните стандарти на поведение на персонала. Тези стандарти включват професионално поведение, лична отговорност, придържане към процедурите, работа в екип и сътрудничество, както и бдителност. И тъй като културата на сигурност не е изолирана, то нейното подобряване ще доведе до подобряване на цялостната организационна култура в институцията и оттам подобряване на цялостната ѝ дейност.

3. Заключение

Инвестицията в подобряване на културата на сигурност ще гарантира, че инвестициите в системите за сигурност ще бъдат максимално ефективни и ще осигурят защитата на активите на организацията. Ефективната култура на сигурност ще даде допълнително многобройни предимства, ще насърчи работната сила да поддържа наблюдателността си, да задава въпроси за неправилни действия, да изпълнява работата си усърдно, да демонстрира високи стандарти на лична и колективна отговорност. Това не е панацея, но може ефикасно да допринесе за жизнено-здрав и безкомпромисен режим на сигурност, разпростиращ се върху всички работещи в организацията. Той спомага институцията да бъде в крак със нарастващите заплахи и рискове, които са толкова многобройни, че дори и най-прозорливите лидери не са в състояние да предскажат.

ЛИТЕРАТУРА

[1] International Atomic Energy Agency, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna 2008.

[2] VladimirYankov, Paul Ebel, Igor Khripunov, Self-Assessment of Nuclear Security Culture at Kozloduy NPP (Bulgaria): Cost and Benefit, Institute of Nuclear Materials Management 57th Annual Meeting, Atlanta 2016

[3] European Network and Information Security Agency, Helping CERTs assessing the cost of (lack of) security, 2012

Име на автора: инж. докторант Владимир Василев Янков
Месторабота: Началник отдел „Ядрена сигурност”, „АЕЦ Козлодуй” ЕАД
E-mail: vladimir@vladoyankov.com

THE CRITICAL FIVE - A PARTNERSHIP FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE

KONSTANTIN I. STOYANOV

ABSTRACT: *The intelligence services of five countries - the United States, Britain, Canada, Australia and New Zealand, are joining forces to protect critical infrastructure, in the alliance of Five Eyes or Critical five. This project supports the ongoing effort to clearly articulate and communicate a common message on the value, purpose, and historical trajectory of this important functional domain and seeks to arrive at a common understanding of critical infrastructure and its role in society. The narrative identifies shared priorities and interconnections among our countries and lays the foundation for future collaboration. The approach used in this narrative is to identify similarities in definition, approach, concept, and implementation in order to arrive at a shared understanding of critical infrastructure.*

KEYWORDS: *protection, sustainability, critical infrastructure, prosperity, cooperation.*

КРИТИЧНАТА ПЕТОРКА – ЕДНО ПАРТНЬОРСТВО В ИМЕТО НА ЗАЩИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

КОНСТАНТИН И. СТОЯНОВ

АБСТРАКТ: *Разузнавателните служби на пет държави – САЩ, Великобритания, Канада, Австралия и Нова Зеландия, обединяват усилия в защита на критичната инфраструктура, в алианса Five Eyes или Critical five (Критичната петорка). Този проект подкрепя продължаващите усилия за ясно формулиране и предаване на общо послание за стойността, целта и историческата траектория на тази важна функционална област и се стреми да постигне общо разбиране за критичната инфраструктура и нейната роля в обществото. В обединението, държавите идентифицират приликите в дефиницията, подхода, концепцията и изпълнението, за да се постигне общо разбиране за критичната инфраструктура [1].*

Статията прави опит да представи перспективите за защита на критичната инфраструктура в рамките на едно трансгранично, дори трансконтинентално сътрудничество. По-специално, тя се фокусира върху възможностите и ползите, които предлага такова сътрудничество. Наред с принципните формулировки и анализи, статията дава и конкретен, актуален пример (доколкото на него е дадена публичност) за резултата от взаимодействието и обмена на информация за обща кауза и/или интерес.

Статията е съсредоточена изцяло върху алианса „Критичната петорка“, извеждайки го от контекста (ако това е възможно) на външна политика и геостратегически интереси на отделните страни.

В днешния взаимозависим и взаимосвързан свят безопасността и сигурността на критичната инфраструктура изисква съгласуваните усилия на публичните и частните партньори по целия свят. Департаментът за вътрешна сигурност (DHS) си сътрудничи с международни партньори за подобряване и насърчаване на трансграничната и глобална сигурност и устойчивост на критичната инфраструктура чрез споделяне на информация, така че всички да могат да се възползват от обмена на най-добри практики, експертни познания и научени уроци.

Критичната петорка е създадена през 2012 г. с цел подобряване на обмена на информация и работа по въпроси от взаимен интерес между Австралия, Канада, Нова Зеландия, Обединеното кралство и САЩ. Групата англоговорящите страни, които споделят общи културни и исторически връзки с Обединеното кралство, известни с термина ***Англосферата***[1] и днес поддържат тясно политическо, дипломатическо и военно сътрудничество. [1]

Националните правителства на държавите са създали отдели и служби, които да подпомагат управляват рисковете за тяхната критична, национално значима инфраструктура:

- **Съединени американски щати:**
  - Министерство на вътрешната сигурност (Department of Homeland Security, DHS);
    - Агенция за киберсигурност и сигурност на инфраструктурата (Cybersecurity & Infrastructure Security Agency, CISA);
- **Канада:**
  - Канадска служба за разузнаване на сигурността (Canadian Security Intelligence Service, CSIS);
  - Институт (агенция) за комуникационна сигурност (Communications Security Establishment, CSE):
    - Канадски център за киберсигурност (Canadian Centre for Cyber Security);
  - Министерство на Обществена Безопасност (Public Safety Canada):
    - Център за държавни операции (Government Operations Centre, GOC);
- **Австралия:**
  - Австралийска организация за разузнаване и сигурност (Australian Security Intelligence Organisation, ASIO);
  - Австралийски център за киберсигурност (Australian Cyber Security Center, ACSC);
  - Център за критична инфраструктура (Critical Infrastructure Centre, нов орган от 2018г.), Мрежа за споделяне на информация за защита на критична инфраструктура (Trusted Information Sharing Network for Critical Infrastructure Protection);
- **Великобритания:**
  - Правителство на Великобритания;
    - Център за защита на националната инфраструктура (Centre for the Protection of National Infrastructure, CPNI);
- **Нова Зеландия:**
  - Комисия по инфраструктура (New Zealand Infrastructure commission, INFRACOM). Нов орган създаден на 29 септември 2019 г. [3].

Критичната петорка има за цел да засили сътрудничеството между страните членки за справяне със заплахите за критичната инфраструктура, както и за споделяне на информация, практики и идеи за вътрешния пазар политически и оперативни подходи за защита и устойчивост на критичната инфраструктура. Едно от първите предизвикателства е да се разбере как всяка държава се отнася към критичната инфраструктура, като основа за

[1] https://www.collinsdictionary.com/dictionary/english/anglosphere, 25.09.2020г. Collins English Dictionary. Copyright © HarperCollins Publishers,

ясно формулиране и предаване на общо послание за стойността, значението и значението на критичната инфраструктура. В резултат формирано общо разбиране за критичната инфраструктура.

За да се постигне общо разбиране за критичната инфраструктура, членовете от Критичната петорка анализират дефинициите и изведените сектори в националните инфраструктурни планове за идентифициране на общи и припокриващи признаци, с което да балансира интересите на всяка от държавите. Въпреки, че всяко национално определение за критична инфраструктура предлага своите специфики те съдържа и общи черти, характерни за всяка среда.

Изведеното определение е отправна точка за дискусия за критична, национално значима инфраструктура: **критична инфраструктура, наричана също национално значима инфраструктура, може да бъде широко определена като системи, активи, съоръжения и мрежи, които предоставят основни услуги и са необходими за национална сигурност, икономическа сигурност, просперитет и здраве и безопасност на съответните държави**.

Дефиниция се препоръчва, за да се осигури обща рамка за оформяне международните ангажименти за сигурност на критична инфраструктура

Всяка от държавите подчертава значението на сигурните и устойчиви системи. Следователно е така важно е да се постигне общо определение за устойчивост на критичната инфраструктура. Всяка от страните признава **устойчивостта, като необходимост системите да имат капацитета да бъдат гъвкави и приспособими към променящите се условия – предвидими и неочаквани, с цел бързо възстановяване при прекъсване или смущение**.

Подобно на устойчивостта на критичната инфраструктура, се стига до общо определение за сигурност на критичната инфраструктура. Подразбира се, че **крайната цел на сигурността е да се използва физическа, персонална и/или мерки за киберзащита за намаляване както на риска за критичната инфраструктура, така и на риска от загуба поради прекъсване в основни услуги чрез минимизиране на уязвимостта на критичните инфраструктурни активи, системи и мрежи**.

Обменът на информация е от решаващо значение и устойчивостта и сигурността на критичната инфраструктура и всяка нация се стреми да споделя навременна и подходяща информация в безопасна и надеждна среда, като австралийската мрежа за доверено споделяне на информация (TISN), или осигурените от Обединеното кралство онлайн инструменти за ориентиране и ресурси за собствениците и оператори, чрез защитен уеб сайт. Всеки страната активно се ангажира с изграждането на тези видове надеждни канали за споделяне на информация чрез използва непублични уебсайтове, информационни портали, партньорства или други подходи.

По-долу е направен кратък преглед на общите действия, които петте правителствата предприемат, за да насърчат устойчивост и запазване на сигурността на критичните инфраструктурна:

- Разглеждане на региони и използване на техните аналитични ресурси за идентифициране на национално значими критични инфраструктурни сектори и услугите, които те предоставят.
- Координиране с партньори от публичния и частния сектор за това как да се подобри сигурността и устойчивостта на тази инфраструктура.
- Споделяне на важна и навременна информация със съответните заинтересовани субекти.

- Сътрудничество с партньори и заинтересовани субекти за споделяне и обмен на добри практики.
- Идентифициране на междусекторни зависимости.
- Развитие на човешките ресурси, за справяне със сложните предизвикателства, които оказват влияние върху критична инфраструктура.
- Идентифициране и оценка на критичността на инфраструктурата.
- Използване на подход за управление на риска, който идентифицира начини за намаляване на риска за критичната инфраструктура.

Всички държави идентифицират критични инфраструктурни сектори. За целите на дискусията също е полезно да се види където има общи черти и разлики между идентифицираните критични инфраструктурни сектори. Всяка от петте държава определя следните сектори като критични:

- Комуникации;
- Енергия;
- Здравеопазване и обществено здраве;
- Транспортни системи;
- Вода (да включва системи за отпадъчни води и дъждовни води). [1]

Без съмнение, през 2020 г., здравеопазването се явява секторът, с особена важност в контекста на пандемията от коронавирус. Очаквано в това направление са съсредоточени и част от усилията на петте държави, с несъмнено водещата роля на САЩ, с оглед тежките последици в страната.

Китай умишлено е скрил или унищожил доказателства за избухването на пандемията от коронавируса. Това се казва в документ, изготвен от разузнавателните служби на САЩ, Великобритания, Канада, Австралия и Нова Зеландия, до който е получило достъп австралийското издание The Saturday Telegraph, цитирано от ТВ канала Фокс нюз. Разузнаванията на петте държави са обединени в алианса Five Eyes, от чието име е доклада. Заключението в него е, че укриването на истината от Китай е „нападение срещу международната прозрачност“.

Според доклада на Five Eyes Китай започва да налага цензура на новините за вируса в интернет търсачките и социалните медии от 31 декември, като изтрива термини като „вариация на ТОРС“, „пазар за морски дарове в Ухан“ и „неизвестна пневмония в Ухан“. На 3 януари Националната здравна комисия на Китай разпорежда проби от вируса да бъдат прехвърлени в определени тестови съоръжения, или да бъдат унищожени, като в същото време е издадена „заповед да не се публикуват данни“ за болестта. На 5 януари Общинската здравна комисия в Ухан спира ежедневно да актуализира броя на новозаразените и в продължение на 13 дни няма съобщения за заболелите, се казва още в документа на разузнавателните служби.

До 20 януари китайските власти отричат, че вирусът може да се разпространява между хората, „въпреки доказателствата за предаване от човек на човек от началото на декември“. През февруари „Пекин настоявал САЩ, Италия, Индия, Австралия, съседни страни в Югоизточна Азия и други да не се защитават чрез ограничения за пътуване, дори когато Китай въвел строги рестрикции на своя територия“. Според 5-те разузнавателни служби „милиони хора напускаха Ухан след избухването на заразата и преди властта в Пекин да затвори града на 23 януари“.

В документа на разузнавателния алианс Five Eyes не са спестени и критики към реакцията на Световната здравна организация. Китай и СЗО нееднократно отхвърлят критиките за действията си спрямо коронавируса.

Американското разузнаване засега не потвърждава съществуването на въпросния документ. Високопоставен US служител обаче заявява, че съобщенията за съдържанието на документа съвпада със становището на разузнаването на САЩ, според което Китай е знаел по-рано отколкото обяви, че заразата се предава между хората, както и че властта в Пекин е била наясно, че става въпрос за нов вид коронавирус и че той се разпространява по-широко, отколкото е докладвано на международната общност в първите седмици от избухването на епидемията. [4]

Всяка от петте държави формулира важността на критичната инфраструктура за насърчаване на икономическия просперитет и икономическа сигурност. Правителствата инвестират в критична инфраструктура - независимо дали пряко или чрез партньорства - с цел укрепване на техните икономики и подпомагане на просперитета на техните обществата. Критичната инфраструктура формира гръбнака на съвременното общество, като предоставя основни услуги, които помагат на растежа на бизнеса, като висикоскоростни комуникации, модерни транспортни мрежи и надеждна доставка на енергия, която улеснява търговията и икономическия растеж.[7]

Последното извежда ролята на критичната инфраструктура като национален просперитет. Държавите подчертават, че устойчивата инфраструктура повишава икономическия развитие и предоставя примери за това как всяка държава работи за увеличаване на инвестициите в инфраструктура.

Петте държави-членки, споделят възгледите си в стратегически обзор за връзката между критичната инфраструктура и националния просперитет. Инфраструктурата дава възможност за производителност на националните икономики, качество на живот и икономически прогрес чрез стимулиране на растежа, създаване на работни места и подобряване на производителността, качество на живот и ефективност.

Критична инфраструктура за петте държави, не е геоцентрична и може да надхвърли националните граници, което изисква трансгранично сътрудничество, взаимопомощ и други споразумения за сътрудничество. Световната икономика и доставките в глобален мащаб са все по-важни фактори, с които бизнесът и държавните структури се съобразяват, поради това че функционирането на критичната инфраструктура разчита на материали, произхождащи извън националните граници и въздействат върху националните икономики. Зависимостта от ресурси и суровини извън съответните страни, необходими за производството, движат националната икономика, което налага концентриране върху устойчивостта на глобалните вериги за доставки

Освен това инвестирането в инфраструктура има реално въздействие върху създаването и поддържането на работни места. Оценка от Съвета на икономическите консултанти на американския президент отбелязва, че всеки 1 милиард щатски долара федерално финансирането на магистрали и транзитни инвестиции подпомага 13 000 работни места за една година. Анализ на Годишните данни на Американското бюро за икономически анализ за 2012 г., както и от Американското бюро по трудова статистика (BLS) сочи, че „68% от работните места, създадени чрез инвестиране в инфраструктура, са в строителството, 10 % в производствения сектор и 6 % в търговията на дребно”.

В Канада, като част от Плана за придвижване на Онтарио, стартиран през 2014 г., правителството на Онтарио изчислява, че инвестициите на обща стойност 130 милиарда канадски долара за 10 години в обществена инфраструктура ще подкрепят повече от 110 000 работни места.

Освен това Федерацията на канадските общини формулира, че всеки един милиард канадски долара в инвестиции в инфраструктура се равнява на приблизително 11 000 работни места.

В Австралия, правителството на предостави стимулиращи плащания към държави и територии, които продават активи и реинвестират постъпленията от продажбата за финансиране на инфраструктура в Австралия. Тази инициатива ще привлече близо 40 млрд. долара нови инвестиции в инфраструктура от държавите и териториите в продължение на пет години да повлияят отрицателно на икономическата конкурентоспособност на нацията или региона.

Тъй като инвестицията в инфраструктура е от съществено значение за икономическия растеж, Съединените щати стартираха Инвестиционната инициатива за изграждане на Америка през лятото на 2014 г. Тази инициатива е предназначена да насърчи сътрудничеството, разширяването на пазара за публично-частни партньорства и предоставяне на федерални кредит-програми за по-широка употреба.

Нова Зеландия направи значителни инвестиции в инфраструктура от 2009 г. насам, включително над 12 милиарда новозеландски долара за пътища, 3.2 милиарда новозеландски долари в железопътния транспорт, 2.1 милиарда новозеландски долари за по-бърз широколентов достъп, 5 милиарда новозеландски долара за увеличаване на капацитета, производителността и надеждността на националната мрежа и 16,5 милиарда долара за възстановяването на Крайстчърч след земетресенията. През 2012 г. беше създаден и инвестиционен фонд, който осигури почти 5 милиарда новозеландски долара нов капиталови разходи, включително почти 1 милиард новозеландски долара за транспорт, над 600 милиона новозеландски долара за образование и почти 700 000 за здраве.

Австралия е поела 29,5 милиарда щатски долара 7 за изграждането на национална широколентова мрежа, която ще се подобри ефективността на телекомуникационната инфраструктура на Австралия. Осигуряване на бърза надеждна мрежа ще подкрепи бъдещия икономически и социален растеж на Австралия. Увеличената свързаност ще позволи достъп до нови пазари, намаляване на разходите и стимулиране на иновациите.

Правителствените действия могат да активизират по-широки инфраструктурни инвестиции и по този начин икономическия просперитет. Правителствата могат да създават и насърчават усилията за постигане на национални цели, насочени към повишаване на сигурността и устойчивостта на националната критична инфраструктура, чрез описване на критичните действия партньори от инфраструктурата на Алианса. Това може да служи за насочване на съвместните усилия на в областта за подобряване на резултатите от сигурността и устойчивостта.

Например САЩ стартира Инициативата за изграждане на Америка през юли 2014 г. Целта на инициативата е за Американските федерални агенции да намерят нови начини за увеличаване на инвестициите в пристанища, пътища, мостове, широколентов достъп, питейна вода и канализационни системи и други проекти чрез улесняване на партньорствата между федерални, държавни и местни правителства и инвеститори от частния сектор. Чрез публично-частни партньорства и инвестиции в инфраструктура, САЩ се ангажира да създава работни места, предоставяйки критични услуги на потребителите и бизнеса и защита на общественото здраве и околната среда.

През 2014 г. правителството на Канада се ангажира да инвестира 80 млрд. канадски долара в обществена инфраструктура за десетгодишен период. Това включва план за ново строителство за 53 милиарда канадски долара за провинциална, териториална и общинска инфраструктура. Планът ***New Building Canada*** е най-големият федерален инфраструктурен план в канадската история, който се фокусира върху подпомагане на проекти, които

засилват икономическия растеж, създаването на работни места и производителност. Канадското правителство инвестира приблизително 14,5 милиарда канадски долара за модернизиране на широк спектър от инфраструктура, включително пътища, мостове, обществени и транзит, паркове и съоръжения за пречистване на вода.

В рамките на новата стратегия за устойчивост на критичната инфраструктура в Австралия, стартирана през 2015 г., връзката между критичната инфраструктура и икономиката се определят като основен основополагащ принцип. През май 2014 г. австралийското правителство също е ангажирало допълнителни 11,6 милиарда австралийски долара като част от Стратегия за създаване на пакет за растеж на инфраструктурата, който ще ускори инвестициите в критични инфраструктури в цялата страна.

В Нова Зеландия, правителството признава значението на устойчивата инфраструктура като изключително важен елемент на икономически растеж и има план за действие в рамките на „Изграждане на инфраструктура“ част от Програмата за растеж на бизнеса, за да се гарантира, че националната инфраструктура е устойчива и координирана и допринася за икономически растеж и повишено качество на живот. В Нова Зеландия функционира и Национално звено за инфраструктура, отговорно за координацията между инфраструктурните сектори и формулирането, и наблюдение на напредъка по Националния план за инфраструктура на страната. [4]

Бедствията и промените в глобалната среда за сигурност също насърчиха нациите да разсъждават широко за редица заплахи и опасности, пред които е изправена националната им инфраструктура [6]. Нациите от критичната петорка приемат подход за справяне с настоящите и бъдещите предизвикателства, пред които е изправена тяхната инфраструктура. По-специално, тенденции като изменението на климата и демографските промени вероятно ще се ускорят в бъдеще и оказват влияние върху инфраструктурните системи и активи. В много случаи най-доброто време за справяне с тези тенденции и други потенциални негативни фактори е в процеса на проектиране на инфраструктурните системи и активи. [1]

Анализ на зависимостите и взаимозависимостите на национално и регионално ниво могат да служат за информиране на планирането и улесняване приоритизиране на ресурсите за осигуряване на непрекъснатост и надеждност на критичните услуги и смекчаване на каскадно въздействие на инциденти, които се случват, за подпомагане на стабилно и уверено осигуряване на бизнес и услуги и по този начин на стабилно икономически развитие. [5]

ЛИТЕРАТУРА:

[1] Forging a Common Understanding for Critical Infrastructure, Shared Narrative, March 2014. Издание на Агенция за киберсигурност и сигурност на инфраструктурата (Cybersecurity & Infrastructure Security Agency, CISA) Официален уебсайт на Министерството на вътрешната сигурност на САЩ.

[2] https://www.cisa.gov/international-critical-infrastructure-engagement, 25.09.2020 г. Официален уебсайт на Министерството на вътрешната сигурност на САЩ.

[3] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-prtnrs-en.aspx , 25.09.2020 г. Официален уебсайт на Министерството на обществената безопасност на Канада.

[4] https://www.segabg.com/category-foreign-country/5-zapadni-razuznavaniya-kitay-skri-i-unishtozhi-danni-za-koronavirusa , 01.10.2020 г.

[5] Role of Critical Infrastructure in National Prosperity - Shared Narrative, October 2015. Издание на Агенция за киберсигурност и сигурност на инфраструктурата (Cybersecurity & Infrastructure Security Agency, CISA) Официален уебсайт на Министерството на вътрешната сигурност на САЩ.

[6] Диманова, Д. Защита при бедствия, аварии и катастрофи, УИ ШУ „Еп. К. Преславски“, Шумен, 2016 ISBN 978-619-201-098-0.

[7] Диманова, Д. Роля на държавата при оповестяване на населението при бедствия възникнали в големи технически инфраструктури. Конференция „Комуникационни умения: Анализ и управления на риска“. РУ „Ангел Кънчев“, Русе, ISBN: 978-619-207-097-7, pp. 86-125.
[8] Кузманов, З. Заплахи за критичната инфраструктура в електроенергийния сектор и комуникационните и информационни технологии. Сборник научни трудове, НВУ „В. Левски”, факултет „Артилерия, ПВО и КИС”, Шумен, 2011.
[9] Кузманов, З. Политики на Европейския съюз при управление на кризи. Сборник научни трудове, НВУ „В. Левски”, факултет „Артилерия, ПВО и КИС”, Шумен, 2014.

Име на автор(ите): докторант инж. Константин Илиев Стоянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Управление на системите за сигурност“

STUDY OF SOME ASPECTS OF THE ECONOMIC SECURITY OF ENTERPRISES IN NORTHEASTERN BULGARIA

LACHEZAR T. HRISTOV

ABSTRACT: *In the present work a study is made among business organizations from Northeastern Bulgaria from the districts of Shumen, Targovishte, Razgrad, Silistra and Dobrich. The results of a survey conducted among company executives on the types of information, sites and links between these sites subject to protection are analyzed. Threats to economic security have also been studied, with an emphasis on those objects and sensitive information thus defined. The role of insiders is considered as part of the threats to the security of the company.*

KEYWORDS: *economic security, trade secret, corporate security service, outsourcing, outstaffing, insiders, security service.*

ПРОУЧВАНЕ НА НЯКОИ ОТ АСПЕКТИТЕ НА ИКОНОМИЧЕСКАТА СИГУРНОСТ НА ПРЕДПРИЯТИЯ В СЕВЕРОИЗТОЧНА БЪЛГАРИЯ

ЛЪЧЕЗАР Т. ХРИСТОВ

АБСТРАКТ *В настоящата работата са дадени резултатите от направеното проучване сред бизнес организации от Североизточна България от областите Шумен, Търговище, Разград, Силистра и Добрич. Анализирани са резултатите от проведена анкета сред ръководители на фирми относно видовете информация, обектите и връзките между тези обекти подлежащи на защита. Изследвани са и заплахите за икономическата сигурност, като се набляга на тези спрямо така дефинираните обекти и чувствителна информация. Разгледана е ролята на инсайдерите, като част заплахите за сигурността на фирмата.*

Въведение

Посегателствата срещу икономическата сигурност на бизнес организациите обективно съществуват. [1] При осигуряване на икономическата сигурност на организациите има три основни групи проблеми. Първият проблем е определянето и оценяването на заплахите за икономическата сигурност, настоящото изследване се ограничава до заплахите за чувствителната информация. Вторият аспект е определяне на обектите и връзките между тези обекти, подлежащи на защита. В много литературни източници се разглежда точно този аспект на защита на информационната сигурност [2]. В тях детайлно се описват всички елементи от структурата, комуникациите и материалните ресурси, които подлежат на защита. Всеки от тези обекти обаче е с различен приоритет.

На трето място е необходимо да се определят информационните ресурси, които трябва да бъдат защитавани. Чувствителната корпоративна информация и личните данни са една

от ценностите на днешната икономика, поради което са изложени на повишен риск.

Една от целите на настоящото изследване е да се определи степента на важност (ценността) на всеки от тях, като се отдели особено внимание на информационните и комуникационните ресурси.

1. Чувствителна информация и търговска тайна на бизнес- организациите.

В процесите на изследвания и иновации в стопанските организации се създава информация, която не попада в обхвата на защитата, предоставена от традиционните права на интелектуална собственост като патенти или авторски права. Освен това някои организации може да не смятат за подходящо информацията им да се защитава законите за интелектуална собственост. Независимо от това, тази информация е ценна за бизнес иновациите и конкурентоспособността. Поради това е важно да се запази такава информация като „поверителна“. Информацията, която се пази като поверителна, за да се запазят конкурентните печалби, се нарича „търговска тайна“ [3]. Понякога компаниите пренебрегват търговските тайни като активи, докато в действителност те могат да бъдат по-ценни от всички патенти, търговски марки и авторски права на компанията.

В предишни публикации на автора се използваше термина защитата на чувствителна информация на компаниите [4]. За да се приведе терминологията към приетите сравнително неотдавна нормативни актове, трябва да се подчертае, че вместо термина чувствителна информация трябва да се използва „търговска тайна“ и да не се смесва това понятие с термина „класифицирана информация“, която е предмет на строго нормативно регламентиране.[5] Съгласно [6] търговска тайна е всяка търговска информация, ноу-хау и технологична информация, която отговаря на определени изисквания – тя не е общоизвестна или леснодостъпна за лица от средите, които обичайно използват такъв вид информация, има търговска стойност, поради тайния си характер и по отношение на нея са предприети мерки за запазването и в тайна. Определението в закона е много общо и не дава конкретика за това каква информация се защитава. Търговска тайна е всяка информация, която има икономическа стойност от това, че не е широко известна на обществеността и която е обект на разумни усилия за запазване на нейната тайна. Търговските тайни могат да включват формули, методи, рецепти, програми, техники, процеси, списъци с клиенти, изисквания на клиента, спецификации на продукти и ценови стратегии.[7]

Повечето малки и средни предприятия не знаят, че трябва да включват клаузи за закрила на търговските си тайни при сключването на договори. [8] Такива клаузи трябва да има при сключване на трудови договори със служителите си и при договори за партньорство с други компании. В противен случай съществува риск от разкриване на търговската тайна. Освен това, много фирми често пренебрегват включването на необходимите клаузи за конфиденциалност в договорните споразумения с партньорите си. Може да се претендира за нарушение на търговските тайни, само ако е налице някакво фактическо доказателство, че са били предприели действия за защита на уникалната бизнес информация. За да бъде защитена уникалната бизнес информация, се налага използването на други видове права върху интелектуална собственост (авторско право, индустриални права). Тези права върху интелектуална собственост са много по-сериозни и осигуряват по-солидна закрила. Бизнес и академичните среди понякога използват други имена, като например „патентовано ноу-хау“ или „патентована технология “, за да се позоват на информация за търговската тайна.[3,9]

Това понятие не покриват с тези, които собствениците и ръководният персонал на фирмите определят като чувствителна за икономическата им сигурност.

2. Цели и резултати на изследването.

С цел оценка на нагласите и подготвеността на ръководителите на бизнес организациите в Североизточна България бе направено изследване сред бизнес организации от Североизточна България от областите Шумен, Търговище, Разград, Силистра и Добрич. То се основава на анализ на регионалните практики, както и на емпиричен подход. Това изследване представя емпиричното разбиране на нагласите на работодателите.

Работодателите са подбрани така, че да има равно представителство на фирмите, които имат известен опит в работата и тези, които се интересуват от проблема. Проучването се състои от лични интервюта и анкета за събиране на отзиви и мнения относно констатациите от интервютата и препоръките за политики, разработени въз основа на тези констатации .

Изготвената анкета [10] бе разпространена сред 75 фирми с различен обхват на дейността и различна категория, според броя на персонала. От тях 55% са с персонал над 250 човека (големи), около 30% са с персонал между 50 и 250 човека (средни) и 15% са с персонал до 50 човека (малки и микро). Подбрани са повече представители на големите и средните предприятия, тъй като при тези категории фирми има възможност да бъде изграден собствен отдел по сигурност. Това от своя страна позволява да се прецени по обективно разликата между използването на такъв собствен отдел и използването на външни услуги като аутсорсинг и аутстафинг от гледна точка на сигурността на икономическата информация. 30% от анкетираните представляват фирми заети в производствената сфера, 24% в търговията, 20% в транспорт, логистика и други, както и 16% са фирми работещи в сферата на услугите [10].

За целта на настоящото изследване към така изготвената анкета бяха добавени три допълнителни въпроса. Тези въпроси имат за цел да оценят, както ценността на икономическата информация в анкетираната фирма, така и заплахите насочени към тази информация – външни и вътрешни. В анкетирането взеха участие пряко ангажираните в планирането и ръководството, а именно управители на фирми и предприятия извършващи дейност в североизточна България, собственици на такива фирми и ръководители осъществяващи друга управленска дейност.

За целите на настоящото изследване бе необходимо да се проучат два основни проблема.

Първият от тях е свързан с фирмената информация, която се създава, обработва, съхранява и предава, както в рамките на самата организация, така и извън нея. Ежедневно във фирмите се създава голямо количество информация, но само част от нея представлява обект на изследване, тъй като е свързана с икономическата дейност на фирмата. Поради тази причина във въпроса от анкетата бе специфицирано какъв тип информация ще се оценява от анкетираните, като чувствителна за фирмата. Дефинирани бяха шест вида информация, която се определя като чувствителна за фирмата (в смисъл на търговска тайна на бизнес- организацията):

- Финансова информация – (бюджет, разходи, печалба и други);
- Информация, свързана с производствени процеси
- Информация, свързана с пазарите
- Информационна и мрежова сигурност
- Информация, свързана с административни дейности (бр. персонал, раб. заплата и др.)

- Организация на сигурността на фирмата.

Останалите информационни потоци са маловажни за финансовата сигурност и не представляват интерес от гледна точка на настоящото изследване. Според представителите на фирмите всеки от посочените по-горе видове информация е с различна степен на важност. За да се определи тази степен на важност за конкретния анкетиран бе предложена скала на ценност със стойности от едно до пет. Съответно стойност пет показва най-високо ниво на ценност, а стойност едно най-ниска.

От посочените отговори като първи бе посочена финансовата информация, като бюджет, разходи, печалба и други, дали се оценява като чувствителна, се вижда (Фигура 1), че повечето анкетирани считат, че тя е от съществена ценност. Дванадесет от анкетираните посочват най-висока ценност (стойност 5) на този тип информация, седем са посочили стойност 4, а единадесет – 3. Това означава, че по-голямата част от анкетираните оценяват този тип информация като особено важна за фирмената икономическа сигурност.

На Фиг. 1 е показано, че информацията свързана с производствените процеси се определя от ръководителите с относително ниска степен на важност и чувствителност спрямо заплахи, като с най-високи стойности е дадена оценка 4 от 16 от анкетираните ръководители.

Фигура 1. Оценка за ценността на фирмената информация

Информацията свързана с пазарите е определена от ръководителите със средна стойност на чувствителност за фирмата с 18 представените отговори и с оценка 3, а с дадена оценка 5 с висока степен на чувствителност са посочили 12 от анкетираните ръководители.

Вторият проблем е познаване нивото на заплаха спрямо конфиденциалността на икономическата информация във фирмата. За да се проучи този проблем в настоящата анкета са включени два въпроса, които оценяват наличието и нивото на заплахите (външни и вътрешни) спрямо чувствителната фирмена информация, определена в по горния въпрос. В първият от тези въпроси се прави оценка на нивото на заплахи спрямо посочения тип чувствителна информация, но са добавени и някои допълнителни обекти подлежащи на заплаха. Подобно на предния въпрос бяха дефинирани основните обекти спрямо, които могат да възникнат заплахи от един или друг вид. Два от обектите определят именно чувствителната информация посочена в предния въпрос – Фирмено ноу хау и Друга чувствителна информация. Другите два обекта бяха добавени като особено важни от гледна точка на сигурността – Персонал и Материални активи.

За да се определи степента на възможните заплахи, с която конкретният анкетиран определя всеки един от тези четири обекта бе предложена скала на ценност със стойности от едно до пет. Съответно стойност пет показва най-високо ниво на заплаха, а стойност едно най-ниска.

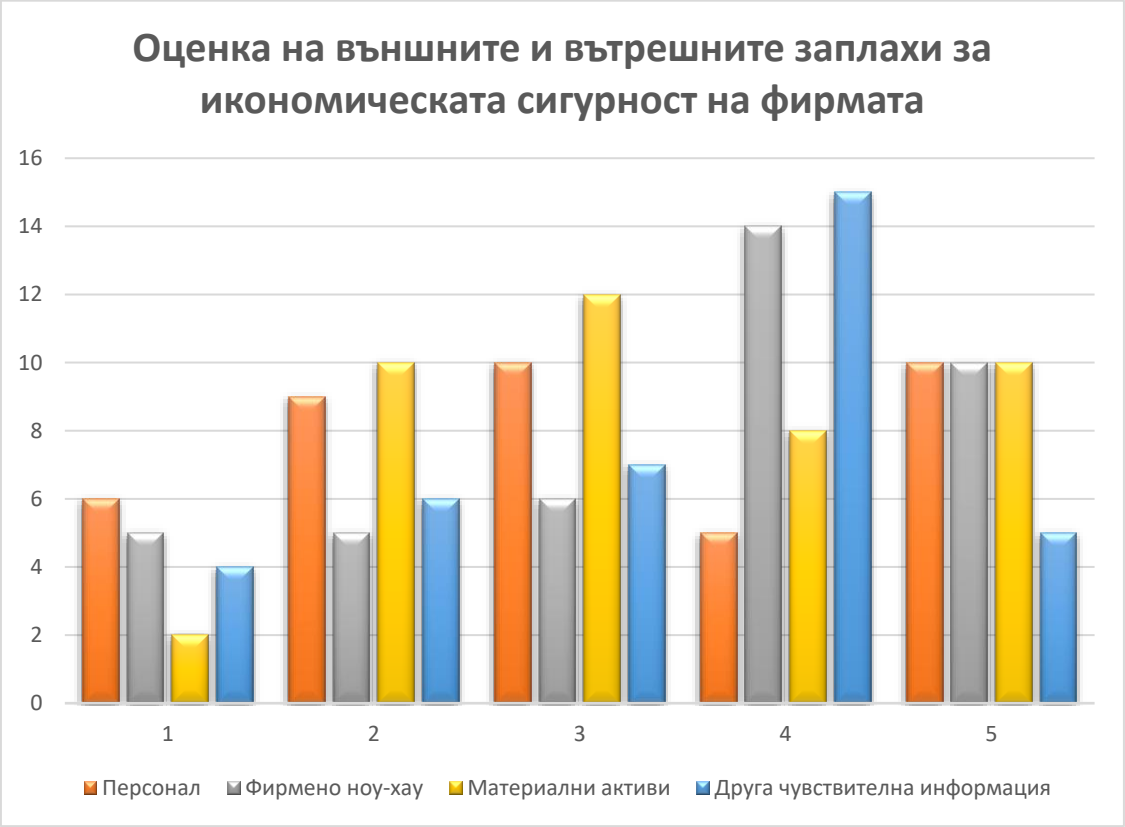
Другият въпрос свързан с оценка на заплахите спрямо чувствителната фирмена информация цели основно да определи възможностите за вътрешни заплахи за тази информация. Служителите на фирмата могат да предизвикат основно от два типа заплахи – преднамерени и непреднамерени [11]. Преднамерените заплахи за сигурността се предизвикват от така наречените „инсайдери“. Това са служители на фирмата, добре запознати с важна чувствителната информация, но недоволни от своето положение в предприятието и потенциални сътрудници на конкурентна фирма. Наличието на такъв тип служители би компрометирало икономическата сигурност на фирмата и дори нейното бъдеще. В [12] са разгледани заплахите от вътрешни зложелатели и тяхното значение за икономическата сигурност на организациите.

От посочените отговори по отношение на това как ръководителите оценяват информационната и мрежова сигурност, изключително голям брой от анкетираните 21, посочват, че тя е с най-висока степен на чувствителност, като същевременно и относителния й дял се нарежда на водещо място в общата оценка на чувствителната информация за стопанската организация.

Анкетираните посочват със средно и ниско ниво на важност и заплаха с 21 от анкетираните, спрямо относителен дял на чувствителност на информацията свързана с административните дейности на фирмата, като работна заплата, брой на персонала и други.

От посочените отговори на това как ръководителите оценяват организацията на сигурността на фирмата, с най-голям голям брой от анкетираните 13, посочват, че тя е с най-висока степен на чувствителност и с най-висок относителен дял, като по този начин се нарежда на водещо място в общата оценка на чувствителната информация за стопанската организация.

От посочените отговори може да се направи обоснован извод, че за ръководителите на фирмите от най-голямо и съществено значение за функционирането им като стопанска организация, се определят информацията като чувствителна по отношение на организацията на сигурността на фирмата и информационната и мрежова сигурност на фирмите извършващи търговска и производствена дейност в североизточна България.



Фигура 2. Оценка за обектите на вътрешни и външни заплахи

В другия от допълнителните въпроси от анкетата бе оценено от анкетираните нивото на заплаха спрямо основните обекти за защита във фирмата. Като първи обект за оценка бе посочен персоналът. Както се вижда на Фигура 2 половината анкетирани считат, че заплахата спрямо персонала варира от средна до висока. Около 25% определят стойност 3, 10% -стойност 4 и 25% - стойност 5. Това означава, че трябва да се обърне сериозно внимание на персонала, като важен за фирмената икономическа сигурност обект.

На Фиг. 2 е показано, че фирменото ноу-хау се определя от ръководителите с най-висока степен на важност и чувствителност спрямо заплахи, като с най-високи стойности са дадени оценка 4 – 35% и оценка 5 – 25% от анкетираните ръководители. Това означава, че 60% от анкетираните смятат за най-застрашен обект спрямо външни и вътрешни заплахи фирменото ноу-хау.

Подобно на персонала материалните активи се определят от ръководителите със средна до висока стойност на заплаха. С 25% от анкетираните определят стойност 2, 35 определят стойност 3, 20% - стойност 4 и 25% - стойност 5. Това означава, че материалните активи също са важен обект подлежащ на външни и вътрешни заплахи.

Логично, посочената като чувствителна в предходния въпрос информация, е определена от близо 70 % от анкетирания ръководен персонал определят този обект като най-застрашен от външни и вътрешни заплахи. С 18% от анкетирани определят стойност 3, 38% определят стойност 4 и 12% - стойност 5.

От посочените отговори може да се направи обоснован извод, че ръководителите на фирмите от североизточна България определят като високо нивото на заплахите (външни и вътрешни) спрямо всички обекти свързани с търговската и производствена дейност на тяхната фирма.

Както се вижда от посочените в предходните два въпроса резултати, чувствителната информация и обектите свързани с нея са определени от анкетираните, като сериозно застрашени от външни и вътрешни заплахи. За да се определи нивото на заплаха от вътрешни източници и по този начин да се определят и външните заплахи, е добавен въпрос свързан с оценка за наличието на нелоялни към фирмата служители (инсайдъри).

Фигура 3. Оценка за наличие на вътрешни заплахи

От посочените отговори по отношение на наличието на инсайдъри, от представените отговори се вижда, че около 56% от анкетираните са уверени, че имат такива в своята организация. Около 24% от анкетираните предполагат или са неуверени, че сред техните служители има такива с нелоялно и користно поведение спрямо организацията, в която работят. Около 10% заявяват, че не знаят дали имат, а други 10% са уверени, че нямат такива служители. Прави впечатление, че по-голямата част от ръководителите и собствениците на големите стопански субекти са убедени или почти сигурни, че сред служителите им има такива с нелоялно поведение спрямо фирмата им. От направеното изследване става ясно, че когато предприятието спада към малките, средни или микро икономически организации, се наблюдава значителен спад на увереността на нейните ръководители и собственици, че се извършват злоупотреби от служителите или че тяхното поведение е нелоялно. Увереността, че по малкия брой служители създава усещането, за контрол на процесите във фирмата, всъщност могат да дадат невярна информация за действителното състояние във фирмата. Основно може да се посочи, че почти всички анкетирани организации изпитват основателни притеснения от дейност на свои нелоялни служители, които могат да навредят сериозно на предприятието, в което работят. Посочените резултати са представени на Фиг. 3

Заключение

Поради широкообхватността на дефиницията за търговска тайна, с настоящото изследване бяха определени видовете информация, които според анкетираните влизат в състава на чувствителната информация т.е. представляват търговска тайна. Според

ръководителите на бизнес – организации в Североизточна България, като най-важна подлежаща на защита търговска тайна е финансовата информация- бюджет, разходи, печалба. Най-голямо и съществено значение за функционирането им като стопанска организация, се определя организацията на сигурността на фирмата и информационната и мрежова сигурност на организациите, извършващи търговска и производствена дейност.

По отношение на обекти подлежащите на външни и вътрешни заплахи, анкетираните отбелязват, че трябва да се обърне сериозно внимание на персонала, като важен за фирмената икономическа сигурност обект. Заплахите от вътрешни източници (инсайдери) са определени като едни от водещите за икономическата сигурност на фирмата. Над 56% от анкетираните посочват наличието на инсайдери в тяхната организация. От това следва, че защитата от тях е от първостепенна важност за по-голямата част от фирмите в региона.

След като са ясно дефинирани търговската тайна, обектите на заплахи и източниците на тези заплахи, може да бъде изградена стратегия за осигуряване на икономическа сигурност на фирмата. Двата основни подхода при изграждането на такава стратегия са – използване на собствена служба за сигурност и/или използване на външни аутсорсинг и аутстафинг услуги. Когато става дума за заплахи към чувствителната информацията породени от инсайдери, практически по разумния подход е делегирането на права за защита на чувствителната информация на външни контрагенти. По този начин се елиминира вероятността неформалните отношения между служителите във фирмата да попречат на ефективността на защитата на икономическата сигурност.

Като резултат може да се обобщи, че използването на аутсорсингови и аутстафингови услуги остава най-доброто решение за осигуряване на икономическа сигурност на малките и средни бизнес-организации. Естествено важно е да се отбележи, че подборът на фирма, която предоставя такъв тип услуги е важен и сигурността на организацията не бива да се оставя в ръцете на неопитни и неутвърдени професионалисти в областта т.е. трябва да се подбират фирми доказали се в сферата на сигурността.

ЛИТЕРАТУРА:

1. 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.

2. Христов, Х., Сигурност на фирмата и противодействие на посегателства срещу нея, Университетско издателство "Епископ Константин Преславски" Шумен, ISBN 978-954-577-981-7, гр. Шумен, 2014 г., 328 с. Монография.

3. Fact Sheet Trade secrets: An efficient tool for competitiveness. European IPR Helpdesk. June 2017.

4. Христов,Л.,С.Станев и Х.Христов. Средства за защита на чувствителната информация на фирмата от вътрешни зложелатели (инсайдери). MATTEX18.

5. Закон за защита на класифицираната информация https://www.lex.bg/laws/ldoc/2135448577

6.Закон за защита на търговската тайна https://lex.bg/bg/laws/ldoc/2137192307.

7. https://www.lgt-law.com/intellectual-property-overview/trade-secrets/trade-secret-faqs/ TRADE SECRET FAQS.

8. Бизнесът не сключва клаузи за закрила на търговските си тайни. ИАНМСП.https://www.sme.government.bg/?p=38359.

9. Powel, J. The Most Important Secret Of A Prosperous Economy https://www.forbes.com/sites/jimpowell/2012/01/16/the-most-important-secret-of-a-prosperous-economy/#31abe67d6556.

10. Hristov, L., (2020), Study on the applicability of outsourcing and outstaffing in the economic security systems of business organizations in northeast Bulgaria, SocioBrains, ISSUE 67, pp. 199-207, ISSN 2367-5721.

11. Станев,С. и С.Железов. Компютърна и мрежова сигурност. Изд. на ШУ, 2005?

12. Христов, Л., Станев, С., Христов, Х., Средства за защита на чувствителната информация на фирмата от вътрешни зложелатели (инсайдери). Научна конференция с международно участие „МАТТЕХ“ , ШУ „Еп. К. Преславски“ 25-27 октомври 2018г.;

Име на автора: Лъчезар Тодоров Христов
Месторабота: Областна дирекция на МВР гр. Шумен
E-mail: luchano@abv.bg

EUROPEAN UNION INTELLIGENCE AGENCY – THE NEED FOR A SINGLE INTELLIGENCE INSTITUTION FOR THE EUROPEAN COMMUNITY

DONCHO H. TILEV

ABSTRACT: *EU cooperation in the field of intelligence is the most important weapon in the fight against radicalization, as well as in the fight against new threats, such as illegal immigration, human trafficking, drug smuggling in the 28 member states of the European Union. The report focuses on the reasons for the European Union to set up a European intelligence agency, which is a necessary institution for the European army. Effective intelligence cooperation is difficult to achieve even at the national level, as different agency competes for resources and attention from decision-makers. The terrorist incid,ents in Europe serve as a basis for the European Commission to promote the sharing of apprehensive information and cooperation between the institutions of the European Union and the Member States.*

KEYWORDS: *European Union Intelligence Agency, EU Intelligence and Situation Centre (EU INTCEN), Single European Act (SEA), NATO Situation Centre (SITCEN)), European External Action Service (EEAS).*

АГЕНЦИЯ ЗА РАЗУЗНАВАНЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ – НЕОБХОДИМОСТТА ОТ ЕДИННА РАЗУЗНАВАТЕЛНА ИНСТИТУЦИЯ ЗА ЕВРОПЕЙСКАТА ОБЩНОСТ

ДОНЧО Х. ТИЛЕВ

АБСТРАКТ: *Сътрудничеството на страните членки на европейския съюз в областта на разузнаването е най-важното оръжие в борбата с радикализацията, както и в борбата с новите заплахи, като нелегална имиграция, трафик на хора, контрабанда на наркотици в 28-те държави-членки на Европейския съюз. Доклада се фокусира върху причините, които карат Европейския съюз да предприеме създаването на Европейска разузнавателна агенция, която е необходима институция за Европейската армия. Ефикасно сътрудничество в разузнаването е трудно да се постигне дори на национално ниво, тъй като различните служби се конкурират за ресурси и внимание от страна на лицата, вземащи решения. Осъществените терористични инциденти в Европа служат като основание на Европейската комисия да насърчи споделянето на чувствителна информация и сътрудничеството между Институциите на Европейския съюз и държавите-членки.*

Краят на Студената война преди повече от три десетилетия създаде свят, в който относителната стабилност между двете супер сили е изчерпана. По време на студената война действията на всяка държава се проектира в светлината на противопоставянето между двете велики сили - Съединените щати и Съветския съюз. Промяната в политическите управления, които се случиха в Централна и Източна Европа неизбежно промениха облика на международните връзки в Европа и в Западния свят като цяло, а гражданската война в Югославия беше първият случай на етнически конфликт в Европа след Студената война. Общият анализ на военните действия на НАТО на територията на бившата СФРЮ показа силната зависимост на Европа от военния и разузнавателен потенциал на САЩ, както и забавянето на ЕС в развитието на сателитните комуникации,

разузнавателната информация и космическото наблюдение. Ясно се очерта тенденцията САЩ да не споделят редовно разузнавателна информация със своите европейски партньори или да го правят избирателно и по конюнктурни съображения. Това усили раздразнението сред водещите европейски държави, заставяйки ги сериозно да се замислят, доколко имат възможност да извършват самостоятелен анализ и оценка въз основа на собствена разузнавателна информация. [4]

Ерата след 11 септември 2011 г. поставя предизвикателството пред правителствата, политиците, религиозните лидери, медиите и обществото да играят критични и конструктивни роли във войната срещу тероризма. Разделителната линия между националната и международната сигурност е силно размита, с оглед на факта, че заплахата сега не е строго национална, а по-скоро транс – национална. Това категорично налага ново отношение и нова трактовка на целта, съдържанието и функционирането на разузнавателната дейност. Процесът трябва да бъде основан на съвместно партньорство, което да се базира на споделените убеждения, ценности и интереси; по-конструктивно да се подхожда към различията и противоречията в общността; да се изгражда бъдеще, основаващо се на признанието, че всички са изправени пред общ враг - тероризма, който може да бъде ефективно задържан и елиминиран само чрез признаване на взаимните интереси и използването на многостранни съюзи, стратегии и действия.

Докато разузнавателната общност върви по пътя си към двадесет и първи век, тя е изправена пред безпрецедентен набор от предизвикателства - хаотична световна среда от епохата след Студената война с активирането на Ислямска държава в Сирия и Ирак, Арабска пролет, Либия, Украйна, икономически сътресения в Еврозоната, транснационални мрежи за организирана престъпност и Иранската ядрената програма. Всичко това предлага широк кръг от различни въпроси, по които трябва да се разберат страните от ЕС. Именно в този контекст са посочени причините подчертаващи необходимостта от създаването на Разузнавателна агенция на Европейския съюз, като необходима институция за Европейска армия. Мястото на Разузнавателна агенция на Европейския съюз е в рамките на Европейските институции и още веднъж се подчертава ролята на Центъра за анализ на разузнаването (INTCEN) към Европейския съюз - потенциална независима оперативна агенция в механизма на Европейския съюз.

Разузнавателната агенция на Европейският съюз като цяло става все по- важен фактор на континента след възраждането на Европейската общност осъществено чрез Единния Европейски акт (SEA), подписан през 1986 г. Единният европейски акт е официалното име на програмата от 1992 г. за отваряне на граници между държавите-членки на Европейския съюз.

От друга страна нестабилността в Близкия изток, северноафрикански регион и Турция, както и в някой държави от бившия Съветски съюз оказват влияние върху развитието на страните - членки на Европейския съюз особено на Балканите и Средиземноморския регион. Ислямския фундаментализмът се повява отново в страните от Близкия Изток и Северна Африка, заедно с увеличаване на радикализацията. Южноевропейските държави-членки на Съюза като Гърция, Италия, Испания и Португалия са изправени пред големи проблеми заради нелегалната имиграция.

Това дава основание на Министрите на вътрешните работи и правосъдието на страните от Европейския съюз да се споразумеят за по-тясно сътрудничество по някои проблеми свързани със сигурността и да вземат решение за назначаване на Координатор по антитероризъм. През 2007 г. на поста е назначен Жил де Керков. Той се ръководи от трите приоритета на ЕС за борба с тероризма, приети през февруари 2015 г., а именно:

гарантиране на сигурността на гражданите;

предотвратяване на радикализацията и защита на ценностите;

сътрудничество с международните партньори.

Координаторът за борбата с тероризма има за задача: да координира работата на Съвета за борбата с тероризма;

да представя на Съвета препоръки за политиката и предлага приоритетни области за действие;

да наблюдава изпълнението на стратегията на ЕС за борба с тероризма;

да прави редовен преглед на всички инструменти на ЕС, като се отчита пред Съвета и предприема последващи действия по решенията на Съвета;

да се координира със съответните подготвителни органи на Съвета, Комисията и ЕСВД;

да предприема необходимото за гарантиране на активната роля на ЕС в борбата с тероризма;

да полага грижи за подобряването на комуникацията между ЕС и трети държави.[5]

Важен момент от споразумението е създаване на клирингова къща, където на първо време разследването провеждано от съдии, полиция и разузнавателните служби могат да насочват събраната информация , която би станала достъпна в реално време за всички членове. Вместо предложението на Белгия и Австрия за установяване на европейска агенция за разузнаване с цел борба с тероризма, Министри на вътрешните работи от пет европейски страни - Обединено кралство, Германия, Франция, Испания и Италия – не желаят да се споразумеят как да споделят информацията придобита от тяхното разузнаване с останалите държави-членки на Съюза и трети страни. Въпреки нежеланието си на 26 февруари 2020 г. Великобритания става един от учредителите на Intelligence College of Europe – разузнавателна колегия за обмен на информация. Оказва се на практика, че Обединеното кралство не желае да споделя информация, но с готовност ще ползва такава. Както казва ген. Съби Събев в интервю пред Фокус „Разузнавателните служби са много чувствителни към независимостта, която имат".[1]

Необходимо е да се очертае мястото на Разузнавателна агенция в рамките на Европейския съюз. Механизмът за сътрудничество на Европейският съюз е уникален и поради факта, че той дефинира съществуването на единна международна европейска организация, която може да се счита за наднационална и политически независима система за взаимопомощ, включително по въпросите на отбраната и сигурността на страните – членки при зачитането на националния суверенитет на всеки от субектите. Както отбелязва специалиста в областта на контраразузнаването Христо Христов „Съвременната среда за сигурност се характеризира с динамични промени и задачите на службите за контраразузнаване са не само на национално ниво , но и трябва да съответстват на общата контраразузнавателна политика, регламентирана от съответните документи на НАТО за контраразузнаване." [2]

Основен момент в съвместните действия е определянето на граници, до които се простират съюзническите интереси и необходимостта от опазване на националните интереси и суверенитет. Независимо от належащата нужда от разузнавателно кооперирание, политическите лидери все още не са склонни да намалят на държавно ниво контрола върху националните разузнавателни служби. В момента различията във външната политика и отбраната, както и националният суверенитет ограничават изграждането на наднационална разузнавателна институция.

С други думи, трябва да се търси компромиса в различията и постигането на общите цели. Желанието на държавите-членки на Европейския съюз да работят в тясно сътрудничество не е често наблюдавано в други международни организации. Три основни

институции в Европейския съюз са важни за формирането и функционирането на европейската Съюзна разузнавателна агенция.

а) Европейският съвет е орган който принципно определя решенията взети от Европейския съюз. Съставен е от Министри на 28-те европейски Държави-членки на Съюза за всяко направление, като външните работи, например.

б) Европейската комисия е отговорна за формулирането на специфичните политики на Европейският съюз, а неговите препоръки в крайна сметка се определят от Европейският съвет. "

в) Европейският парламент - е съставен от представители на страните членки на Европейския съюз .

Резонен е въпроса - Как разузнавателната агенция на Европейския съюз се вписва в европейския Механизъм на Съюза? Механизма на Европейският Съюз е критикуван поради липсата на яснота на вземане на решенията и разработване на прилаганите политики. По този начин липсата на прозрачност може да направи по-трудно определянето на позицията на разузнаването на Европейския съюз.

Европейската агенция за разузнаване би трябвало да бъде независима институция. Това би помогнало да се гарантира, че ще провежда събирането на информация и анализ на данните по възможно най-обективен начин. Тя трябва да е отговорна пряко пред ръководството на Европейския парламент. Комисарят на Европейския съюз отговарящ за външните работи, също трябва да бъде информиран от директора на Агенцията за разузнаване на Европейския съюз ежедневно.

Европейската комисия е постоянен орган и се очаква членовете и да представляват Европейския съюз, а не собствените си страни. Разузнаването трябва да докладва относно сигурността за важни за Европа въпроси на Европейската комисия редовно. Освен това, когато разузнавателна агенция предвижда ситуация, която би могла да бъде заплашителна за Европейския съюз, като Сирийската или Либийската криза например, тогава е добре Съветът на Министрите да бъде включен в обсъждането. Може би Съвета на министрите, като официален представител на Европейския съюз и орган за вземане на решения, също трябва редовно да получава отчети и анализи от европейската разузнавателна агенция. Но проблемът е, че например, министър на външните работи от съвета на министрите на ЕС, може да има трудности или конфликти във външните работи на своята собствена страна и тези на Европейски съюз едновременно.

Това се явява друга причина способстваща да се пропусне ежедневния контрол на Агенция за Разузнаване на Европейския съюз към Европейската комисия. Съветът би трябвало да взема решения за Европейския съюз. Дейността на разузнавателната агенция трябва да се отнася за въпроси, които имат голямо значение за Европейският съюз, но Европейският парламент ще бъде този, който трябва да одобри бюджета на европейската агенция за разузнаване.

Европейският парламент може да стане и институцията за осигуряване на надзор над Разузнаването на Европейския съюз и по-специално операциите на Агенцията. Парламентът също може да участва при определяне на въпросите, които трябва да бъдат обект на наблюдение от Агенцията за Разузнаването на Европейския съюз.

След като Европейският съюз вземе решение да имат европейска армия ще възникне въпроса относно връзката между организацията за защита (НАТО) и Разузнавателна агенция на Европейския съюз. Най-вероятно Европейската комисията ще назначи Комисар, който да отговаря за Отбраната. Съюзната агенция за разузнаване ще трябва да докладва и на него. В САЩ военните имат свои собствени разузнавателни агенции. Ето защо е вярно предположението, че Европейската армия също ще има свое собствено разузнаване. Една

от причините да има собствено разузнаване е, че военните изискват различна, специфична, разузнавателна информация. Европейската Разузнавателната агенция ще координира стратегическо разузнаване, включително и това на военните. В дългосрочен план, Агенцията за разузнаване на Европейския съюз трябва да има капацитета да наема и обучава собствен персонал за процеса на цялостното събиране на информация. Тя не трябва да се превръща в Агенция, която наема само офицери за разузнаване от държавите-членки на Европейския съюз. Трябва да се провежда политика която да направи Агенцията за разузнаване на европейския съюз, истинска европейска агенция.

От Обединен ситуационен център (SITCEN) към Европейски разузнавателен център (INTCEN) и Европейска Разузнавателна агенция (EUIA) .

Центъра за разузнаване на Европейския съюз (INTCEN) се присъедини към европейската Служба за външни действия през 2010 г., но има далеч по-дълга история. Произходът му е от „работеща структура изключително на отворен код на разузнаване (OSINT) ", на подчинение в Западноевропейски съюз (ЗЕС), междуправителствен военен съюз, който официално се разпусна през юни 2011 г. След разпускането на ЗЕС, неговата функция постепенно се прехвърли през последното десетилетие на Обща политика за сигурност и отбрана. Общата политика за сигурност и отбрана (ОПСО) определя рамките, уреждащи политическите и военните структури на ЕС и военните и гражданските мисии и операции в чужбина.

През 2012 г. Европейският Център за разузнаване (INTCEN) като предшестваща организация създадена като дирекция на Генералния секретариат на Европейския Съвет, даде името на Съвместен ситуационен Център на Европейския съюз (SITCEN). Персонала е набран от седем държави-членки на Европейския съюз - Франция, Германия, Италия, Холандия, Испания, Швеция и Великобритания, които са командировани в центъра за разузнавателни услуги и започват да обменят разузнавателна информация и извършват анализи за нуждите на центъра.

През 2007 г. Европейския ситуационния център за анализ на ситуации извън европейското пространство е преустроен в Единния център за анализ на разузнаването (SIAC), който обединява гражданско разузнаване, с разузнавателната информация получена от разузнавателното отделение на военния щаб на Европейския съюз.

Единния център за анализ на разузнаването осъществява „Въвеждане на информация за ранно предупреждение и оценка на ситуацията ", както и „Подпомагане на разузнаването при реакция на кризи, планиране и оценка на оперативни действия."

Военният щаб на Европейския съюз е преместен в европейската Служба за външни действия (ЕСВД) през 2010 г. едновременно с европейския ситуационен център на Съюза, въпреки че самите институции не са се слели. През 2010 г. Европейският Центърът за разузнаване става част от Европейската служба за външна дейност. Дейността е разширена за покриване вътрешни и външни заплахи и позволява събиране (главно от отворени източници –OSINT), обработка, анализ и споделяне на поверителна информация. Директорът на Центъра за разузнаване на Европейския съюз, Илка Салми посочва: „Мисията на Европейския Съюзен разузнавателен център е да предоставя анализи на разузнаването, ранно предупреждение и ситуативно осъществяване, както и вземане на различни решения от Общата Външна Сигурност и политика на сигурност(ОВППС), Общата Политика за Сигурност и Отбрана (ОПСО) и противодействие на тероризмът към държави-членки на Европейския съюз."[6]

Необходимо е Европейския съюз да трансформира Центъра за разузнаване на Европейския съюз в независима Европейска Разузнавателна агенция, защото международният ред се променя драматично през последните десетилетия и света е е станал

по-стабилен. Източната и южната периферия на Европа (предимно Украйна, Сирия и Либия) са региони със значителна нестабилност. Следователно Европейският съюз трябва да станете по-активен на международната арена. Липсата на знания за реалния потенциал на конфликтите в региона могат да бъдат по - скъпи от поддържането на жизнеспособна Европейска разузнавателна структура.

Основни задачи на Европейската Агенцията за разузнаване е да събира информация от членовете на Европейския съюз - държавните разузнавателни организации и да я анализира обективно и независимо. Тогава анализът ще позволи на Агенцията да изготви предложения за Европейската комисия и Съветът по отношения на проблеми със сигурността, които да бъдат адекватни с проблематиката. Повечето от информацията, необходима за задълбочен анализ може да бъде събрана явно. В случай на липса на разузнаване и наличие на жизненоважна необходимост Агенцията може да прибягва до скрито събиране на информация. Разузнавателна агенция на Европейския съюз може да стане много полезна институция за Европейския съюз, политиците и лицата, вземащи решения, както и в областта на военното дело, когато Европейският съюз създаде Европейска армия.

В наши дни сирийците, Украйна и Либийските кризи са достатъчно травматизиращ пример за предаване на съобщението, че ако Европейският съюз е решен да постигне целта за обща външна и отбранителна политика, изискването за обща Разузнавателната политика на Европейския съюз е неотложно.

Разузнавателното сътрудничество е най - важното оръжие в битката за преодоляване на новите заплахи - трафик на хора, нелегална имиграция, транснационална организирана престъпност, разпространяването на джихадистки мрежи и радикализация в страните - членки на Съюза и неговата значимост е дори по-голяма. Международното внимание е привлечено от терористичните атаки, икономическата нестабилност и социалните размирици, щрихи които рисуват критичната картина на имигрантската криза в Европа. Милиони отделни потоци мигранти в Гърция, Италия и Испания, използващи морския път независимо дали като бежанци от конфликт или нелегални имигранти, силно напрягат европейския институционален капацитет и търпението на хората. Докато политици се упражняват в реторика около терористичните заспали клетки, инфилтриращи се в бежански движения, вниманието бе силно фокусирано в дните около атентатите в Париж (13 ноември 2015) и Брюксел (22 март 2016). Изказаха се опасения относно сигурността на средиземноморския район за доставки на стоки и храни – поради популярността на морския път сред трафикантите на хора.

Концепцията на израза „световен ред“ не трябва да разглежда само международните отношения, като борбата за власт между конкурентни партии или последиците за международната система от разпределение на властта между държавите, а по-скоро, както казва Хедли Бул: „като връзка между ред и анархия в по фундаментален смисъл. " [7]

Това означава, че международните отношения трябва да бъдат разглеждани от гледната точка на ценностите, като се разглежда тълкуването на морал, свобода, справедливост, цивилизация и индивидуалност в разбиране на връзката между закон и власт както на национално, така и на международно ниво. В този контекст ефективно разузнавателно сътрудничество е трудно постижимо дори на национално ниво, тъй като различните разузнавателните служби се състезават за ресурси и внимание от страна на вземащите решения.

Миналите терористични инциденти в Европа (Мадрид, 2004 г., Лондон, 2005, Осло, 2011, Бургас 2012 г., Париж 2015 г. и Брюксел, 2016) послужиха за сигнализиране и събуждане за Европейската комисия за подобряване обмена на разузнавателна информация

сред 28-те държави-членки с Разузнавателния център на Европейския съюз (INTCEN), който би могъл да бъде трансформиран в Европейска Съюзна Агенция за Разузнаване (EUIA), като необходима институция за бъдещата Европейска армия.

В края на 21-ви век общността за разузнаване и сигурност на 28-те членки на Европейския съюз изисква диспергирано разузнаване, не концентрирано, отворено за различни източници, да не се ограничават с „държавни тайни“, необходимо е споделяне на вътрешна информация и анализ с различни коалиционни партньори, включително експерти и хора извън системата, а не да се пази информацията скрита под гриф "Строго секретно" .

Колективните действия зависят от споделеното разузнаване и общата оценка е стратегически необходима за националните разузнавателни служби в Европа. Това прави създаването на Европейска Съюзна Агенция за Разузнаване (EUIA) неотложно. Необходим е Съюз с цел недопускане и предотвратяване на други големи терористични инциденти в бъдеще. Крайно време е страните членки на Европейския съюз да разберат, че само с общи усилия може да бъде гарантиран мира, сигурността и спокойствието на обединена Европа.

ЛИТЕРАТУРА:

[10] Събев, С. Нашата разузнавателна общност би трябвало да се присъедини към Разузнавателната колегия на Европа, онлайн, достъпно на http://m.focus-news.net/?action=opinion&id=53028, видяно на 12.07.2020.

[11] Христов, Х. Военното контраразузнаване в разузнавателните общности. Университетско издателство „Епископ Константин Преславски“, Шумен, (2019), 10.

[12] Nomikos, John M., ‘A European Union Intelligence Service for Confronting Terrorism’, International Journal of Intelligence and Counterintelligence, Vol.18, No.2, (2005).

[13] https://geopolitica.eu/spisanie-geopolitika/144-2016/broi-4-2016/2530-tendentsii-v-razuznavatelnata-politika-na-es.

[14] https://www.consilium.europa.eu/bg/policies/fight-against-terrorism/counter-terrorism-coordinator.

[15] https://www.tandfonline.com/doi/abs/10.1080/08850607.2020.1754682.

[16] https://cyberleninka.ru/article/n/mezhdunarodnyy-poryadok-hedli-bulla-i-angliyskaya-shkola-teorii-mezhdunarodnyh-otnosheniy.

Име на автора: д-р инж. Дончо Христов Тилев
Месторабота: ВУСИ, Пловдив
E-mail: d_tilev@abv.bg

THE CORRELATION: NATIONAL SECURITY - NATIONAL POLITIC AND CRIME IN THE CONTEXT OF ECONOMIC PROBLEMS OF THE SECURITY SYSTEMS

YANA M. NIKOLOVA

ABSTRACT: *The resume is focused on aspects of national security considered as system which consist of many subsystems. Special attention is paid on the implementation of the tax policy and on the effords of minimizing ot the numbers of the crimes in that area in conection of the stabilization of her sustainabilty.*

KEYWORDS: *national security, tax crimes, economic security, system and subsystems.*

КОРЕЛАЦИЯТА: НАЦИОНАЛНА СИГУРНОСТ – ДАНЪЧНА ПОЛИТИКА И ПРЕСТЪПЛЕНИЯ, В КОНТЕКСТА НА ИКОНОМИЧЕСКИТЕ ПРОБЛЕМИ НА СИСТЕМАТА ЗА СИГУРНОСТ

ЯНА М. НИКОЛОВА

АБСТРАКТ: *Докладът обследва аспекти на националната сигурност като система, състояща се от множество подсистеми. Ключово място за сигурността е отредено на икономическата подсистема. Разгледано е значението на провежданата данъчна политика и намаляване на престъпленията в тази сфера с оглед стабилизиране на нейната устойчивост.*

Системата за сигурност е сложна обществена система, съставена от множество подсистеми, взаимно проникващи се, създаващи синергетичен ефект. Икономическите измерения на системата заемат централно място в нея, като голяма част от ядрото в този сектор е изпълнено от взаимовръзката – национална сигурност – данъчни престъпления.

Нейното изучаване е невъзможно, без да се декомпозира на функционалнно – самостоятелни подсистеми, като основните от тях са: политическа, икономическа, информационна, социална, военна, екологична сигурност, сигурност на гражданската защита и сигурност на обществената система. Всяка от тези подсистеми притежава обособени самостоятелни функции в общия функционален модел на сложната система национална сигурност. Както системата за национална сигурност, така и нейните подсистеми, притежават известна неопределеност на параметрите, която се обуславя от: случайността на събитията в природните и обществените процеси; прояви на агресия, терор и провокации; неправилен подход в собственото управляващо звено, субективизъм. В основата на общата система на сигурността стои подсистемата на икономическата сигурност, която синергетично си взеимодейства с останалите подсистеми. Икономическата сигурност е такова състояние на основните икономически показатели, които осигуряват нормално обществено производство за удовлетворяване на икономическите потребности на обществения живот и за постигане на цялостната национална сигурност в страната.

В статията „Актуални проблеми на икономическата сигурност“, публикувана в Брод за България, бр.1/18г. https://www.brodbg.com/news- 5 - 694 -Aktualni_ problemi_ na _

ikonomicheskata _ sigurnost.html, професор Евгений Сачев определя икономическата сигурност като основополагаща всред видовете сигурност. Икономическата сигурност влияе върху всички елементи и връзки в системата на националната сигурност. Тя осигурява социалната сигурност, основа е на военната сигурност, допринася за намаляване на социално – битовите престъпления. Чрез нея се намалява рискът от възникване на етнически и социални сблъсъци и успешно се преодоляват последствията от природни и промишлени бедствия и екологични катастрофи. Всяка държава заделя средства за решаване на своите нужди в отделните подсистеми – военно дело, здравеопазване, култура, научни изследвания, социални нужди и пр. Отделната подсистема има собствена относителна тежест в системата на националната сигурност и за своя основа – икономическата сигурност. Укрепването на националната икономическа сигурност разширява възможностите на националната сигурност и в международен план. Националната икономическа стабилност дава национално самочувствие и намалява влиянието на външния натиск в международен план.[1]

Икономическата сигурност на националното стопанство е важен съставен компонент на комплексната сигурност и заедно с политическата и военната сигурност създава основата, върху която се изграждат и останалите пластове на сигурността. Така в Стратегията за национална сигурност на САЩ от 2015г. четем: „Укрепването на икономическата мощ на Америка е в основата на нашата национална сигурност“. В съвременните условия във всички държави протича процес, при който целият обществен живот се поставя на икономическа основа и има икономически измерения, известен като „икономизация на политиката.[2]

Заплашващ фактор, който действа с голям интензитет в посока – разрушаване на системата, е престъпността. Конкретно данъчните престъпления са пряко насочени към ощетяване на държавния бюджет. Фискът е материалната основа, върху която се гради сигурността – той обезпечава военното дело, правосъдието, образованието, здравеопазването и пр. Колкото по – развита е данъчната престъпност, толкова по – малка е сигурността в държавата. Намаляват предвидимостта, устойчивостта и стабилността в развитието. Налага се извод, че данъчната престъпност подкопава устоите на подсистемата на икономическата сигурност, която крепи всички останали подсистеми в системата на националната сигурност.

Поддържането на данъчната система на суверенната държава е един от основните компоненти на обезпечаването на сигурността на държавата и нейните граждани. Данъчните престъпления сериозно дестабилизират фискалната система и произвеждат негативен икономически ефект. В криминологичен аспект извършването и несанкционирането на данъчни престъпления води до неконтролируемо развитие на сивата икономика, разрастване на организираната престъпност. По данни на ДАНС за 2014г. при извършен анализ на паричните потоци със съмнителен произход се установява тенденция престъпленията срещу фиска да остават основни предикатни престъпления за изпирането на пари.[3]

[1] Сандев, Г. Система и политика на националната сигурност. Шумен: Унив.изд. Епископ Константин Преславски, 2003.

[2] Велкова, Л. Икономически измерения в стратегията за национална сигурност на САЩ (2015г.) // Военен журнал: двумесечно издание на Министерство на отбраната, 2015, № 2, с. 55 – 60.

[3] Йорданова, Хр. Противодействието на данъчните престъпления в системата за обезпечаване на национална сигурност // Сборник на научен форум на департамент „Национална и международна сигурност“ при НБУ. София, 2016.с. 545 – 551.

На 09.01.2020г. на сайта на ДАНС е публикуван доклад за Национална оценка на риска от изпиране на пари и финансиране на тероризма. В него е заключено, че борбата срещу изпирането на пари и финансирането на тероризма е от изключително значение за сигурността и просперитета на България. В списъка с основни рискови събития са включени: изпиране на пари от широк кръг предикатни престъпления, свързани с данъчни престъпления, като най – висок риск е установен по отношение на търговията с храни, горива и скрап; изпиране на пари от данъчни престъпления (избягване установяването на данъчни задължения и измами с ДДС) чрез използването на подставени лица, местни и чуждестранни ЮЛ в сложни схеми за разслояване и с помощта на „професионални перачи“; изпиране на средства, придобити от данъчни престъпления в сферата на търговията с храни и горива чрез използването на кухи компании и номинални собственици, подпомагано от корупционната среда.

Източването на данък добавена стойност от държавния бюджет се определя като престъпление с висока степен на обществена опасност, защото е кражба на вече постъпили средства в бюджета, платени от порядъчните данъкоплатци, които разбират необходимостта от плащането на данъци и нормалното функциониране на икономиката. През 2005г. директорът на Агенцията за финансово разузнаване – д-р Васил Киров, заявява по повод анализ „Корупцията в данъчното облагане“, че 30 на сто от потока „мръсни пари“ у нас са от неправомерно източване на ДДС. Данъчната корупция е основен двигател на други видове корупция. Тя осигурява черни каси и прикриване на доходи. Заметник – директорът на Главна данъчна дирекция (НАП) – Валентин Видолов, по повод горния анализ, е заявил през 2005г. разкрива, че Данъчните ревизии на физически лица показват, че във всеки голям град, където са проверявани собственици на имоти и коли за стотици хиляди левове, поне десет човека са укрили данъци за над сто хиляди лева.[4]

Делът на ДДС заема голям дял в бюджетните приходи. България се нарежда сред страните, в които косвените данъци осигуряват основен процент от приходите на бюджета. Така престъпните схеми с предмет ДДС засягат сериозно сигурността на страната ни. Не без значение за увеличаване на бюджетните приходи е и фискалната политика на държавата. Ако липсва конкурентноспособност на националните производители, правителството би следвало да се опита да я създаде. В данъчната сфера най – елементарното действие би било намаляване и диференциаране на стоките от първа необходимост. Намалението на цената при тези стоки, посредством снижаването на данъка върху добавената стойност , би увеличило тяхното търсене и потребление, което от своя страна би било причина за повишение на производството им, а увеличението на производството би довело до ново снижаване на цената в резултат на т.нар. икономия на мащаба.[5]

Фискалната политика на държавата има голямо значение и за намаляване или увеличаване на данъчната престъпност, а оттам и връзка с нивата на влияние върху националната сигурност. Данъчната политика на всяка държава не се изгражда самоцелно, тя винаги е част от нейната финансова политика, която включва още бюджетна политика, парично – кредитна политика, ценова политика, митническа политика, социална пилитика и пр. Когато цялостната политика на правителството постига ликвидация на частния дребен и среден бизнес, който финансира бюджета чрез данъците, които плаща, то и предприемачите търсят начини за избягване плащането им, за да оцелеят. Така например,

[4] Григоров, М. Данъчните престъпления са основен двигател на сивата икономика у нас. // Българска армия – вестник за национална сигурност и отбрана, 2005, №16, с.11.

[5] Николов, Ч. Фискалната политика у нас консолидира социалната несправедливост // Ново време: месечен преглед на умствения и обществения живот, 2004, № 12, с. 21 – 26.

увеличаването на данъчната ставка на ДДС от 18% на 22% в средата на 90 – те години на миналия век, в условия на криза, свива потреблението, без да повишава данъчните приходи и дава по – големи възможности за престъпно приспадане на ДДС. През същия времеви период, изискването за задължително безналично разплащане по вземания и задължения на фирмите над определена сума има за цел да осигури информация, която може да бъде използвана и за целите на облагането. Неочакваната ликвидация на някои банки обаче, застига неподготвени техните клиенти. Много фирми са потърпевши от това, че са спазвали разпоредбите за ограничения на кешовите операции и са извършвали разплащанията си по банков път. Загубите, които понасят, водят някои от тях до фалит. Тези от тях, които оцелеят, в бъдеще преминават предимно към кешови разплащания, за да избегнат финансовия риск от проблеми с ликвидността на обслужващата ги банка. Така се оформят предпоставки за разширяване на обхвата на вериги от нерегистрирани сделки , върху които не се начислява и се избягва плащането на ДДС. Друга причина за прикриване на обороти от облагаеми сделки и ниска данъчна събираемост е слабо действаща контролна система. Получава се омагьосан кръг – държавата не може да си събере нужните за функционирането и данъчни приходи и задлъжнява. Налага се да увеличава данъчното бреме, а колкото повече го увеличава, толкова повече дребни и средни търговци разорява и принуждава оцелелите да укриват сделките и доходите си от облагане.[6] Ето как фискалната политика има косвено касателство към нивата на данъчна престъпност в държавата, а оттам и към сигурността на нацията.

Данъчната политика на държавата не следва да се разглежда изолирано от социално – икономическия контекст. Друг фактор, който влияе по веригата – фискална политика – данъчни престъпления – национална сигурност, е икономическата криза. В хода на криза една от централните теми на политическите и икономическите дебати е темата за използването на данъчно бюджетните стимули като антикризисно средство за стабилизиране и възстановяване на икономиката. Успешното преодоляване на кризата зависи много от ефикасността на водената фискална политика. Така например могат да се предвиждат мерки за стимулиране на потреблението като увеличаване на необлагаемия минимум и намаляване на данъците за хората с по- ниски доходи.[7]

В статията „Приходната част на бюджета и фискалната политика“, публикувана в сп. „Икономика и икономическо регулиране: месечно издание за теория и бизнес“, 1999, №2, с. 4 – 7, авторът Йосиф Аврамов споделя виждането, че в условия на криза за развитието в районите с по – висока безработица от средните за страната нива е необходимо предоставянето на осезателни облекчения при данъчното облагане. Действително, при разследване на данъчни престъпления, извършени по схемата с т. нар.„кухи фирми“, се наблюдава, че често пъти лицата, на чието име се прехвърлят фирми – фантоми, произхождат от икономически слабо развити и бедни региони.

В интервю пред в.“Банкеръ“ (Кризата рязко увеличи опитите за данъчни измами // Банкеръ: национален седмичник за финанси, икономика и политика, 2010, №27, с.10) изпълнителният директор на НАП – Кр. Стефанов разкрива, че когато икономиката ни е в криза и фирмите изпитват затруднения да финансират дейността си, липсва им оборотен капитал, потреблението се свива, респ. – намаляват постъпленията от данъци, пред НАП стоят две възможности. Първата е да започне да започне да прилага цялата тежест на репресивния апаратпри събиране на дължимите данъци. В този случай, в последващия

[6] Ботева, М. Крахът на фискалната политика обрече България на просия // Банки. Инвестиции. Пари, 1996, № 6, с. 31 – 38.

[7] Владимиров, Вл. Фискалната политика в условията на икономическа криза // Известия – списание на Икономическия университет – Варна, 2020, №1, с. 58 – 69.

времеви период няма да има бизнес, върху който да налага репресии. НАП е избрала друг подход – проява на разбиране към фирмите и съсредоточаване усилията върху данъчните измами. Създаден е специален ресор за борба с измамите под прякото ръководство на един от заместниците на изпълнителния директор. Следва изводът, че към остта: фискална политика – данъчни престъпления – национална сигурност, след фискалната политика, място заема и политиката в условия на оперативна самостоятелност, провеждана от правоприлагащия орган в лицето на приходната администрация.

В заключение може да се направи извод, че фискалната политика на държавата има голямо значение за намаляване или увеличаване на данъчната престъпност, а оттам и връзка с нивата на влияние върху равнището на националната сигурност. Данъчната система има функция да осигури приходи в държавния бюджет с цел – финансово обезпечаване на дейностите, които способстват за запазване на държавността. Това е един от факторите за гарантиране на сигурността и в този смисъл данъчната престъпност подкопава устоите на подсистемата на икономическа сигурност, която крепи всички останали подсистеми в системата на националната сигурност.

ЛИТЕРАТУРА:

[1] Сандев, Г. Система и политика на националната сигурност. Шумен: Унив.изд. Епископ Константин Преславски, 2003.

[2] Велкова, Л. Икономически измерения в стратегията за национална сигурност на САЩ (2015г.) // Военен журнал: двумесечно издание на Министерство на отбраната, 2015, № 2, с. 55 – 60.

[3] Йорданова, Хр. Противодействието на данъчните престъпления в системата за обезпечаване на национална сигурност // Сборник на научен форум на департамент „Национална и международна сигурност“ при НБУ. София, 2016.с. 545 – 551.

[4] Григоров, М. Данъчните престъпления са основен двигател на сивата икономика у нас. // Българска армия – вестник за национална сигурност и отбрана, 2005, №16, с.11.

[5] Николов, Ч. Фискалната политика у нас консолидира социалната несправедливост // Ново време: месечен преглед на умствения и обществения живот, 2004, № 12, с. 21 – 26.

[6] Ботева, М. Крахът на фискалната политика обрече България на просия // Банки. Инвестиции. Пари, 1996, № 6, с. 31 – 38.

[7] Владимиров, Вл. Фискалната политика в условията на икономическа криза // Известия – списание на Икономическия университет – Варна, 2020, №1, с. 58 – 69..

Име на автора: Яна Миткова Николова
Месторабота: Окръжна прокуратура, гр. Шумен
E-mail: yananikolova@abv.bg

THE STATE AND THE RELIGIOUS COMMUNITIES IN THE PERIOD 1944 - 1989

TIHOMIR I. SOLAKOV

ABSTRACT: *Between 1944 and 1989. The Bulgarian State, through its state security structures, has controlled religious communities that have been active on the territory of the country with a focus on those with overseas representations, since they, in addition to carryng out an activity aimed at spiritual security, have carried out intelligence activities in the interest of foreign states.*

KEYWORDS: *religions; state security religious communities; sects.*

ДЪРЖАВАТА И РЕЛИГИОЗНИТЕ ОБЩНОСТИ В ПЕРИОДА 1944 Г. – 1989 Г.

ТИХОМИР И. СОЛАКОВ

АНОТАЦИЯ: *В периода 1944г.-1989г. Държавата посредством структурите на държавна сигурност е осъществявала контрол над религиозни общности, които са развивали дейност на територията на страната с акцент върху тези имащи задгранични представителства, тъй като те, освен че са развивали дейност, насочена срещу духовната сигурност, са осъществявали разузнавателна дейност в интерес на чужди държави.*

1. Въведение

През периода 1944г.-1989г. властта в България предприема редица целенасочени и организирани действия свързани с раздалечаване на духовенството от светската власт и отдалечаване на народа от религията без значение към кой етнос принадлежи и каква религия изповядва човек с цел приобщаване към господстващата идеология на марксизма и ленинизма. В същото време различни западни деноминации, възползвайки се от дейността на държавата към традиционните религи и от настъпилия духовен вакуум в обществото, правят опити, някои успешни, а други не, да навлязат на територията на България. Последните същевременно са използвани от различни разузнавателни служби, за да проникнат на територията на страната и да събират разузнавателна информация от разнороден характер. За постигане на целите си, държавата възлага на държавна сигурност задачи свързани с осъществяването на контрол по линия на духовната сигурност на всички религиозни общности.

2. Изложение

Религиозните общности в тоталитарна България присъстват трайно в полезрението на комунистическата власт в контекста на конкретните задачи, които тя си поставя за решаване в процеса на изграждане на социалистическата държава и общество по съветски модел. В периода 1944г.-1989г. в страната са регистрирани и имат право да извършват дейност 12

църкви, изповедания и деноминации: Българската православна църква; Мюсюлманско изповедание; Католическата църква; Евангелската съборна църква; Евангелска методистка църква; Петдесятната църква; Църква на адвентистите от седмия ден; Баптистката църква; Църква на адвентистите от седмия ден – Реформаторска движение; Арменогрегорианската църква; израилтянското движение и верската общност „Бялото братство". Всички изброени църкви и вероизповедания присъстват в България от преди 9 септември 1944г. , официално са признати за такива и се толерират, с изключение на „Бялото братство". [1]

Всички вероизповедания и секти от една страна и държавната власт в Народна република България от друга, в периода от 1944 г. до 1989 г., имат свои особени взаимоотношения, които се формират на базата на конституциите от 1947 г. и 1971 г., на Закона за изповеданията от 1949 г. и от влиянието на Държавна сигурност. Основният посредник и свързващ елемент във взаимоотношенията между религиозните общности и държавата е Дирекцията по изповеданията, която в различни моменти от разглеждания период преминава от Министерство на външните работи към Министерски съвет и обратно в зависимост от ролята, която трябва да изиграе в решаването на даден въпрос. [2] В посочения период от време (1944 г. - 1989г.) действащите религиозни организации и общности са по-скоро предприемчиви и оптимисти. В противовес на всяко очакване те правят неистови опити да заемат завидни позиции в българското духовно пространство и да евангелизират народа въпреки строгия контрол на Държавна сигурност.[3] В подкрепа на предходното се явява фактът, че религиозната обстановка след 1944г. в страната се променя. Българската православна църква е отделена от държавата[4], като и държавата, и Църквата в България са в процес на радикални промени. В края на 1945 г. часовете по класически езици и религия са изхвърлени от учебните програми. На 24 февруари 1949 г. е гласуван Религиозният закон, чрез който се осигурява пълен контрол на Комунистическата партия върху българската православна църква (БПЦ). Църквата губи постепенно властта и авторитета си сред народа, и дейността ѝ е сведена до минимум. Останалите традиционни религиозни общности съществуват и проповядват почти нелегално.[5]

След 09.09.1944г. новото управление на държавата смята, че една от заплахите за сигурността на страната за този период от време идва от различните религиозни общности, деноминации, вероизповедания и църкви. В тази връзка тя прави така, че в новосъздадената ДС да има приемственост, като в този период от време се извършва ускорено обучение на служителите на ДС назначени от правителството на БКП. Техни лектори са бивши служители на ДС като Андрей Праматаров, Коста Велчев, Владимир Караманов, които преди 09.09.1944г. са работили в отделение на „Б" на ДС . Техни знайни и незнайни колеги се оказват доста схватливи и не пропускат да приложат на практика новопридобитите знания и умения. На първо място като се възползват от вече готовия продукт. Така например документите, с които след 9 септември 1944 г. се открива делото за католиците, всъщност са извадки от годишните доклади на отделение „Б" за проявите на религиозните пропаганди и секти в страната от края на 30-те и началото на 40-те години. По аналогичен начин през 1948 г. е открито и досие на френското търговско консулство в Пловдив. На челно място оперативният работник е поставил оригиналния доклад на началника на група „Б" при Пловдивското областно полицейско управление Л. Червенков от 1943 г. за персонала на

[1] Лефтеров Живко, „Религиозната политика на Българската комунистическа държава и „Бялото братство (1944г.-1953г.)", издателство „Нов Български-университет", ISBN 9786192330248, 2018г., стр.83

[2] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти" , „Държавна сигурност и вероизповеданията", част III, София, 2017г., ISBN 978-619-7361-22-3, стр.7

[3] Христова Милка, „Религиозните движения в България", 19.06.2006г., https://dveri.bg/uc8

[4] http://pomagalo1.com/art/syshtnost-i-istoriq-na-sektanstvoto-v-bylgariq/28292/p2

[5] Христова Милка, „Религиозните движения в България", 19.06.2006г., https://dveri.bg/uc8

консулството, френската колония и франкофонските дружества и институции в града. Списъкът на приоритетните обекти е окупиран почти изключително от католици, които заедно с други техни събратя и едноверци, свещеници и миряни, са смятани от бившата ДС за агенти на френското разузнаване. На същата архивна основа са положени и досиетата на всички други чужди легации, консулства, дружества и колонии. Предходното е в следствие на факта, че приемствеността между „бившата" и „новата" ДС не се ограничава само до споделен професионален опит, обща информационна база и идентични обекти, а отива и по – далеч - чак до апарата на секретните сътрудници. Най-ценни в това отношение са агентите на Гестапо, чиито разкрития са друг източник на професионален опит за начинаещите български контраразузнавачи в периода 1945 - 1946г., които са едни от най-издирваните от ДС обекти в страната, както и бившите щатни и нещатни служители на ДС от преди 9 септември 1944г. В резултат посятите между 1934 и 1944 г. семена на съмнение за предполагаема шпионска дейност на католически свещеници и миряни в полза на Франция и нейните англо-американски съюзници след 09.09.1944г. подпомагат водения съдебен процес срещу „шпионската и заговорническа католическа организация в България" през 1952 г.[6]

През 1955г. държавата и в частност ДС обръща внимание и започва да наблюдава религиозната секта „Казълбаши-алияни", при която религиозните обичаи и празници се провеждат на строго конспиративни начала, като последователите не признават никаква власт. Интересът на Държавна сигурност към тази изключително затворена група хора не секва като в хода на изпълнение на своята дейност към 1959г. те установяват, че мюсюлманските секти провеждат своята религиозна дейност в частни, нерегистрирани като молитвени домове помещения, което противоречи на закона. В резултат са набелязани мероприятия за закриването и забраната на домовете и местата, където се провеждат религиозните обреди на сектите.[7]

Напълно логично след 9 септември 1944 г., освен че се е гледало на католически свещеници и миряни в България като на лица извършващи предполагаема шпионска дейност осъществявана в полза на Франция и нейните англо-американски съюзници[8], по същия начин се е гледало и на евангелските деноминации като на проводници на западното влияние, а на пасторите и миряните като агенти на чужди разузнавания. Евангелските секти през 1946 г. според ДС са използвани от американското разузнаване в България и като преди тази година идейно и ръководно евангелските деноминации са били под германски борд на управление, след което официално преминават под американски. С това цялото им съществуване и дейност е в ръцете на американското разузнаване, като Държавна сигурност е имала сведения, че всички пастори и отделни ръководители на „американските секти" са ревностни агенти на американското разузнаване, проводници на американската пропаганда сред евангелистите и „отлични събирачи на сведения от различно естество". Две години по-късно (1948г.) ДС отчита, че от страна на евангелистите пропагандата се води по един фин начин, като чуждото разузнаване, респективно англо – американското, използва по всякакъв начин евангелските мисионери и пастори в изграждането на шпионски мрежи във военния, политическия и културния отрасли в страните, където е разпространен евангелизмът. Този анализ е в резултат на водена разработката в ДС на евангелските

[6] Елдъров Светлозар, „Католиците в България (1878-1989) ", София, 2002г., Стр.275-стр.276, http://www.bulgari-istoria-2010.com/booksBG/S_Elderov_Katolicite_v_BG.pdf

[7] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти", „Държавна сигурност и вероизповеданията", част II, София, 2017г., ISBN 978-619-7361-19-3 , стр.9

[8] Елдъров Светлозар, „Католиците в България (1878-1989)", София, 2002г., стр.276, http://www.bulgari-istoria-2010.com/booksBG/S_Elderov_Katolicite_v_BG.pdf

пастори, уличени в провеждане на валутно – доларова афера и противонародна шпионска дейност в резултат на което след 20 юли 1948 г. са задържани петнадесет души пастори, влизащи във Върховния съвет на евангелистите, които са създали и развили противонародна шпионска дейност, изразяваща се в даване на сведения на чужди мисии за военно, политическо и друго състояние на Народна република България. В резултат с Присъда № 118 от 8 март 1949 г. срещу евангелските пастори са наложени четири доживотни присъди; четири присъди по петнадесет години лишаване от свобода; три – на десет години и други с различна продължителност. [9]

През 1962г. Комитетът по вероизповеданията при Министерство на външните работи и отдел „Народни съвети“ при Министерски съвет изпращат до всички председатели на окръжни народни съвети и градски съвети в София, Пловдив и Варна окръжно с № А—1-455/12.XI.1962г съгласно което се дават указания за извършване на регистрация на сектантските евангелски секти (Евангелска баптистка църква, Евангелска методистка църква, евангелска петдесятна църква и адвентисти от седмия ден) и верската общност „Бялото братство”, като останалите секти, самостоятелни групи и общности нямат право на регистрация и трябва да преустановят своята дейност. В резултат в началото на 1964г. се извършва регистрация на протестантските изповедания в България. [10]

За изпълнение на решенията на Секретариата на ЦК на БКП от 24 януари 1967 г., отнасящи се за по-нататъшното подобряване на работата за атеистическото възпитание на трудещите се и решенията на ръководството на МВР за организиране борбата срещу идеологическото проникване на противника, пресичане и компрометиране каналите и дейността на задграничните религиозни централи и организация работещи срещу Народна република България се предприемат мероприятия с цел изясняване замислите, формите на работа, каналите за проникване и техните връзки в страната. В резултат са задържани, разследвани, разобличени чрез пресата и изгонени от страната мисионери, конфискувани са леките им коли и голямо количество различна религиозна литература, внесена по нелегален път. Наред с мероприятията по задграничните централи и мисионери са проведени и такива по техните връзки в страната. Спрямо по-активните духовници ДС провежда мероприятия за компрометиране и дискредитиране пред вярващите, други са разобличавани в пресата, а трети предавани на съд или изселвани. За ограничаване и занижаване дейността на религията са обсъждани и провеждани съвместни мероприятия с градските комитети на Комсомола, домът на атеиста, отдела за агитация и пропаганда при ЦК на БКП. [11]

През 1982г., сектите в България имат 161 молитвени домове, обслужвани от 150 пастори и проповедници и около 18000 вярващи. Признати от Закона за изповеданията и в положение на търпимост (които нямат юридически права) са сектите: „Петдесятници”, „Адвентисти от седмия ден”, „Конгрешани”, „Баптисти”, „Методисти” и „Бяло братство” – дъновисти. Освен тях незаконно съществуват сектите „Адвентисти-реформатори”, „Свидетели на Йехова”, „Тинчевисти” и други, които са поставени извън закона и дейността им е забранена. Протестантските секти в страната са на самоиздръжка. Повечето от тях набират средствата си от дарения на вярващите под формата на „дискос” . Само Адвентистите от седмия ден и Адвентистите – реформатори събират от вярващите

[9] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти”, „Държавна сигурност и вероизповеданията“, част III, София, 2017г., ISBN 978-619-7361-22-3, стр.7

[10] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти”, „Държавна сигурност и вероизповеданията“, част III, София, 2017г., ISBN 978-619-7361-22-3, стр.156-168

[11] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти”, „Държавна сигурност и вероизповеданията“, част III, София, 2017г., ISBN 978-619-7361-22-3, стр.9

„десятък". Всички секти са добре обезпечени материално и имат големи приходи, които им дават възможност да изплащат добри възнаграждения на служителите си. Характерна за сектите е тяхната активна религиозна дейност и обработка за привличане на младежи за членове на различните религиозни общности. За тази цел те осъвременяват и модернизират методите и формите на работа, като организират младежки служби за изучаване на библията, туристически излети, екскурзии и др. Отчетено е в този период от време, че се забелязва активизиране на протестантските секти под влияние на западните реакционни религиозни централи като: „Славянска мисия", „Мисия за евангелизиране на комунистическите страни", „Международна федерация на свободните евангелски църкви"' „Операция мобилизация" , „Йеховистки център – Бруклин" и др. Задграничните централи ползват възможностите на разширения международен туристически, културен обмен, като изпращат в страната техни емисари, големи количества религиозна и друга пропагандна литература, парични средства, покани за следване или гостуване в техни богословски институти и училища.[12]

През 1983 г. държавата и в частност ДС установяват и наблюдават активизиране на дейността на задграничните религиозни централи за проникване, оказване на влияние и активизиране на религиозните общности в България, като за оказване на идеологическо въздействие върху български граждани се ползва международния туристически обмен, средствата за масова информация и др. Чрез тях под прикритието на религията се прокарват идеи, насочени към подбуждане на вярващите в страната към антиобществени прояви. Отправят се искания за свободно разпространение на религиозна литература, внасяна от Запад, за въвеждане на религиозно обучение в училищата и религиозни предавания по радиото и телевизията.[13]

Видно от гореизложеното е, че в периода 1944г. – 198г. Държавата и в частност Държавна сигурност са наблюдавали и контролирали дейността на нетрадиционните религиозни общности на територията на България, които са развивали активна мисионерска дейнот за набиране на нови последователи и разпространение на постулатите на представените от мисионерите секти. Предходното се подкрепя от факта, че във времето протестантските църкви успяват да разширят влиянието си в страната, като през 1944 г. те имат 5-6 000 привърженици, а през 1989 г. вече около 25 000 души. Това се дължи на активната религиозна дейност на църквите и нейните членове, помощта на техните задгранични центрове, отливът на вярващи от православието. През периода 1944г. – 1989г. има опити от страната на „Свидетели на Йехова" да създадат свои организирани групи в страната. Най – сериозната група е на американката от български произход Мария Калой, която през 1969г. успява да изгради у нас нелегално действаща секта от около стотина йеховисти в София, Пловдив и Видин, но не достига особени успехи. Слаби опити за придобиване на позиция в България правят последователите на сектата „Назорей" с ръководител Анастасия Христова. Това е секта, разпространена в САЩ и пренесена в България в началото на века от Тодор Костурков от Пазарджик. Нейните последователи вярват в прераждането на душата и приемането на идеята за „полярността" – всеки мъж и жена има предопределен от Бога двойник, с когото трябва да встъпи в брак. През 80-те години тяхната дейност постепенно замира.[14] Дейността на други нетрадиционни религиозни общности, в България е илегална и контролирана от Държавна сигурност.

[12] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти", „Държавна сигурност и вероизповеданията", част III, София, 2017г., ISBN 978-619-7361-22-3, стр.10-стр.11

[13] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти", „Държавна сигурност и вероизповеданията", част III, София, 2017г., ISBN 978-619-7361-22-3, стр.10-стр.11

[14] http://pomagalo1.com/art/syshtnost-i-istoriq-na-sektanstvoto-v-bylgariq/28292/p2

Нелегална религиозна пропаганда през 70-те години развиват Славянска религиозна мисия със седалище в Швеция, Християнска мисия за евангелизация на комунистическите държави със седалище в САЩ, Операция-мобилизация създадена в Испания, Международна религиозна мисия – Германия и австрийския Институт за религиозно образование. Освен посочените религиозни общности в България проповядват също така нелегално и неорганизирано назареите, „Свидетелите на Йехова" (1969 г.), Трансцедентална медитация (1979) и Международно общество за Кришна съзнание (70-80-те години), правят се успешни или неуспешни опити за внасяне на религиозна литература в страната.[15]

3. Заключение

В обощение на изложеното може да се направят следните изводи:

- в периода 1944г.-1989г. различни религиозни деноминации със седалища извън пределите на България са правили неуспешни опити, а други са навлизали на територията на страната за неофициално развиване на религиозна дейност;

- държавата посредством ДС е наблюдавала и осъществявала контрол над дейността на тези религиозни деноминации имайки предвид, че освен, че дейността им е насочена срещу духовната сигурност, то те осъществяват и дейност свързана с чужди разузнавателни служби.

- за развиването на своята нерегламентирана дейност на територията на България в периода 1944г.-1989г. задграничните централи на деноминациите, възползвайки се от възможностите на разширения международен туристически, културен обмен са изпращали в страната техни емисари, големи количества религиозна и друга пропагандна литература, парични средства, покани за следване или гостуване в техни богословски институти и училища, за да разширяват влиянието на деноминациите си.

ЛИТЕРАТУРА:

[1.] Живко Лефтеров, „Религиозната политика на Българската комунистическа държава и „Бялото братство (1944г.-1953г.)", издателство „Нов Български-университет", ISBN 9786192330248, 2018г.
[2.] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти", „Държавна сигурност и вероизповеданията", част III, София, 2017г., ISBN 978-619-7361-22-3.
[3.] КРДОПБГДСРСБНА, „Протестантска църква и религиозни секти", „Държавна сигурност и вероизповеданията", част II, София, 2017г., ISBN 978-619-7361-19-3
[4.] Милка Христова, „Религиозните движения в България", 19.06.2006 г., https://dveri.bg/uc8
[5.] Светлозар Елдъров, „Католиците в България (1878-1989)", София, 2002г., http://www.bulgari-istoria-2010.com/booksBG/S_Elderov_Katolicite_v_BG.pdf
[6.] Светлозар Елдъров, „Католиците в България (1878-1989)", София, 2002г., http://www.bulgari-istoria-2010.com/booksBG/S_Elderov_Katolicite_v_BG.pdf
[7.] http://pomagalo1.com/art/syshtnost-i-istoriq-na-sektanstvoto-v-bylgariq/28292/p2

Име на автора: д-р Тихомир Иванов Солаков
Месторабота: ВТУ „Св.Св.Кирил и Методий", Факултет по „Философия", катедра „Национална сигурност"
E-mail: tihi35@abv.bg

[15] Христова Милка, „Религиозните движения в България", 19.06.2006г., https://dveri.bg/uc8

MOON'S CHURCH (SECT) A THREAT TO NATIONAL SECURITY

TIHOMIR I. SOLAKOV

ABSTRACT: *The Unification Church (UC), also known as Moon's church or sect is a worldwide religious movement whose members are called "Moonies". Often characterized as dangerous cult, Moon's sect threatens national security by carrying out activities which are focused on the spiritual security of the nation and intelligence activities in countries of interest to the Korean intelligence and to the American CIA.*

KEYWORDS: *Moon's church ; sect; intelligence.*

ЦЪРКВАТА (СЕКТАТА) НА МУУН ЗАПЛАХА ЗА НАЦИОНАЛНАТА СИГУРНОСТ

ТИХОМИР И. СОЛАКОВ

АБСТРАКТ: *Обединената църква, известна още като църквата или сектата на Муун, е световно религиозно движение, чиито членове се наричат „мууниси". Често характеризирана като опасен култ, сектата на Муун застрашаваа националната сигурност чрез извършване на дейности, които са фокусирани върху духовната сигурност на нацията и разузнавателни дейности в страни, които представляват интерес за корейското разузнаване и Американското ЦРУ.*

1. Въведение

Църквата на Сун Мюнг Муун е основана през 1954г. и е едно от най-големите нетрадиционни религиозни движения в целия свят. Същата за няколко десетилетия се е разпространила по целия свят и има от пет до десет милиона последователи. В църковното движение членуват самостоятелни религиозни деноминации като например Християнска църква „Сион", Съюз на Евангелските баптиски църкви и др. Проповядваната религия от Църквата на обединението е смесица от християнство и източноазиатски доктрини, която няма нищо общо с проповядванто от традиционните конфесии. Освен религиозна дейност Църквата на Муун осъществява дейност в интерес на корейското и американско ЦРУ посредством своите центрове в различни страни от света.

2. Изложение

Сектата на Муун може да се охарактеризира като окултно-синкретична шаманска духовна месианска секта в обвивка от няколко термина, заимствани от християнството.[1] Същата е по-известна, като „Църквата на обединението" (Асоциация на Светия Дух за обединение на световното християнство) и е основана през 1954 г. в Сеул. Нейният основател, Сан Мьюнг Муун, е роден на 6 януари 1920 г. в християнско семейство в провинция Пюнган Букдо (сега Северна Корея). Призванието на мисията на религиозен водач той почувствал на 16-годишна възраст, когато преживял „първо появата на Исус

[1] Миссионерско-Апологетический проект Кистине, „Движение объединения" Сан Мен Муна, Русские юноши и девушки клянутся в верности „истинным родителям" Муну с женой и "истинному отечеству" Корее", Секты / „Церковь Объединения" - секта Сан Мен Муна, http://www.k-istine.ru/sects/moon/moon_about.htm

Христос, а след това на Буда, Лао Цзе, Конфуций и Мохамед". На 1 май 1954 г. в Сеул е основана Обединителната църква (Сдружение на Светия Дух за обединението на световното християнство). Системата на собствените им религиозни вярвания е очертана в книгата „Божествен принцип".[2] Въпреки че желанието на мунистите е да обединят християните, те сами не са християни в традиционния каноничен смисъл на думата като последователите на Мун не изповядват Светата Троица, не вярват в Божествеността на Христос, отхвърлят Неговото възкресение, разпъването му, считат го за провал на Неговата мисия, отричат свещеничеството на Божията Майка. Във вероучението на „Църквата на обединението" личността на Муун Сан Мена заема централно място, което се основава на откровенията на основателя (това обстоятелство дава възможност да се нарече учението на Муун мунизъм, а неговите последователи мунисти). Повечето от трудовете на Муун не са преведени от корейски на европейски езици, което усложнява изучаването на неговия мироглед. Частично основите на учението на Луната са представени в две негови книги като допълнителна информация се съдържа в безбройните му речи и проповеди. За членовете на АСД-ОМХ (Асоциация на Светия Дух за обединяване на световните християни) на Муун има Месия и това определя целия живот и дейност на всеки мунист и на асоциацията като цяло. [3]

Последователите на Муун твърдят, че се опират на Библията, и дори се наричат християни, но това няма нищо общо с действителността. Самият Муун открито заявява, че ползва Библията единствено за камуфлаж: „Докато не завършим мисията си в християнската църква, ние трябва да цитираме Библията и да я използваме, за да обясняваме. След като получим наследството на християните, ще бъдем свободни да поучаваме без Библията"[4]. За изграждане на своята религиозна доктрина Мууните усвоили християнската терминология като са я адаптирали към своето учение[5], като основната идея на учението на Муун е, че Бог има Отец, а хората са неговите деца. Божието сърце е преизпълнено с неизразима болка на Родителя, отхвърлен от заблудените деца, като в резултат на тази празнина те също страдат. Приключването със страданието, постигането на всеобщо помирение и хармония може да бъде преодоляно само чрез три основни препятствия: нравствен егоцентризъм, разобличаване на световните религии, всепроникващото влияние на безбожната идеология. Според Муун Бог е вечната енергия, пулсираща между мъжкото и женското начало, като целта на създаването е перфектното семейство. Грехопадането на Ева е довело до загуба на вяра и извращение на първоначалния идеал на истинската любов. След като съгреши със Сатана, Ева му роди Каин, като за спасението на човечеството може да се стане само от съвършеният човек, който е създал перфектното семейство. За спасението на хората, Бог изпратил Месията – Исус, който е бил неразбран от съвременниците му, е бил отхвърлен и разпнат. Той е давал на хората само духовно спасение, без да изпълни основната си задача. През 1960 г. Муун се оженва за перфектна жена, Хак Джа Хан Муун, като от този момент започва спасението на човечеството и Корея става център на Вселената и целият духовете свят трябва да признае Муун като техен господар. Главното култово действие в църквата на Муун е пречистването на „кръвта на света", неговото освобождаване от сатанинското начало. Той се произвежда с помощта на церемонията по „осоляване" на помещенията, както и с причастието на

[2] Трофимчука Н.А., Свищева М.П. „Церковь объединения (Церковь Муна)", „Миссионерство и новые культы в России, Глава из монографии „Экспансия", М, 2000г., https://psyfactor.org/expan7.htm

[3] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

[4] http://www.chitatel.net/forum/topic/6606

[5] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

„специално вино", което заедно с други 20 компонента включва и кръвта на преподобния Муун.[6]

Вербуването на нови членове на „Църквата" се извършваше съвсем открито, но само до момента, в който жертвата падне в поставените примки, като новите „деца" ги подлагат на последователно „обучение" за 7, 21, 40 и 120 дни. В този период от време, „Децата" не са оставяни сами за дори една минута като те са принудени да работят, да слушат лекции, да се молят и да пеят химни за 14-1 базисни пункта на ден. На тях им е забранено да контактуват с родители, които според проповедниците са сатанинската страна, ако не признават „Църквата" на Муун".[7] За постигане на успешни вербовки сектата на Муун насочва основната част от своята дейност към провеждане на различни конференции и проекти целящи постигането на мир и издигане на семейните ценности, което на практика дава визията, че това всъщност не е църква, а ядро от неправителствени организации.[8] Обикновено Обединителната църква на Муун се представя за обществена и социална организация. Кандидатите биват канени на лекции или семинари, на които са обграждани с изключително внимание и получават предложения за съвместни лагери. На тези лагери обаче хората биват натоварени с много лекции, дава им се и много литература, така че те да не могат да осмислят всичко веднага. Отново се демонстрира внимание и доброжелателство, като целта е хората да пожелаят да се пренесат да живеят в комуните. Там психическата обработка продължава, като се използват и такива методи като ограничаване на съня, внушаване на чувство за вина и страх. Целта е да се стигне до идеята, че вън от комуната е невъзможно да се живее и че трябва да се изпълнява безпрекословно волята на „татко Муун". Членовете на сектата живеят в условията на почти военизирана йерархична пирамида. По-напредналите стават пастири. [9]

Централно място в религиозната практика на мунистите заема церемонията „Благословията", която включва в себе си „церемония на святото вино" и „свещеното бракосъчетание, разбиращо се като рождение за нов живот посредством изчистване на първородния грях и едновременно с това като встъпване в „благословен" брак. „Благословението" се провежда едновременно за много двойки превръщайки го в зрелище. Бракосъчетанието е предшествано от ангажимент като правилото е мунистите да доверят избора на своята бъдеща съпруга на Муун с което често се занимават опитните членове на „Църквата на обединението" или религиозните лидери.[10] Въпреки факта, че Благословията често се възприема само като сватба е много по значимо от предшестващото „свещено бракосъчетание" и „церемонията по свято вино" или ритуала за смяна на родословието, чиито участници, пиейки специално приготвена напитка, са жизнено свързани с Муун и семейството му. Същността на винената церемония следователно се състои в пречистването на „замърлената кръв" от сатанинското влияние, и за това тя използва „вино, което съдържа двадесет и един вида вещества, а също и кръвта на Отец и Майка". В същото време човек, който приема такова вино, по същество се отказва вътрешно от поколенията на своите

[6] Трофимчука Н.А. и Свищева М.П. „Церковь объединения (Церковь Муна)", „Миссионерство и новые культы в России, Глава из монографии „Экспансия", М, 2000г., https://psyfactor.org/expan7.htm

[7] Макарова Н., „Тайные общества и секты", часть II. Секты Раздел 4, Религии „Нового века", https://www.gumer.info/bogoslov_Buks/sekta/makar/12.php

[8] Петрова Мария, Зарибяват ни „Свидетели на Йехова", 18.03.2010г., https://arhiv.marica.bg/

[9] „Обединителна църква на Муун", („Църква на обединението". „Църква на Мун". „Мунисти"), http://www.pravoslavieto.com/inoverie/moonies/index.htm

[10] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

предци, отрича родството с тях, предпочитайки вместо тях Муун.[11] Едва след като са преминали обреда „благословение", последователите на Муун стават всъщност членове на „семейството", истинските членове на „Църквата на обединението", а самия „благословен" Муун Сан Мена се почита от мунистите като безценен дар, чиято милостиня давана от „Истинския Отец" е винаги недостойна за неговите „деца".[12]

„Църквата на обединението" не отхвърля официално нито една религия, считайки всяка една от тях, че е подготовена за пристигането на „Истинските Родители". Но именно в това становище се крие много по-дълбоко отричане, което по същество се отхвърля от мууністите, които се опитват да изключат от всяко вероучение всичко, което не е съчетано със собствената им идеология като по този начин формират своя лъжлив образ. Мууністите говорят за толерантност, но самите те са най-малко толерантната религиозна група признавайки другите религии само като подготвителни стъпки за приемането на „Божествения принцип", „Църквата на обединението" изгражда отношенията си с тях само на тази основа. Муун определя своето разбиране за ролята на християнството: „Бог е приготвил християнството като втори Израел, като основание, на която може да дойде вторият Месия. Да се постави такава основа е задача на християнството. Крайната цел на християните по света е да приемат Месия (Муна)". Замяната на християнството с мууниъм има, като по мнение на мууністите, свещената задача на човечеството, и по-специално на християните: „Това е надеждата на християнството - да познаваме, приемаме и приемаме Господа на Второто пришествие." Мууністите ценят своята съдба толкова високо, че считат себе си за по-свещени от Самия Бог. Вдъхновявайки своите последователи, Муун е заявил: „Всички светии, включително Исус, трябва да ви уважават, защото дори Исус не може да върши работата, която вършите сега."[13]

През 1954 година Преподобният Муун основава в Сеул „Асоциация на Светия Дух за обединение на световното християнство", която само за 10 години се развива по цяла Корея. Това предизвиква вълна от негативност от страна на нетолерантни фанатизирани християни. През 1965 учителят Муун изпраща мисионери в 120 страни. В края на 1971 година Сан Мьон Муун се премества в САЩ, където бързо печели последователи и бързо достига силно влияние върху Американския обществено политическия живот. През 1995 г. тя прераства в Семейна Федерация за световен мир и обединение - Неправителствена организация с признание в ООН. Днес организациите му са развити в над 200 държави и обхващат дейност във всички свери на човешкия живот[14], като Муун не се смята само за религиозен водач, но и за обединител на човечеството. Той организира Обединително движение, което обхваща най – различни организации. Според списък, представен през 1997 год., движението включва 60 организации, от които 10 са религиозни, 5 - политически, 10 от областта на културата, науката и изкуството, 7 медийни, 3 младежки, 2 женски и 3 спортни. Към обединението са включени издателство „Вашингтон Таймс", 8 университета, институти, училища, благотворителни организации. [15]

---

[11] Кузнецова Т., „Церковь Объединения» как ядро Движения Объединения Сан-Мен Муна", Доклад прочитанный на конференции „Православие, современное общество и тоталитарные секты", г. Клин Московской обл., 25-26 марта 1996 г., http://www.odinblago.ru/sektovedenie/cerkov_obiedeneniya/

[12] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

[13] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

[14] Какво не знаем за „Обединителна църква на Муун", http://istinski.blogspot.bg/2011/03/blog-post_09.html

[15] „Обединителна църква на Муун", („Църква на обединението". „Църква на Мун". „Мунисти"), http://www.pravoslavieto.com/inoverie/moonies/index.htm

Ядрото и жизнена сила на Обединителното движение е Асоциацията на Светия Дух за обединението на световното християнство (АСД-ОМХ) което стана известно като „Църквата на Обединението" (ЦО). Всички останали организации съществуват и действат единствено благодарение на Църквата на обединението, като проектите, които те изпълняват, се финансират, организират и често се изпълняват от членове на АСД-ОМХ. Сред всички сдружения, основани от Сан Мьон Муун, трябва да се споменат няколко важни: Междууниверситетска асоциация за изследване на Принципа („CARP"); Международният фонд за образование (МФО) - издава учебни пособия „Моят мир и аз"; Междурелигиозна федерация за мир по целият свят; Международен религиозен фонд; Международната федерация на жените за мир по целия свят; Международна федерация на семействата за мир по целият свят; Академия на професорите за мир по целият свят; Международен културен фонд; Световна асоциация на работещите в средствата за медийна информация, като към тях има десетки различни фондове, федерации и асоциации. Освен това Движението на Асоциацията притежава предприятия за машиностроене, корабостроене и преработка на риба и друга високотехнологична индустрия, включително производство на части от военно оборудване и оръжие, два университета, вестници и списания, включително „Вашингтон таймс", училището за изкуство „Малки ангели" и много други.[16]

„Църквата на обединението" е с изразена йерархична структура с пълно подчинение на Муун.[17] В книгата „Империя на „Преподобния Муун" е представена схема на официалната структура на сектата, разработена от самия Муун или от най-близкото му обкръжение. Според схема, Вътрешния кръг е самият Муун, който е „Истинският човек" и „Господин (Господ) на Второто пришествие", следващият кръг е „Истински родители" (Муун със своята съпруга), кръгът зад тях са техните 13 деца („Истинско семейство"), след това „Клуб на зетя" - 13 деца със съпруги и съпрузи. След това са 36 първи двойки, които се ожениха с „благословията" на Муун (те същевременно са и „Ръководещата група"). След това останалите са „благословени двойки", CARP, щатни сътрудници и други членове на църквата, като с този кръг завършва „Църквата на обединението" и започва „Обединително движение", в което влизат предприятията на Муун, множество организации и фондации, основани от него - асоциирани членове на сектата. Самите мунити подреждат членовете на „Обединителното движение" на „симпатизанти", „участващи" и „под влиянието". Но все пак всички тези кръгове имат един център - това е техният „Истински баща" и „нов Адам", „Преподобния" Муун.[18]

Ръководителите извършващи каквато и да е дейност в „Църквата на обединението" се наричат „централни личности" и по отношение на тях от „по-младите" се изисква безусловно послушание, „любов и служение". По този начин надеждно се гарантира единството на преценката, като мууністите предпочитат основно юноши и девойки, които са порядъчни, скрити и неуверени в себе като рядко използват кадри от средите на хората с „бунтовно" настроение. В учебника по „вербуване" се казва: „Трябва да впечатлим хората с нашето спокойствие, нашата самоувереност и концентрация ... Трябва дълбоко да вярваме в това, което казваме, да говорим с особено убеждение ... Трябва да сме психолози и да можем да четем по лица". Във връзка с предходното, повечето от младите членове на

[16] Кузнецова Т., „Церковь Объединения" как ядро Движения Объединения Сан-Мен Муна", Доклад прочитанный на конференции „Православие, современное общество и тоталитарные секты", г. Клин Московской обл., 25-26 марта 1996 г., http://www.odinblago.ru/sektovedenie/cerkov_obiedeneniya/

[17] Сектовед - сайт о сектах, лжеучениях, и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

[18] Гандоу Т., „Империя „преподобного" Муна", http://www.orthedu.ru/books/sects/moon/8.htm#8_2

„Църквата на обединението" живеят в специални общежития на центровете с отделяне от „сатанинския свят", като те напълно са се отдали да служат на „Истинските Родители". Тези, които идват в „Църквата на обединението", трябва радикално да се променят, да се откажат от всички предишни навици и привързаности (понякога това служи като своеобразни методи - например, от новите се искат да сменят своя гардероб или прическата си). Изменението на човешката личност се способства от обстоятелството, че муунистът живеещ в центъра, практически никога не остава сам със себе си, което пречи на критическото мислене в него. [19]

Според Н.Кривлевская[20] в пресата многократно се е появявала информация за тесните връзки на Муун с южнокорейските разузнавателни служби. В подкрепа на предходното се явява и даденото потвърждение от бившият началник на управление „С" при ПГУ КГБ СССР Ю. Дроздов според което „Църквата на обединението" на Муун е била създала две Централни разузнавателни управление – южнокорейско и американско, а в структурата на тази религиозна организация има подразделения, занимаващи се с оказване на помощ на народи водещи въоръжена борба…. В подкрепа на тази теза са и съществуващите убедителни индикации, че движението на Муун придобива политическата окраска единствено в Южна Корея при подготовката и провеждането на държавен преврат през 1961 г. и укрепването на установения по това време режим на генерал Парк Йонг Хи. В края на 50-те години, „посланието" на Муун бе благоприятно прието от четирима млади корейски военнослужещи говорещи английски език като всички те, след 1961 г., осигуриха важните връзки с корейското правителство. Единият от тях Бо Хи Пак влиза през 1950 г. в така наречената РОК-армия. Хан Сок Кок, поддръжник на Муун от края на 50-те години, е личен асистент на Ким Йонг Пил, духовният ръководител на преврата от 1961 г. и основател на Южнокорейското ЦРУ... След преврата от 1961 г. Ким Йон Пил основава Корейското ЦРУ и ръководи формирането на политическите основи на новия режим. През февруари 1963 г. докладът на ЦРУ на САЩ доказва, че Ким Йонг Пил е организирал „Църквата на Обединението", като директор на Южнокорейското ЦРУ и го използва като „политически инструмент". Във всеки случай, има ясни доказателства, че ръководството или влиянието на корейската тайна служба на Корейското ЦРУ продължава до 70-те години. Така например, Южнокорейското ЦРУ подстрекава организирането от движението на Муун на анти-японски демонстрации в САЩ на 12 септември 1974 г., което самото Корейското ЦРУ за кратко време спира, за това Муун сравнително директно говори в изнесената си реч от 22 септември 1974 г. Анализът на сегашната ситуация позволява да се предположи съществуването на връзките на „Обединителната църква" на Муун с Южнокорейския ЦРУ и сега.

Сред приближените на Муун се отличава упоменатия Бо Хи Пак — висш високопоставен служител на южнокорейското ЦРУ, след това военно аташе във Вашингтон, оглавил при Муун вестник на движението „Вашингтон таймс", а също така и пресгрупа „Ню Уорлд Коммюникейшънс". Пенсионираният офицер от разузнаването довел в движението на Муун много свои колеги, които не се притеснявали да имат редовни контакти с американските специални служби. Известният френски експерт Гилбърт Пикар в своето аналитично проучване „Адски секти" отбеляза, че с появата на полковник Пак и неговите кадри в сектата в служба на Муун са били използвани от всички разклонения на ЦРУ, а сектата е станала отлично прикритие за секретни агенти от висок ранг. В резултат както ЦРУ намери своя интерес в сектата, така и Муун намери своя интерес в ЦРУ, като по

[19] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)", http://www.sektoved.ru/enciclopedia.php?cat_id=39

[20] Кривельская Н., „Шпионы в религиозной одежде", http://old.nasledie.ru/oboz/N05_98/5ST20.HTM

този начин сектата намери подкрепа в най-мощната организация в Америка гарантираща й невидима експанзия на сектанти към различни страни.[21]

Обединителната църква навлиза организирано у нас след 1989 г., използвайки прикритието на Студентска благотворителна организация – КАРП, Професорска академия за мир в света и Международна асоциация за религиозно изследване на общочовешките ценности. Тя създава и няколко свои сдружения у нас в периода 1992-1997: Междууниверситетска организация за изследване на принципа, Женска федерация за мир в света, Българска асоциация на доброволците, Българска федерация по уънхуадо, Фондация „Ашока", Семейна фондация за световен мир и единство. [22]

През 1991 година е учреден образователен център „Логос", който започва да проповядва учението на Муун. Закрит е през 1995 г. след опит да бъде убита 24-годишна сектантка. Чрез различни организации, Обединителната църква създава свои структури в страната. [23]

През 1992 и през 1994 г. на Обединителната църква е отказана регистрация у нас. През 1995 г. е отнета и регистрацията на КАРП. Мууністите обаче имат известно влияние у нас, за което свидетелствуват и участието на българи в организираните масови брачни церемонии. През 1994 г. 12 българи са се венчали в Сеул по този начин. През 1997 година 25 български брачни двойки участват в такъв ритуал във Вашингтон, а няколко десетки сключват брак чрез Интернет. [24]

Според председателя на Центъра за проучвания на нови религиозни движения професор Иван Желев, Църквата на Муун, се цели във високите етажи на властта. Тя има привърженици сред интелектуалците, хората от научните среди в университетите, стига дори до съветници на правителствено равнище.[25]

На 27 януари 2011г. Европейският съд по правата на човека в Страсбург (ЕСПЧ) осъжда България за нарушаване на правото на религиозна свобода на членовете на Обединителната църква на Муун по дело „Бойчев и други срещу България" с Жалба №77185/01 за това, че на 6 април 1997г. няколко полицейски служители са влезли по време на мероприятие на Семейната федерация на преподобния Муун, която е официално регистрирана в България. [26] По време на нахлуването полицията иззема голямо количество книги, документи и видеоматериали. [27]

Обединителната църква не е официално регистрирана в България като вероизповедание, но е „регистрирана през януари 2002 г. като сдружение – Семейна федерация за световен мир и обединение, по новия Закон за юридическите лица с нестопанска цел" като сдружението си поставя за цел постигането на мир и единство в света чрез възпитаване на зрели и хармонични личности в здрави и стабилни семейства[28].

---

[21] Кривельская Н., „Шпионы в религиозной одежде", http://old.nasledie.ru/oboz/N05_98/5ST20.HTM

[22] http://religiabg.com/

[23] „Обединителна църква на Муун", („Църква на обединението". „Църква на Мун". „Мунисти"), http://www.pravoslavieto.com/inoverie/moonies/index.htm

[24] http://religiabg.com/

[25] Желев И. „15 опасни секти има у нас", 20.11.2018г., https://dnes.dir.bg/obshtestvo/-5238602

[26] Европейският съд по правата на човека в Страсбург осъди България за нарушаване на правото на религиозна свобода. www.BGHelsinki.org. Посетен на 30.12.2019г.

[27] Шишманова Т., „Лукавият си прибра „преподобния" Муун", национален информационен портал „Атака", 17.10.2018г., http://www.vestnikataka.bg/2012/09/лукавият-си-прибра-преподобния-му-2/

[28] Европейски съд по правата на човека, „Бойчев и други срещу България", Окончателно решение по Жалба № 77185/01, Страстбург, 27./04/2011г.

3. Заключение

В обощение на гореизложеното могат да се изведат следните изводи:

- осъществяваната дейност от страна на „Църквата на Муун” е заплаха за националната сигурност по направление духовна сигурност и по направление чужди разузнавателни служби (свързана е с централните разузнавателни управления на Корея и Америка).

- „Църквата на Муун” не развива дейност като вероизповедание, тъй като няма дадена регистрация от Дирекция по вероизповеданията при министерски съвет на Р България, а като като регистрирано сдружение.

ЛИТЕРАТУРА:

[1] Миссионерско-Апологетический проект Кистине, „Движение объединения” Сан Мен Муна, Русские юноши и девушки клянутся в верности „истинным родителям” Муну с женой и „истинному отечеству” Корее”, Секты / „Церковь Объединения“ - секта Сан Мен Муна, http://www.k-istine.ru/sects/moon/moon_about.htm

[2] Н.А. Трофимчука, М.П. Свищева „Церковь объединения (Церковь Муна)”, „Миссионерство и новые культы в России, Глава из монографии „Экспансия”, М, 2000г., https://psyfactor.org/expan7.htm

[3] Сектовед - сайт о сектах, лжеучениях,и деструктивных культах „Церковь Объединения (движение Муна)”, http://www.sektoved.ru/enciclopedia.php?cat_id=39

[4] Н.Макарова, „Тайные общества и секты”, часть II. Секты Раздел 4, Религии „Нового века”, https://www.gumer.info/bogoslov_Buks/sekta/makar/12.php

[5] М. Петрова, Зарибяват ни „Свидетели на Йехова”, 18.03.2010г., https://arhiv.marica.bg/

[6] „Обединителна църква на Муун”, („Църква на обединението”. „Църква на Мун”. „Мунисти”), http://www.pravoslavieto.com/inoverie/moonies/index.htm

[7] Т. Кузнецова, „Церковь Объединения» как ядро Движения Объединения Сан-Мен Муна”, Доклад прочитанный на конференции „Православие, современное общество и тоталитарные секты”, г. Клин Московской обл., 25-26 марта 1996 г., http://www.odinblago.ru/sektovedenie/cerkov_obiedeneniya/

[8] Какво не знаем за „Обединителна църква на Муун”, http://istinski.blogspot.bg/2011/03/blog-post_09.html

[9] Т. Гандоу, „Империя „преподобного” Муна”, http://www.orthedu.ru/books/sects/moon/8.htm#8_2

[10] Н. Кривельская, „Шпионы в религиозной одежде”, http://old.nasledie.ru/oboz/N05_98/5ST20.HTM

[11] Шишманова Т., „Лукавият си прибра „преподобния” Муун”, национален информационен портал „Атака”, 17.10.2018г., http://www.vestnikataka.bg/2012/09/лукавият-си-прибра-преподобния-му-2/

[12] Желев И. „15 опасни секти има у нас”, 20.11.2018г., https://dnes.dir.bg/obshtestvo/-5238602

[13] Европейски съд по правата на човека, „Бойчев и други срещу България”, Окончателно решение по Жалба №77185/01, Страстбург, 27./04/2011г.,

[14] Европейският съд по правата на човека в Страсбург осъди България за нарушаване на правото на религиозна свобода. www.BGHelsinki.org. Посетен на 30.12.2019г.

[15] http://www.chitatel.net/forum/topic/6606

[16] http://religiabg.com/

Име на автора: д-р Тихомир Иванов Солаков
Месторабота: ВТУ „Св.Св.Кирил и Методий“, Факултет по „Философия“, катедра „Национална сигурност“
E-mail: tihi35@abv.bg

OPPORTUNITIES FOR IMPROVING THE CRISIS MANAGEMENT PROCESS IN THE REPUBLIC OF BULGARIA

STANIMIR S. STANCHEV

ABSTRACT: *In the modern and technological world, there is no area of public life that is protected and guaranteed from ongoing crises. Crisis events occur periodically and irreversibly, because the crisis is a prerequisite, an element of evolutionary development, as related to human activity. The higher the evolutionary development, the more often man and social systems fall into a state of crisis. Therefore, experts in various fields of science define crises as natural, environmental, technological, socio-political and others. This report examines the phases of the NATO Crisis Management Process (NCMP) and offers guidelines for its improvement.*

KEYWORDS: *Comprehensive approach, NATO, operations planning.*

ВЪЗМОЖНОСТИ ЗА УСЪВЪРШЕНСТВАНЕ НА ПРОЦЕСА НА УПРАВЛЕНИЕТО ПРИ КРИЗИ В РЕПУБЛИКА БЪЛГАРИЯ

СТАНИМИР С. СТАНЧЕВ

АБСТРАКТ: *В съвременния модерен и технологичен свят не съществува област на обществения живот, която да е защитена и гарантирана от случващи се кризи. Кризисните събития се случват периодично и необратимо, защото кризата е предпоставка, елемент на еволюционното развитие, както свързано с дейността на човека. Колкото е по-високо еволюционното развитие, толкова по-често човекът и обществените системи изпадат в състояние на криза. Поради това специалистите в различните области на науката определят кризите като природни, екологични, технологични, социално-политически и др. В настоящия доклад са разгледани фазите на процеса на управление при кризи в НАТО и са предложени насоки за неговото усъвършенстване.*

1 Въведение

Средата за сигурност в наши дни е комплексна и заплахите пред нея са многовекторни. Кризите и конфликтите се случват и се разпростират като правило не само на територията на една държава, а обхващат цели региони и в кратки срокове могат да се разпространят по цялата планета[1].

В този контекст, организацията и функционирането на националната система за управление на кризи следва да бъдат постоянно изменяни и настройвани към проявленията на заплахите по отношение не само на националната сигурност като самоцел, но и като част от единните системи и подходи за управлението на кризи в НАТО и в Европейския съюз.

За да бъде отговорът на такива кризи адекватен и навременен[2-7] и за постигане на удовлетворителни резултати за цялото общество, е необходимо прилагането на всеобхватния подход по отношение на националната система за управление на кризи, да се анализират и определят средствата и механизмите за нейното оптимизиране във всички сфери, аспекти и проявления на инструментариума, с който борави националната мощ.

Необходимостта от прилагане на всеобхватния подход при управление на кризи в нашата страна допълнително се обуславя и от поетите международни ангажименти и

участието в организации, имащи водеща роля в опазването на глобалния мир и сигурност.

В настоящия доклад ще бъдат потърсени отговори на въпроси, свързани с процесите, конкретните задължения, нивата на планиране и отговорности на министерствата, ведомствата и дружествата, гражданските и неправителствените организации, изграждащи гръбнака на Националната система и органите за управление при кризи и способностите своевременно, адекватно и всеобхватно да планират и провеждат съвместни операции и дейности в отговор на кризи от всякакъв характер.

2 Организация на националната система за управление на кризи.

Основните рискове и заплахи за възникване на кризи от военен характер за нашата страна могат да бъдат породени от влошаване на отношенията с други държави или с терористични организации и образувания, представящи се за държави, участие във въоръжен конфликт във връзка с принадлежността на Р България към международни организации като ООН, ЕС и НАТО и не на последно място – открит военно-политически конфликт с държава-членка на някоя от изброените организации. Оценката на съюзно ниво за вероятността от настъпването на подобни събития варира от малка до незначителна, което ограничава подготвяния от държавата отговор до обхвата на ВС, както и до изброените в Закон за отбраната и въоръжените сили на Р България (ЗОВС)[3-5] невоенни организации с възложени военновременни задачи. Точно в това направление липсва всеобхватност на подготвяния отговор, законодателната норма дава насоки за работа „на парче“, липсва спойката между подготвяните от организациите планове[8]. Тази спойка би могла да се реализира чрез съвместяване на подготовката и действията по овладяване на кризи на отделните участници, както и в изграждането на структури на оперативно ниво[9], в които да има представители с необходимите експертни познания и управленски опит.

Невоенните потенциални източници за възникване и развитие на обществено значими кризи, които може да ангажират участието на военен компонент включват земетресения, наводнения и свлачища, пожари и засушаване, невзривени бойни припаси, а така също и от терористични действия и масово навлизане на лица, търсещи временна закрила в страната, кибератака и/или инцидент с различен приоритет и други фактори.

За наблюдение, оценка, прогнозиране, планиране, ранно предупреждение, предотвратяване, максимално ограничаване на негативните последствия и бързо възстановяване на функционирането на държавния и обществен живот при възникване на криза, Република България следва да изгражда и развива *Национална система за управление на кризи*.

Съгласно приетите в нашата страна стратегически документи[6,7], Националната система за управление на кризи е **предназначена** и се изгражда със задача да осигурява действията по предотвратяване, овладяване и преодоляване на последиците от кризи на територията на страната или извън нея - при изпълнение на задължения, произтичащи от международни договори, по които Република България е страна[1]. Тя се изгражда на централно и на териториално ниво.

За да изпълни своето предназначение, Националната система за управление на кризи трябва да отговаря на определени изисквания, като осигуряване на възможност за наблюдение, анализ и оценка на риска и на потенциално опасните обекти и дейности;

[1] Национална отбранителна стратегия на Република България, т. 65-67, София. 2016.

осигуряване на готовност за действие и способност за своевременно реагиране при кризи; изграждане на единна комуникационно-информационна система и др.

Само по себе си управлението на кризи е съществен елемент от националната сигурност на нашата страна и включва дейности като прогнозиране развитието на кризи и предварително планиране; анализ на кризите и определяне на алтернативи за реагиране; след-кризисно възстановяване и др.

За да функционира правилно системата за управление при кризи трябва да бъде включва в себе си някои от следните принципи: единна система за разрешаването на всички кризисни ситуации; съчетаване на ведомствените системи от органи, сили и средства с териториалните принципи на управление; отговорност на длъжностните лица за разработването на плановете за управление при кризи и готовността на подчинените им органи, сили и средства за действие в условия на кризи; и не на последно място финансиране от държавния бюджет на дейностите по изграждането и финансирането на цялостната система за управление при кризи.

3 Възгледи на прилагане на всеобхватния подход при планиране на операции в националната система за управление на кризи

а.Когнитивни възгледи

Прилагането на всеобхватен подход е в състояние да осигури синхронизиране на дейността на екипите, изпълняващи различни задачи, да подреди приоритетите и да установи подходящата за всеки отделен случай йерархия. И ако в нашата страна на стратегическо ниво се наблюдава някаква институционализация и концептуална подреденост, оперативното ниво, което е двигател на всяка операция по управление на криза, може да бъде значително оптимизирано, ако в неговия обхват се намери място за прилагане на всеобхватния подход.

Теоретично, основните **принципи на всеобхватния подход** в НАТО се свеждат до:

- активно взаимодействие и премерена инициативност;
- колегиалност и споделени отговорности;
- мислене и планиране, базирани на крайното състояние (ефекта);
- взаимно уважение по отношение на свободата за действие и налаганите от средата ограничения в комуникацията.

Важно е разбирането, че *всеобхватният подход не се стреми към постигане на единство на усилията, а обединяване около общата цел* (обикновено определена от държавното и политическото ръководство) за разрешаване или ограничаване на кризата и последиците от нея.

Постигането на обединение около общата цел е възможно при споделянето на общи ценности. Нормално, в основата на всяко решение за използването на НАТО за овладяване на криза където и да е по света, би следвало да са указаните във Вашингтонския договор защита на свободата и независимостта на страните-членки, както и произтичащите от тях свобода на личността, демократичност, човешки права и върховенство на закона, които са общи ценности на почти цялата международна общност. НАТО, в този ред на мисли, се явява естествен избор, когато е необходим партньор, който има развити военни способности. По същия начин, за подпомагане на провеждането на операцията,

Успешният всеобхватен подход *зависи от привличането на голям брой участници, притежаващи широк спектър от взаимно допълващи се способности*. Широко разпространено е схващането за ключовата роля на НАТО, независимо че Алиансът е само една от участващите в управлението на кризата организации. Поради безпрецедентната си способност в кратки срокове да развърне и поддържа устойчиво военно присъствие и натрупания в управлението на кризи опит, НАТО често е единствения наличен инструмент за подготовка, водене и поддръжка на операции в отдалечени, враждебни по отношение както на климатични особености, така и на противостоящи сили зони. А това се постига чрез ежегодни различни по насоченост тренировки и учения на формированията, съставляващи Силите за незабавен отговор за текущата година по голям набор сценарии, с привличане на евентуалните партниращи организации, в зони, в които е вероятно да възникне криза, която налага операция в отговор и проверка на способностите на страната-домакин да осигури поддръжка, доколкото това е част от подписаните меморандуми.

Отвъд океана, в периода на изграждане на споменатата модерна система за управление на кризи, на всички управленски нива са проведени стимулационни игри и компютърно-подпомагани учения. Те показват редица слабости в области като оповестяване на ангажираните с кризата агенции, мобилизация, комуникационно-информационни системи и тяхната защита, логистична и административна поддръжка, информационен мениджмънт и др. В резултат на проведен операционен анализ на всички нива и на задълбочени изследвания на докладите от наблюдателите и групите за ръководство и контрол, са изведени четири **основни принципа**, на които се базира американският всеобхватен подход:

- Ограничаване на съществуващите рискове – включва набор от дългосрочни мерки за намаляване на възможността за проявление на кризата, а ако тя все пак се случи – да се намалят до минимум потенциалните загуби;
- Поддържане на готовност за реакция – обхваща дейностите, които се предприемат преди настъпване на кризата – наемане на персонал, обучение, тренировка, тестове, складиране на оборудване, изграждане на съоръжения като Оперативни центрове за спешни ситуации и най-съществения елемент – разработване на планове, които детайлно свързват всички ресурси, определени за управление на кризата;
- Отговор – комплекс от мероприятия, силно зависими от бързодействието, насочени към запазване на живота и собствеността на гражданите, оказване на помощ на пострадалите, осигуряване на безопасността и контрол на придвижването в засегнатата зона, оценка на пораженията и необходимата поддръжка, евакуиране и осигуряване на убежище на засегнатите, информиране на обществеността и заявка за оказване на помощ при липса на необходимата юрисдикция;
- Възстановяване – усилията, насочени към възстановяване на инфраструктурата и на социалния живот и обществено-икономическите взаимоотношения. В краткосрочен план се набляга на основните потребности като електроенергия, комуникации, водоснабдяване и канализация и обществен транспорт, допълнени от осигуряване на храна и облекло за нуждаещите се, а в дългосрочен – на възстановяването на икономическия живот, предприятията и повторното построяване на домовете и др.

НАТО също обръща сериозно внимание на двете страни на монетата – военния и невоенния компонент (ВК и НВК). Трите **направления**, в които се търси координация[8] и взаимодействие са: осигуряване на непрекъснатост на държавното управление; поддръжка на жизнено-важните услуги за населението; и поддръжка на военни операции от гражданския сектор. В обхвата на *Комитета за планиране на гражданските ресурси за справяне с извънредни ситуации* (Civil Emergency Planning Committee – CEPC) попадат следните **седем сектора**, които се явяват критични за осигуряване на посочените по-горе направления: непрекъснатост на работата на правителството и най-важните държавни служби и агенции; доставки на енергийни ресурси; ефективно справяне с безконтролното придвижване на големи групи хора; запаси от вода и храна; способност за справяне с масови жертви; телекомуникационни мрежи; транспортна мрежа.

В основата на „скърцащите механизми“ на Националната система за управление на кризи стоят липсата на заинтересованост на политическо ниво да бъдат погледнати процеса на управление на кризи стратегически („отгоре“). Планирането, превенцията и подготовката на компетентни органи за преодоляване на последствията от кризи не са и не могат да бъдат междуведомствена дейност. В такъв тип дейност в нашата държава, по правило основният обем работа се извършва от ведомството с основни отговорности.

Тези разсъждения предизвикват въпроса има ли Р България реално изградена система за управление на кризи? Анализът на цялостна организация като процес - органи, КИС, центрове, процедури за работа категорично доказва липсата на такава. Тя не е нормативно уредена, липсват ключови взаимовръзки. Няма централизирани ръководства и процедури, които да описват отговорностите, санкциите за бездействие и да се прилагат (не само формално) от всички субекти.

Решение на тези проблеми е създаване на държавна агенция (министерство, Център за управление). Такава стратегическа организация би имала законови правомощия в направления като, провеждане на подготовка и обучение, мероприятия по превенция, изграждане на способности, структури, система за командване, управление и комуникации. Към настоящия момент всичко това е организирано отделно и комуникацията между тях е затруднена.

По отношение на въпросите, свързани с бюджетирането и финансирането на подобна организация, е че е необходимо да има един отговорен орган, който да изпълнява всички тези дейности. Истината, обаче е, че всяка криза, която не се управлява от единен закон и е с разпръснати между ведомствата функции и отговорности по управление на съпътстващите я процеси и овладяване на последствията, винаги ще излиза много по-скъпо на данъкоплатеца след отчитане на всички направени разходи.

b. Правни аспекти

От началото на членството на Р България в НАТО е леко трудно да се каже, че България може да се счита за пълноправен член по отношение на управлението на кризи и те, за съжаление, не са изцяло позитивни. Причините, които се забелязват с на първо време могат да се обединят около следните направления:

- Спорадични опити за нагаждане на правната рамка, нерядко посредством буквален превод на съюзна документация и проста екстраполация посредством сваляне на нивото;
- Липса на единен държавнически подход при създаване на нормативната уредба, допускане всяко министерство и агенция само да определя своите

приоритети при управление на различните кризи, което създава условия за дублиране на усилия и липса на субординация;

- На национално ниво, взаимодействието с НАТО е поделено между МО и МВнР и преимуществено се отделя внимание само на два домейна – военния и дипломатическия. Липсват, обаче, ясни взаимовръзки и общ институционализиран, национален процес на планиране на отбраната и свързаните с него кодификация, стандарти и оперативна съвместимост в национален аспект, изрично разписани правила за привличане на НВК в планирането и подготовката на страната за управлението на кризи.

Негативните ефекти се подсилват от липсата на изградена по вертикала и хоризонтала система за управление - с определени, формирани и работещи органи за непрекъснато наблюдение, прогнозиране, оповестяване, оценка, предлагане на мерки, вземане на решение, планиране (предварително и последващо). Тези недостатъци не могат да се компенсират само на ведомствено ниво – легализирането и обличането в правна норма на междуведомствени щабове и структури за взаимодействие на оперативно ниво, които да подпомагат процеса на вземане на решения от държавните органи и да координират усилията на институциите по изпълнението на цялостния процес на превенция, подготовка, реакция и възстановяване би било една правилна стъпка в оптимизирането на Националната система за управление на кризи. Всичко това следва да е част от ясно нормативно разписан процес на кризисно планиране на държавно/стратегическо ниво. Само така може да бъдат привлечени всички в този процес, в т.ч. и чрез вменяване на разписани в закон ангажименти (функции) от държавата към всички ангажирани с управлението на кризи, както и към самата държава като правен субект.

Всичко описано тук очертава трите основни аспекта, в които всеобхватният подход може да окаже позитивно влияние върху управлението на кризи в нашата страна – **подобряване на нормативната база** посредством имплементиране на разгледаните принципи и универсализиране на справянето с възможните рискове и заплахи за възникване на територията на страната и в региона, **постигане на институционален интегритет** посредством изграждане на интегрирани структури на оперативно ниво, в които военни експерти заемат щатни длъжности за подпомагане на експертизата на НВК, ангажиран с разрешаването на кризи от невоенен характер и обратно – цивилни експерти да бъдат използвани при планирането, подготовката и провеждането на национална или съюзна операция за защита на суверенитета и териториалната цялост на Алианса / Р България и целево финансиране и задълбочаване на дейностите, свързани с **подготовката и обучението** на всички участници в управлението на кризи от различен характер.

Заключение

Направените в настоящия доклад предложения могат да допринесат за повишаване на ефективността на националната система за управление на кризи посредством прилагане на всеобхватния подход по отношение на подобряване на нормативната база, постигане на институционален интегритет и насочване на усилията към повишаване на обучението и подготовката на привличаните в тези процеси организации.

ЛИТЕРАТУРА

[1] Богданов, Б., Иванов, В., „Планиране в отговор на кризи от невоенен характер“, София, 2020 г.
[2] Бяла книга за отбраната и Въоръжените сили на Република България, приета с Решение на Народното събрание от 28.10.2010 г.
[3] Закон за отбраната и въоръжените сили на Р България, Обн. ДВ. бр. 35 от 12 Май 2009 г.
[4] Закон за управление и функциониране на системата за защита на националната сигурност, Обн. ДВ. бр. 61 от 11 Август 2015 г.
[5] Закон за управление при кризи, София, 2005г. - отменен с Преходни и Заключителни разпоредби на Закона за отбраната и въоръжените сили на Република България, Обн. ДВ. бр. 35 от 12 Май 2009 г.
[6] Национална отбранителна стратегия на Република България, София, 2011 г. - отменена с Решение № 283 на Министерския съвет от 18.04.2016 г.
[7] Национална отбранителна стратегия на Република България, приета с Решение № 283 на Министерския съвет от 18.04.2016 г.
[8] Георгиев В, „Повишаването на координацията и взаимодействието –основно изискване при прилагането на всеобхватния подход“, Сборник доклади от годишна университетска научна конференция 28-29 май 2020, НВУ „Васил Левски”, В Търново, ISSN 2367-7481, с. 1062-1073
[9] Фаразов Д, „Изисквания към системата за командване и управление на съвместно (оперативно) ниво“, Сборник доклади от годишна университетска научна конференция 28-29 май 2020, НВУ „Васил Левски”, В Търново, ISSN 2367-7481, с. 1182-1190

Майор ас. инж. Станимир Стоянов Станчев
Месторабота: Военна академия „Г. С. Раковски“
E-mail: s.stanchev@rndc.bg

MISINFORMATION IN THE 21ST CENTURY AND THE BOOM OF "FAKE NEWS"

KALOYAN A. ILIEV

ABSTRACT: *Misinformation is widely spread in modern societies and keeps evolving while damaging the principles of democracy. Social media and traditional media like television and newspapers distribute new information at an unseen speed which results in floods of information impossible to assimilate. Every citizen's voice can be heard but also anyone can make misleading information public. For this reason, there should be regulatory mechanisms established. In the arising era of deep fakes media competence and critical thinking are becoming more important than ever before.*

KEYWORDS: *misinformation, fake news, conspiracy, misinformation, social media, media, coping mechanisms, critical thinking, freedom of speech, public figures*

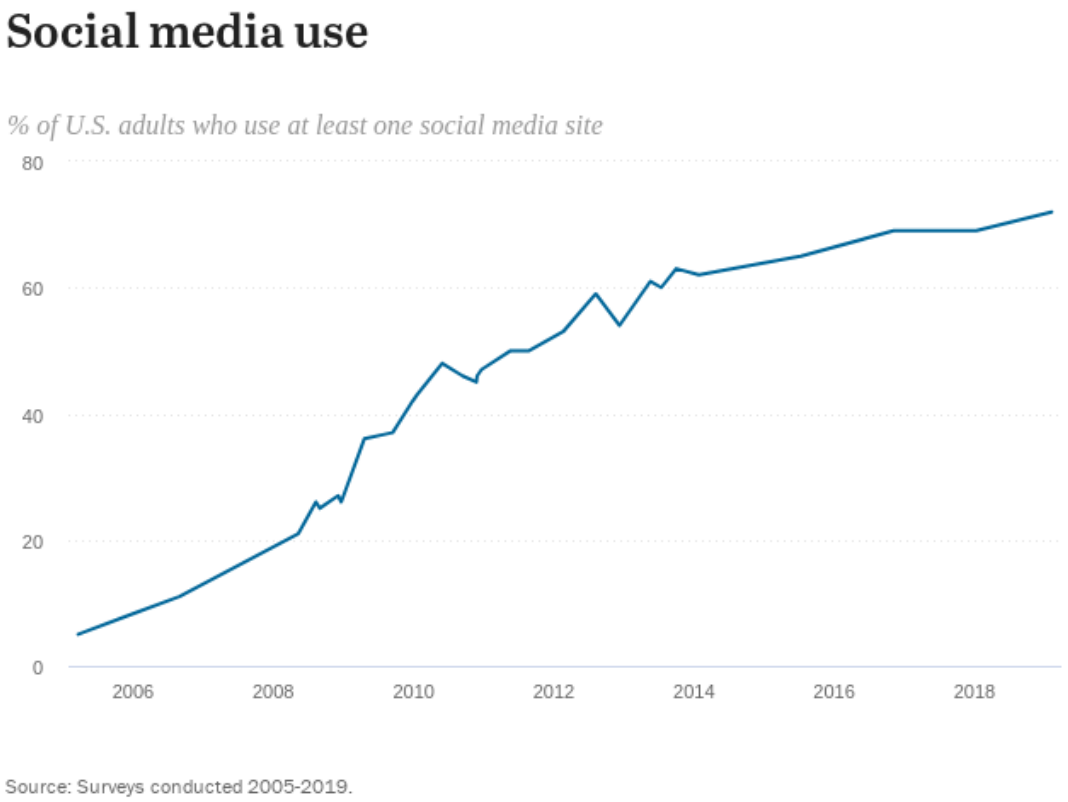
ДЕЗИНФОРМАЦИЯТА В 21. ВЕК И БУМЪТ НА „ФАЛШИВИТЕ НОВИНИ"

КАЛОЯН А. ИЛИЕВ

АБСТРАКТ: *Подвеждащата и невярната информация са широко разпространени в модерните общества и продължават да се развиват ощетявайки принципите на демокрацията. Социалните мрежи и традиционните медии като телевизии и вестници разпространяват нова информация с невиждани досега скорости, което резултира в приливи от информация невъзможни за обработка. Гласът на всеки гражданин може да бъде чут, но и всеки може да публикува невярна информация. Поради тази причина трябва да се въведат регулиращи механизми. В изгряващата ера на deep-fakes медийната компетентност и критичното мислене са все по-важни от когато и да било досега.*

Във времето на двадесет и първи век информацията и информираността на населението на планетата са по-важни от когато и да било досега. Широкото разпространение на технологии, които позволяват лесния и своевременен достъп до информация, предоставя и трибуна за лесна изява и разпространение на дезинформация сред обществата. Манипулацията на изходи от важни събития като политически избори с помощта на „фалшивите новини" е реалност, подкрепена с примери от Мианмар, Филипините и Индонезия.[1] Все повече и повече хора получават своята информация през социалните мрежи, където всеки, анонимно или не, може да изрази своето мнение или да публикува невярна информация или факти по определена тема без никаква научна обоснованост. Борбата с дезинформацията е много трудна поради възможността за ощетяване на демократичните ценности и ограничаването на свободата на изразяване на отделните индивиди.

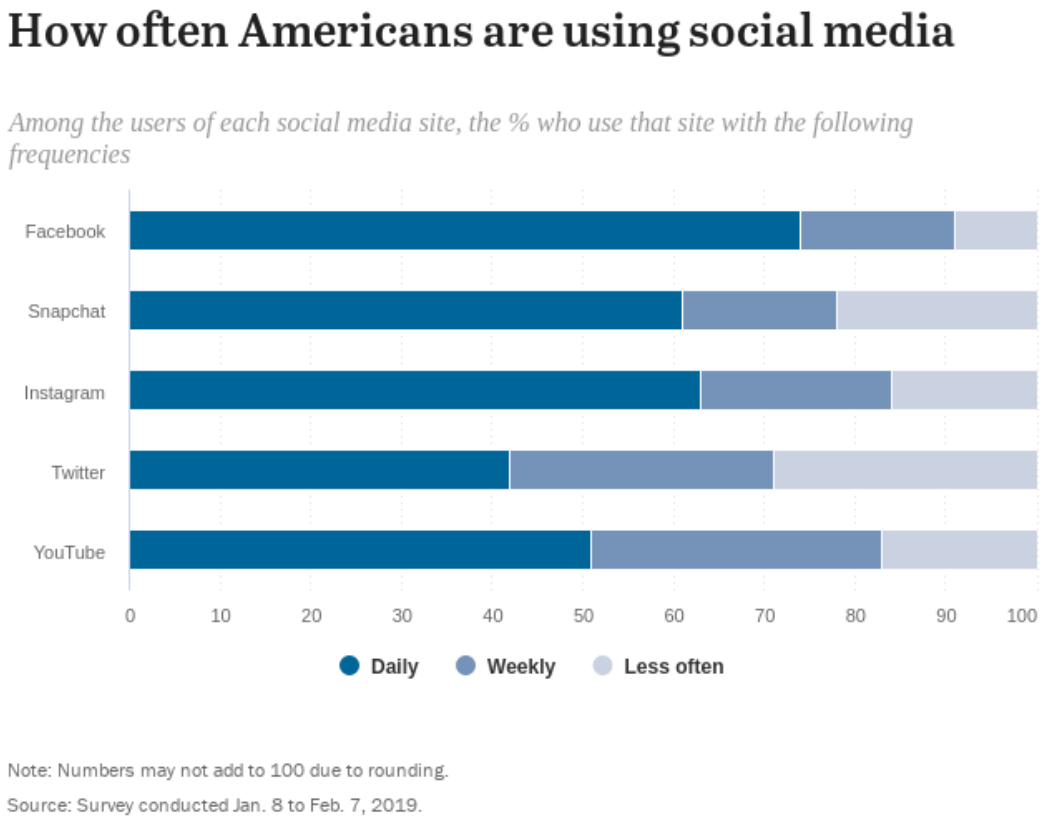
С напредване на технологиите все повече и повече стават възможностите за създаване на подвеждащи новини и факти и тяхното споделяне в интернет, до който почти всеки има достъп. Социалните мрежи няма как да не бъдат споменати като едно от най-добрите места за разпространяване на информация и лични мнения в онлайн пространството. Двете графики по-долу съответно показват каква част от населението на САЩ използва социални мрежи през периода от 2005 до 2019 година (фиг. 1) и какъв процент от хората, участвали в



анкета от 8. Януари до 7. Февруари 2019 година, използват определени социални мрежи ежедневно, поне веднъж в седмицата и по-рядко (фиг. 2).

Фиг. 1: Процентуална част на хората използващи поне една социална мрежа в САЩ през периода от 2005 до 2019 година. източник: https://www.pewresearch.org/

С помощта на графиката от фигура 1. се забелязва колко голяма част от населението използва поне една социална мрежа и как тази част не спира да нараства. Това е голям проблем в сферата на журналистиката и достигането на факти до хората, защото всеки може да влезе в ролята на журналист, но не всеки може да понесе отговорност като такъв и да представи информацията си по неутрален начин и да покаже няколко гледни точки на това, което иска да предаде. Информация, зад която не заставаме с името си и за която не поемаме отговорност, е много по-лесна за споделяне и бързо разпространяване в социалните мрежи. Проблемът тук е, че в много случаи разпространението на невярна информация, която поражда съмнения в по-късно представената вярна информация, се случва първо. Много медии, които претендират за сериозност и достоверност, всъщност копират информацията си от други, без да я проверяват. Един от последните примери е разпространението на стари кадри към нови събития, свързани с протестите на движението Black lives matter [15], което още веднъж показва колко лесно се постига заблуда и каква е нуждата от достатъчна медийна компетентност. Увеличението на използващите социални мрежи само по себе си не е достатъчно за да се потвърди значението на публикуваните там новини. От друго проучване на Pew Research Center става ясно, че 55 % от възрастните американци през 2019 г. „често“ или „понякога“ научават за новините от социалните мрежи.[8] С помощта и на следващата диаграма (фиг. 2) може да се забележи огромното значение на социалните мрежи като Facebook, които около 72% от възрастните използват ежедневно.



Фиг. 2: Колко често американците използват определени социални мрежи. източник: https://www.pewresearch.org/

Друг проблем със социалните мрежи е монополизацията на бранша. Много от основните медии, които се използват в Европа принадлежат на Facebook, от който сравнително често изтичат големи количества лични данни.[5] На много пъти се оказва, че данни, които по декларация не се събират или се изтриват, всъщност се съхраняват[16].

Информационният дигитален век предразполага създаването на паралелна реалност и инструментаризацията си като средство за манипулация предвид факта, че зад много големи медии стоят близки до политиката лица, които придобиват силата да манипулират големи групи (пример: Пеевски, България). Подобни факти се превръщат в обществена тайна и биват неглижирани, а липсата на голяма медийна опозиция задълбочава проблема, защото липсва алтернативна медия. България все още е на 111. място по свобода на словото.[6]

Ефектът на дезинформацията се характеризира с това, че новоприета информация замества стара такава и възпрепятства нейното спомняне. Повтарянето на една и съща информация има способността да заличи стара, дори новата да е грешна, а старата вярна. Без значение дали човек е запознат с определена тема повтарянето на една и съща невярна информация би могло да замести утвърдените знания.[9] Подобен ефект представлява и confirmation bias (утвърдителна склонност) - както става ясно от самия термин, това представлява склонността да търсим, интерпретираме, предпочитаме и спомняме потвърдителна информация за собственото си мнение. Пример за това са набиращите популярност и привърженици клубове на Flat-Earthers (Плоскоземци), които поддържат конспиративната теория, че земята е плоска и в същото време подкопават авторитета на

науката. В много от случаите чувството за безпомощност и безсилие, за нищожност и страхът са водещи в образуването на алтернативни факти, от които произлизат конспиративните теории. Названието алтернативни факти само по себе си е парадокс и е в разрез с науката. Факт означава определена даденост да бъде непоклатима и доказана множество пъти. В този смисъл алтернативните факти навеждат на мисълта, че не става въпрос за реалността, а за паралелен свят. Хората, вярващи в конспиративни теории, не са откъснати напълно от реалността, но в някои отношения са оттласкани в отделни нейни измерения. При конфронтиране с обратна аргументация те се позовават на отричащи емоционални твърдения от типа на „Всички журналисти са купени.“, „Всички медии лъжат.“.

В технологичната ера, в която живеем има възможност за създаване на собствен сайт, блог или подкаст. Множество сайтове сугерират сериозност чрез използване на понятия като новини, новости, наука, Европа, и домейни .com, .org, .net. Заглавията на техните статии най-често са шокиращи или преувеличени, за да привличат колкото се може повече внимание и кликове към на страницата, които генерират средства (кликбейт). Част от хората не притежават достатъчната медийна компетентност и критично мислене за разпознаване на фалшивата информация. Дори индикатори като неправилна пунктуация, правопис или словоред не ги подсещат. В социалните мрежи друг фактор е лицето, което споделя информацията. Поради невъзможност за проверка на източниците и информираност за всичко и всеки по всяко време получателите на информацията я приемат за истинна, ако тя е разпространена от авторитетно за тях лице. Така например някои професори са провеждали своите социални експерименти чрез проследяване на реакциите върху споделяния на фалшиви новини в профилите си. Много хора нямат време и желание за прочитане на цяла статия и предпочитат просто да реагират или споделят според заглавието, така че то е изключително важно като квинтестенция на съдържанието. [10] Ключова компетентност на модерното време е критичното мислене, с което Финландия се опитва да снабди всеки един от своите жители още в училищния му период и успява доста успешно според световните класации. [7]

Сравнително нов начин за манипулация на медийната информация е така наречената технология за създаване на Deep-Fakes на хора. Тази технология позволява автентично използване на глас, физика и маниери на която и да е личност. За създаването им е нужна база данни с достатъчно видео и аудио материали на съответната личност. [3, 4]

Оттук изниква въпросът за възможните механизми, чрез които да се противодейства на умишлената дезинформация. Най-ефективно е образованието като инструмент за обучение на критично мислещи и отсяващи граждани. Фундаменталният проблем в този подход е, че не всички слоеве на обществото имат еднакъв достъп до образование. Друго слабо място е, че това е двустранен процес - колкото по-добри стават гражданите в разпознаването на лъжлива информация, толкова по-истинно биват представяни фалшивите новини. Затова неизменно се стига до дилемата дали трябва да се въведат контролни органи, които да забраняват и премахват фалшивата и подвеждаща информация. Дали трябва да има само определени платформи, на които може да се вярва или пък е по-добре да се въведе изкуствен интелект, който да контролира съдържанието в интернет и да предупреждава потребителите за възможни лъжи и преиначавания.

Кога ответните мерки се сблъскват с правата за свобода на словото? Съществува определен риск контролните механизми да бъдат използвани от влиятелни фигури, например политици, в тяхна полза. Пример за това е Китай с неговата цензура. Тя е инструмент за политическа пропаганда и задържане на властта. Най-новият пример е

опитът за прикриване на новината за новия коронавирус, за който се спекулира, че първите случаи са били във времето между октомври и декември 2019 г. [11]

Определени събития и личности, свързани с тях, получават голямо медийно внимание и поради позициите им в обществото, очакванията към тях са високи. Примери за това са 11. септември при управлението на Джордж Буш, смъртта на принцеса Даяна и убийството на Джон Кенеди. Твърди се, че около всички тези събития има мистериозни обстоятелства, което предразполага създаването на множество версии за тях. Това може да бъде обосновано с психиката на хората. Очаква се, че хора на високи позиции са необикновени и това се свежда и до обстоятелствата около събитията, свързани с тях.

Друг интересен признак , по който хората могат да бъдат сравнявани са белезите на тяхната култура. Българите например са индивидуалисти, но в много ситуации се приобщават към групата, пример за това е образователната система, която се основава на класове и приравнява всички ученици. Това подтиква индивидите да търсят причини и отговорност във външния свят, погледът върху нещата е по-скоро субективен. За разлика от българите, американците например са идивидуалисти във всички отношения. Те се учат на това още в училище, когато например не принадлежат на цял клас, а всяко дете има индивидуална учебна програма. Така се възпитава обективно възприятие на света и вглеждане в себе си. Българите са много по-податливи на конспиративни теории. [17]

В последно време се наблюдава тенденцията за напасване на социалните мрежи към реалността, а не обратното както досега. Пример за това са #nofilter-кампаниите в Instagram или рекламите със средностатистически хора, а не модели. Въпреки това голяма част от по-младите хора прекарват значителен процент от времето си в социалните мрежи и възгледите им за света се формират от тях. От това произлиза и желанието за промяна на външния вид от все по-ранна възраст. Много пластични хирурзи докладват, че техни пациенти и пациентки искат да изглеждат както на селфитата си с филтър.[12,13] Тоест се наблюдават две противоположни развития – признаване на човешкото многообразие и приемането му и стремежът за напасване към общ идеал. Оттам произлизат разпалените спорове по контроверсни теми, като понякога се стига до вербално насилие, което отчасти се предава и в ежедневието.[14]

ЛИТЕРАТУРА:

[1] BLOOMBERG: Philippines taps fake news busters for elections, The Straitstimes, 05.05.2019 https://www.straitstimes.com/asia/se-asia/philippines-taps-fake-news-busters-for-elections [достъпно на: 15.10.2020]

[2] Pew Research Center: Social Media Fact Sheet, 12.06.2019, https://www.pewresearch.org/internet/fact-sheet/social-media/ . [достъпно на: 13.10.2020]

[3] NORTON: Deepfakes: What they are and why they're threatening, https://us.norton.com/internetsecurity-emerging-threats-what-are-deepfakes.html#politics [достъпно на: 15.10.2020]

[4] The Atlantic: The Very Real Threat of Trump's Deepfake, David Frum, 27.04.2020 https://www.theatlantic.com/ideas/archive/2020/04/trumps-first-deepfake/610750/ [достъпно на: 18.10.2020]

[5] NBC News: A timeline of Facebook's privacy issues — and its responses, Alyssa Newcomb, 24.04.2018, https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651 [достъпно на: 17.10.2020]

[6] Reporters Without Borders: 2020 WORLD PRESS FREEDOM INDEX, Reporters Without Borders, https://rsf.org/en/ranking [достъпно на: 19.10.2020]

[7] CNN: How Finland is winning the war against fake news, CNN, https://edition.cnn.com/videos/business/2019/05/17/fake-news-disinformation-education-finland-eu-russia-lon-orig-ejk.cnn [достъпно на: 18.10.2020]

[8] Forbes: More Americans Are Getting Their News From Social Media, Peter Suciu, 11.10.2019, https://www.forbes.com/sites/petersuciu/2019/10/11/more-americans-are-getting-their-news-from-social-media/#73c8ef603e17 [достъпно на: 16.10.2020]

[9] Loftus EF. Planting misinformation in the human mind: a 30-year investigation of the malleability of memory. Learn Mem. 2005 Jul-Aug;12(4):361-6. doi: 10.1101/lm.94705 Epub 2005 Jul 18. PMID: 16027179

[10] Maksym Gabielkov, Arthi Ramachandran, Augustin Chaintreau, and Arnaud Legout. 2016. Social Clicks: What and Who Gets Read on Twitter? In Proceedings of the 2016 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Science (SIGMETRICS '16). Association for Computing Machinery, New York, NY, USA, 179–192. DOI: https://doi.org/10.1145/2896377.2901462

[11] Alliance For Science: Covid pandemic might have begun as early as October, experts say, Mark Lynas, 06.05.2020, https://allianceforscience.cornell.edu/blog/2020/05/covid-pandemic-might-have-begun-as-early-as-october-experts-say/?fbclid=IwAR3rw0sqYXM4oma_X_uKweRXE0xFTmOnj93IczOqvcY7siPTriDwJ-RkKAs [достъпно на: 12.10.2020]

[12] The Guardian: Snapchat photo filters linked to rise in cosmetic surgery requests, Sam Wolfson, 09.08.2018, https://www.theguardian.com/technology/2018/aug/08/snapchat-surgery-doctors-report-rise-in-patient-requests-to-look-filtered [достъпно на: 13.10.2020]

[13] Insider: People are seeking plastic surgery to look like their edited selfies in real life — here's why doctors think the trend is 'alarming' , Lacy Yang, 07.08.2018, https://www.insider.com/plastic-surgery-selfie-filters-2018-8 [достъпно на: 13.10.2020]

[14] Карбовски, Втори план, Проект: Играчка плачка - Двете гледни точки към едно интернет запознанство, 2017

[15] BBC Reality Check: George Floyd protests: Misleading footage and conspiracy theories spread online, 02.06.2020, https://www.bbc.com/news/52877751 [достъпно на: 13.10.2020]

[16] Aimee Picchi: OK, you've deleted Facebook, but is your data still out there?, 23.03.2018, https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/ [достъпно на: 13.10.2020]

[17] Валери Найденов, „Тухла и панел“, в. „24 часа“, 15.06.2002 г.

Име на автора: Калоян А. Илиев
Месторабота: Национален военен университет „Васил Левски“, Факултет „Артилерия, ПВО и КИС“ – гр. Шумен
E-mail: kacho_78@abv.bg

CORRUPTION IN THE PUBLIC SECTOR

STILIANA G. STANCHEVA, SIBEL H. FEVZIEVA

Abstract: *Corruption is a global threat that manifests itself both in terms of the economic development of individual countries and their international relations, as well as in terms of the world economy and politics in general. The various forms of abuse of power for personal or group gain to the detriment or at the expense of the public interest are becoming especially relevant in countries in transition, which face the need to simultaneously build new democratic institutions and create the necessary prerequisites for market economic relations.*

Keywords: *corruption, public administration.*

КОРУПЦИЯ В ПУБЛИЧНИЯ СЕКТОР

СТИЛИАНА Г. СТАНЧЕВА, СИБЕЛ Х. ФЕВЗИЕВА

АБСТРАКТ: *Корупцията представлява глобална заплаха, която се проявява както по отношение на икономическото развитие на отделните страни и за международните им връзки, така и по отношение на световната икономика и политика като цяло. Различните форми на злоупотреба с власт за лично или групово облагодетелстване в ущърб или за сметка на обществения интерес придобиват особено голяма актуалност в страните в преход, които са изправени пред необходимостта едновременно да изграждат новите демократични институции и да създават нужните предпоставки за развитието на пазарни стопански отношения.*

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 доколкото 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 гореспоменатата 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.

Имена на авторите:
Стилиана Г. Станчева, фак. номер: 1870070025, e-mail: stiliana.stancheva@gmail.com
Сибел Х. Февзиева, фак. номер: 1870070022, e-mail: sibito.bis@gmail.com
ШУ „Епископ К. Преславски“, Факултет по технически науки, студенти от специалност „Системи за сигурност“, III курс.

COMPARATIVE ANALYSIS OF MODERN TERRORIST ORGANIZATIONS

NURAY M. IDAETOVA, ANASTASIYA G. HRISTOVA

Abstract: *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 widespread on all continents and equally instills fear in people regardless of their location.*

Keywords: *terrorism, terrorist organizations, terrorist attacks.*

СРАВНИТЕЛЕН АНАЛИЗ НА СЪВРЕМЕННИТЕ ТЕРОРИСТИЧНИ ОРГАНИЗАЦИИ

НУРАЙ М. ИДАЕТОВА, АНАСТАСИЯ Г. ХРИСТОВА

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.*

Ключови думи: *тероризъм, терористични организации, терористични атаки.*

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:

- 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, изигран 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.

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.

За съществуването на терористични организации и за ефективността на техните действия са необходими три условия:

- 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).

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).

Задачи на терористичните организации:

- 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, обществеици 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.

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.

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:

- 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.

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.

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.

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.

2004. 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.

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.

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.

2012. 18 юли – Атентат на летището в Бургас срещу израелски туристи. Загиват 5 човека и около 35 са ранени.

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.

2016. 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”.

2016. 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.

2016. 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.

2017. Нова година - Истанбул. Нападател, предрешен като Дядо Коледа откри безразборна стрелба в модна дискотека на Босфора. Загиват 39 души и 69 са ранени.

2017.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.

2017.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.

3 Заключение

Борбата с тероризма. 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.

ЛИТЕРАТУРА:

[1] bg.wikipedia.org
[2] www.e-dnrs.org

Имена на авторите: Нурай М. Идаетова, фак. номер: 1870070023, e-mail: nurito0o0o0@abv.bg
Анастасия Г. Христова, фак. номер: 1870070021, e-mail: anastasiqniki991@gmail.com
ШУ „Епископ К. Преславски“, Факултет по технически науки, студенти от специалност „Системи за сигурност“, III курс.

RISK MANAGEMENT IN MEGA SOT EOOD

CVETELIN D. CONEV

Abstract: *The functions assigned to the risk management system suggest the content of the management process itself, which boils down to the following actions:developing a risk management policy; risk situation analysis - identification and assessment of all threats faced by the organization. Based on the analysis and assessment of the risk, the management of the organization decides which of the risks will be accepted and which will be ignored; identification of available routes and means for risk minimization.*

Keywords: *risk assessment, risk management, prevention.*

УПРАВЛЕНИЕ НА РИСКА В МЕГА СОТ ЕООД

ЦВЕТЕЛИН Д. ЦОНЕВ

АБСТРАКТ: *Функциите, възлагани на системата за управление на риска, предполагат съдържанието на самия процес на управление, който се свежда до следните действия: разработване на политика за управлението на риска; анализ на ситуацията на риска - идентификация и оценка на всички заплахи, с които се сблъсква организацията. Въз основа на анализа и оценката на риска ръководството на организацията взема решение кои от рисковете ще бъдат приети и кои пренебрегнати; определяне на достъпните пътища и средства за минимизация на риска.*

1 Въведение

Рискът е една от най-важните категории, които изразяват мярката за опасност на определени ситуации, в които има фактори, неблагоприятно въздействащи върху човека, обществото или природата. Тази категория се използва в много науки като: обществени, природни, математически, медицински, технически и военни. В зависимост от предмета и обекта на изследване всяка от тези науки има свои специфични методи за изследване на риска. Изследването на риска предполага разкриване на неговата същност, елементи, свойства и вътрешна противоречивост[1].

Повечето хората свързват риска с опасност и заплаха, затова в много от определенията, той се описва с отрицателните си последици.

В сферата на безопасността и охраната на труда обикновено се приема, че рискът има само отрицателна страна, поради това и стратегията за управление е превенция и ограничаване на потенциалните вреди.

Рискът е вероятността от протичане на неблагоприятно събитие или процес, свързани с човешка дейност, която подлежи на рационализация и управление[2].

Директива Севезо II определя риска като „вероятността от специфично въздействие, настъпващо в рамките на определен период от време или при определени обстоятелства“. Като такъв, рискът е сложна функция от опасности, свързани с определена система.

[1] Диманова Д, Управление на риска, УИ на ШУ „Епископ Константин Преславски“, ISBN 978-619-201-095-9, 2016, с.21.
[2] Национална сигурност на България: Рискове до 2020 – 2025, с.10

Приемливостта на определени рискове зависи от много аспекти, такива като: контрол, страх, знание, доверие[3].

Съществен елемент от процедурата по разкриване на риска е определяне на факторите, които му влияят. Това са реални дейности, които оказват или са в състояние да окажат въздействие върху хода и съдържанието на процесите, имащи значение за конкретния риск.

В тази връзка целта на изложението е на база направената оценка на риска съгласно наредба № 5 в Мега СОТ ЕООД, да се планират мерки за управление на различните категории рискове на работните места.

2 Изложение

Мега СОТ ЕООД си поставя за цел да бъде максимално лоялно дружество, както за своите клиенти, така и за всички заинтересовани лица. Оценяването на риска обхваща: работните процеси, работното оборудване, помещенията, работните места, организацията на труда, използването на суровини и материали, и други странични фактори, които могат да породят риск.

Оценяването на риска се извършва от работодателя, като в него участват и служби по трудова медицина. На основа оценката на риска работодателите[4]:

- планират и прилагат подходящи мерки за предотвратяване на риска;
- осигуряват защита на работниците, служителите и лицата, намиращи се в близост до мястото на риск;
- степенуват по приоритети мерките за предотвратяване, намаляване и ограничаване на риска, като отчита установения риск, причините за възникване на опасностите, алтернативните решения и новостите по съответните проблеми, осъществимостта на решенията и възможността за инвестиции;
- осъществяват контрол за изпълнението и ефикасността на предприетите мерки.

Дейността за оценяване на риска включва утвърдена програма от работодателя за оценяването на риска, която съдържа[5]:

- организацията и координацията на дейностите по оценяването на риска;
- подходите и методите за извършване на оценката на риска, включително осигуряването на достоверност на резултатите и разработването при необходимост на подходящи за предприятието методи;
- оценителите на риска;
- необходимите ресурси за оценяване на риска;
- начините за осигуряване на информация, обучение и консултации на оценителите;
- етапите, последователността и сроковете за оценяване на риска;
- начина за допитване и консултации с работниците и служителите, работещи на или свързани с конкретното оценявано място.

В Мега СОТ ЕООД трудовите дейности са класифицирани на три основни групи, както следва:

Административни офиси - управител, счетоводство, каса:

- Административно - управленска дейност;

[3] Директива Севезо II

[4] Диманова Д, Управление на риска, УИ на ШУ „Епископ Константин Преславски“, ISBN 978-619-201-095-9, 2016, с.193.

[5] Диманова Д, Управление на риска, УИ на ШУ „Епископ Константин Преславски“, ISBN 978-619-201-095-9, 2016, с.193.

- Административни дейности и финансови операции;
- Обработка на финансово - счетоводна документация;
- Обработка и съхранение на документация, свързана с трудово право;
- Обработка и съхранение на документация, свързана с осигурителното право;
- Обслужване на видеодисплеи;
- Обслужване на офис техника - телефон, принтер и др.;
- Обслужване на касов апарат;
- Обслужване на климатик;
- Обслужване на диспенсър за минерална вода;
- Обслужване на кафемашина;
- Почистване на работните места;

Охранителна дейност - автопатрул, физическа охрана, диспечери, техници:

- Мониторинг и реакция на автопатрулни сили;
- Мониторинг на обекти - охрана с видеонаблюдение на стационарни обекти;
- Охрана със системи за видеонаблюдение;
- Физическа охрана на обекти;
- Проектиране и инсталация на охранителни системи - подготовка, монтаж, технически ремонт и поддръжка;
- Обслужване на монитори за видеонаблюдение и сигнали;
- Почистване на работните места;

Транспорт:

- Управление на лек автомобил „Рено Меган“;
- Управление на лек автомобил „Шевролет“;
- Управление на лек автомобил „Ауди А4“;
- Хигиенизиране и текуща поддръжка на автомобилния парк;
- Почистване на работните места;

Процедури за управление на различните категории рискове.

- Постоянен риск. Мускулно-скелетни увреждания и общи заболявания представлява нервно-психическото напрежение и стрес при административно-управленските дейности, при работа на компютър, при обслужване на СОТ и извършване на охраната на обекти, както и при работа с клиенти. Фирмата е предвидила осигуряване на тонизиращи и ободряващи напитки за нощните дежурства, както и провеждането на периодични медицински прегледи със съдействието на Службата по трудова медицина към „СТМ – 2000“ ООД, съгласно Раздел II и III на Наредба № 3, за ранно откриване и лечение на налични отклонения от здравословното състояние при извършваните дейности.
- Риск за мускулно-скелетните увреждания. Общи заболявания от охлаждане на работещите се създава при работа през студения период на годината в контакт с ниски температури особено при автопатрулиране и при обход на охраняваните обекти. Осигурени са отоплителни помещения за периодична релаксация, топли напитки, топло работно облекло, ръкавици и обувки. Предстои провеждане на периодични медицински прегледи със съдействието на „СТМ - 2000” ООД.
- Възможност за възникване на пожар. В административната сграда на фирмата с оглед съхранението на документация на хартиен носител и техника. Като превантивна мярка е изготвена инструкция за безопасна работа в посочените условия. Работниците са обучени и инструктирани за безопасна работа, съоръженията са приведени в съответствие с нормативните изисквания. Изготвен е ситуационен план за действия при бедствия и

аварии със схема за евакуация, осигурени са необходимите пожарогасителни средства, работниците са инструктирани и периодично се проверят знанията им за боравене с пожарогасителните средства и се следи строго от административното ръководство за недопускане тютюнопушенето в пожароопасните места. Осигурена е телефонна връзка с РСПБЗН.

Възможни рискове при автопатрул.

- Възникване на пътно-транспортно произшествие. В резултат на това има опасност от нанасяне на вреди на пътуващите и водачите на моторните превозни средства (леки автомобили „Рено Меган“, „Дачия Логан“, „Шевролет” и „Ауди А4”). Взетите мерки за намаляване на риска включват предварителен ежедневен технически преглед и заверка на пътните листи, проверка на водача за алкохол и периодични СО и ТО на техниката, като възникналите неизправности се отстраняват своевременно. Провеждат се редовни сезонни и технически прегледи.
- Риск при боравенето с огнестрелно оръжие и охрана на съответните обекти. За недопускане на злополуки работещите периодично се инструктират за безопасна работа с цел недопускане на евентуално отклоняване на вниманието или неправилна употреба на повереното оръжие. Провежда се постоянен медицински мониторинг и медицински прегледи.

Възможни рискове при работещите в офиса.

- Работа на компютър. За работещите в офиса (ръководител отдел ЧР, счетоводител, специалист маркетинг и реклама, касиер счетоводител, организатор охрана, техник пром. електроника, оператор въвеждане на данни и Управител) са осигурени предпазни екрани на мониторите, поставени са щори на прозорците, физиологичен режим на труд и почивка със съдействието на СТМ, съгласно изискванията на Наредба № 7/05 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи. Провеждат се офталмологични прегледи на работещите с видеодисплеи над 4 часа дневно и не се допуска назначаване на работници и служители със здравословни противопоказания.
- Риск за мускулно-скелетни увреждания и общи заболявания. Принудителната седяща работна поза при работа с видеодисплейни терминали създава предпоставка за гръбначно увреждане, застой на кръвта в кръвоносните съдове и долните крайници, утилизация на кристали в пикочната система, евентуални усложнения на бременността. Ел. инсталациите и контактните мрежи са обезопасени и периодично се извършват измервания. Физиологичен режим за труд и почивка се спазва.

Възможни рискове при отдел техническа поддръжка.

- Увреждане от електрически ток (при експлоатацията на ел. осветлението и ел. уреди, съоръжения и присъединителните елементи). До ремонт на ел. инсталациите и ел. съоръженията се допускат само квалифицирани специалисти с редовно защитена квалификационна група по електрическа безопасност. Работещите са инструктирани за безопасна работа, съоръженията са занулени и заземени съгласно изискванията. Редовно се извършват ел. измервания с доказване на ефективността на заземяване и зануляване.
- Работа на височина (при подмяна на ел. осветителни тела, при монтаж на охранителни системи и инсталации и др.). Осигурени са всички условия за недопускане на злополуки, използват се изправни и надеждни стълби, ремонт на ел. съоръжения се извършват от квалифицирани и инструктирани по електробезопасност специалисти. Редовно се провеждат периодичните инструктажи за безопасна работа.

- Работа с ръчни електрически инструменти. При работа с тях съществува риск от наранявания и злополуки на горните крайници, при отклонено внимание и при настройка на технологичното оборудване. При евентуално невнимателно манипулиране и отклоняване на вниманието са възможни тежки трудови злополуки. За недопускане на злополуки въртящите детайли на машините са обезопасени, а работниците периодично се инструктират за безопасна работа. При работа с тях се използват специално работно облекло и лични предпазни средства. Води се дневник за ежемесечна проверка на състоянието на преносими електрически инструменти от специалист.
- Контузии, порязвания и др. Наранявания могат да се получат при монтажа на охранителни системи и инсталации на обекти по договор. Работниците периодично се инструктират за безопасна работа с цел недопускане на евентуално отклоняване на вниманието или употреба на алкохол преди и по време на работа. Провежда се постоянен медицински мониторинг. Осигурени са необходимите специални работни облекла и лични предпазни средства. Експозицията е минимална. Редовни са периодичните инструктажи за безопасна работа.

3 Заключение

Проблемът със сигурността на хората остава и се разглежда като сложен, широкообхватен и с динамично променящи се параметри. Процесът на управление на сигурността не се ограничава само в идентифициране, анализ и оценка на рисковете и заплахите. Чрез него се формират решения, планират се и се изпълняват дейности, насочени към своевременното неутрализиране, отблъскване, отразяване и смекчаване на рисковете и заплахите. От предоставения доклад се вижда, че охранителна фирма „ МЕГА СОТ” ЕООД гр. Шумен покрива изискванията за предотвратяване на трудови злополуки и намаляване на риска за възникване на щети и злополуки на работното място.

ЛИТЕРАТУРА:

[1] Диманова Д, Управление на риска, УИ на ШУ „Епископ Константин Преславски“, ISBN 978-619-201-095-9, 2016.

[2] Директива 96/82/ЕО - Севезо II

[3] Национална сигурност на България: Рискове до 2020 – 2025.

Име на автора: Цветелин Димитров Цонев, фак. № 2070090001, e-mail: cvetelin.conev2000@gmail.com
ШУ „Епископ К. Преславски“, Факултет по технически науки, студенти от специалност „Сигнално-охранителни системи и сигурност“, II курс.

ANALYSIS OF MINE SURVEYING DEFORMATION'S RESULTS FROM MONITORING SYSTEM IN OPEN PIT COPER MINE

YASEN T. PROKOPOV

***ABSTRACT**: The management of mine operations development is connected with three basic areas – Geological, Technological and Mine surveying. The last one is mainly related to the observation and control of the deformation processes in the rock massif. A particularly important stage in the mine operations is the monitoring of the boards condition and the built-up embankments in terms of their stability. Determination of the deformations and their analysis ensure operational safety and reliable control of their forecasts. The probabilistic nature of the initial data, caused by the uncertainty of the environment in which the parameters of the Open pit are formed, requires analysis and assessment of their reliability. The survey results use, in addition to laboratory and natural tests and geophysical surveys, ensures the correctness and reliability in the modeling and the slope stability determination.*

***KEYWORDS:** deformations, monitoring, analysis, model*

АНАЛИЗ НА МАРКШАЙДЕРСКИ НАБЛЮДЕНИЯ НА РЕПЕРНА МРЕЖА ПРИ РЕАЛИЗАЦИЯ НА МОНИТОРИНГОВА СИСТЕМА В ОТКРИТ РУДНИК ЗА ДОБИВ НА МЕДНА РУДА

ЯСЕН Т. ПРОКОПОВ

***АБСТРАКТ:** Управлението на развитието на минните работи е в три взаимно свързани насоки: геоложка, технологична и маркшайдерска, която основно се отнася до наблюдение и контрол на деформационните процеси в скалния масив. Особено важен етап при експлоатацията на един рудник е мониторинга на състоянието на бордовете и на изграждените насипища по отношение на тяхната устойчивост. Деформациите и тяхното определяне осигуряват безопасност при експлоатацията и надеждни прогнози при управлението. Вероятностният характер на изходните данни, във връзка с неопределеността на средата, в която се формират параметрите на рудника, налага анализ и оценка на тяхната достоверност. Използването на резултати от маркшайдерски наблюдения, освен лабораторни и естествени изпитвания и геофизични изследвания гарантира коректността и достоверността при моделиране и изчисляване на устойчивостта на откосите. .*

1 ВЪВЕДЕНИЕ

Нарушеното природно равновесие, в резултат на изземването на минна маса и оформянето на насипища води до разрушаване на бордовете на рудниците, а оттук и до значими, катастрофални понякога последствия. Мониторингът на деформационните процеси е основно в две направления – безопасност на съоръжението като цяло от една страна и анализ на факторите, оказващи влияние, с цел прогнозиране и управление на процеса, от друга.

Дистанционните изследвания в обектите за открит добив имат значимо присъствие при цялостната им експлоатация, особено по отношение на тяхната сигурност и надеждност, както и за осигуряване на технологичната им схема на разработване, обусловена от разнообразните минно-технологични условия и технически средства, които се прилагат. При активните методи за дистанционно изследване на Земята се регистрират отразените от земната повърхност изпратени сигнали, които могат да бъдат с голям обхват

и нагледност - за глобални и локални наблюдения, при много добра разделителна способност.

Сравнението между различните методи за мониторинг безусловно налага т. нар. *система "георобот"*, като комбинация от роботизирана тотална станция и прецизни ГНСС измервания, допълнени с радарната система за ранно предупреждение.

Поради спецификата на минните работи [5] в откритите рудници и тяхната форма, заради изземването на природните богатства в дълбочина, се налага оптимално разполагане на изходните точки за наблюдение. Най-ниските хоризонти, които по принцип не са опасни, могат да бъдат наблюдавани, ако станцията е в близост до ръба на котлована. Това улеснява следенето на бордовете на по-високите стъпала, а промяната на работните участъци налага и активно поставяне на нови контролните репери и премахване на някои от съществуващите.

Началният етап от реализацията на една цялостна мониторингова система за условията на рудник "Асарел" [2] е свързан с анализа на хиляди наблюдения на положената реперна мрежа, която е в основата на изводите за перспективната устойчивост и безопасната експлоатация на съоръжението.

2 КОНТРОЛНИ РЕПЕРИ – РАЗПОЛОЖЕНИЕ, ОРГАНИЗАЦИЯ НА ИЗМЕРВАНИЯТА, ОБОБЩЕНИ ХАРАКТЕРИСТИКИ

От последните двадесет години на миналия век при изследване на деформации в минни обекти за открит добив се спазват основно инструкционните изисквания посочени в [3] и [4]. За рудника се прилагат и нормативни документи в областта на маркшайдерството, някои от които са ведомствени инструкции или указания. В маркшайдерската практиката този процес в рудниците при научно-изследователски разработки е съобразени именно с тези документи.

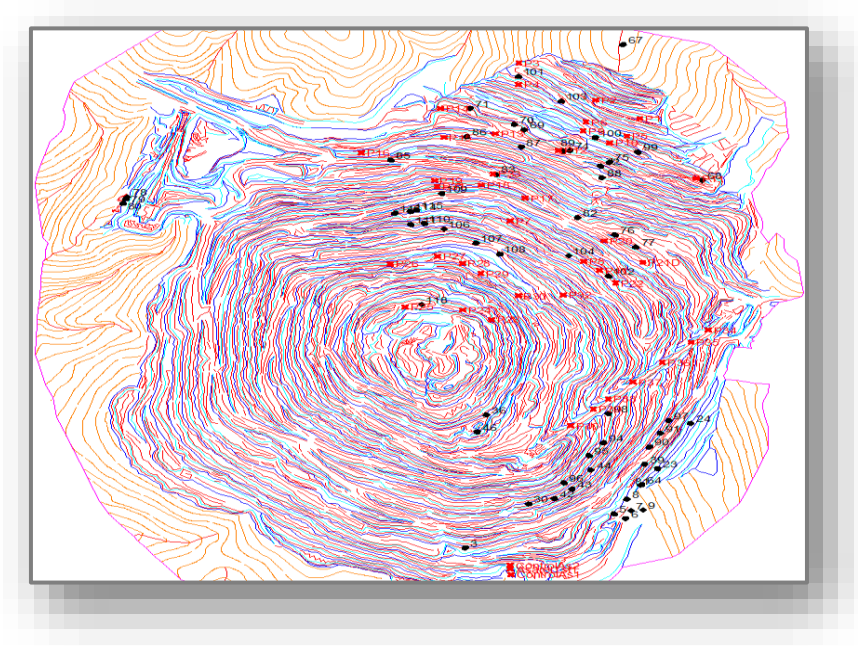
При анализа са използвани данни (включително координати, освен "суровите" измервания) от периодични наблюдения на точки, разположени в целия котлован на рудника. По-голямата част от точките са извън зоната на предпазния целик и условно могат да се разделят на две групи. В първата група са включени точките, които са сигнализирани чрез постоянно монтирани отражателни призми. Пространственото положение на точките от тази група се определя чрез ъглови и линейни измервания - условно те са наречени "призми". Втората група обхваща точки, чието положение в пространството е определено с измервания чрез ГНСС технология – това са т.нар. "репери". На фиг. 1 е показано разположението на точките в план - "призмите" са в червен цвят, а "реперите" – в черен.

Използвани са резултати от измервания за периода от 09.2014 до 08.2015 г., като те са извършвани по нерегулярна схема, като в голямата си част включват повторни регистрации през различни часове в денонощието. Обемът на направените измервания включва над 476000 записа, а този с координати на реперите – над 20500, основно за точки разположени на различни хоризонти в северния неработен борд на рудника. Измервателната станция е разположена в стабилен, незасегнат от рудничната дейност участък на южния борд, като е използвана роботизирана тотална станция Trimble S8.

Върху точността на измерванията оказват въздействие фактори, влияещи върху линейността на оптическия канал като изменение на температурата и налягането, прозрачността на въздуха, наличието на дисперсни частици и други във времето, както и

разпределението на тези фактори в пространството между измервателната станция и съответните репери

Разчети за минималната стойност на преместванията Q_{min} и максималната стойност Q_{max} [1] не са извършвани, а са използвани наличните измерителни средства и технологии.



Фиг.1 Схема с разположението на призмите и реперите

Анализът е свързан с търсене на пространствено-времеви зависимости между компонентите на деформационното поле с използване на статистически методи и интерпретация на получени данни от позициите на геодинамичния подход. Основание за определена надеждност осигурява наличието на значителен брой данни, за определен период от измервания в рудник "Асарел", което позволява да се извърши реална оценка на постигнатата точност при измерванията с използваната апаратура.

3 АНАЛИЗ НА ПЪРВИЧНИТЕ ДАННИ ОТ ИЗМЕРВАНИЯ С ТОТАЛНА СТАНЦИЯ

Обработените данни са от измервания, извършени с тотална станция модел Trimble S8, *Точността* при полярното определяне положението на точките зависи от различни фактори, които могат да се отнесат към следните *три групи*:

- инструментални грешки;
- грешки при измерванията;
- грешки от метереологичните условия.

Прилаганите в рудника технически средства и технология позволяват свеждането до минимум на влиянието на грешките от първите две групи. Това се осигурява от принудителното центриране на инструмента и сигналите, автоматизираното насочване на инструмента, използването на контролни точки и др.

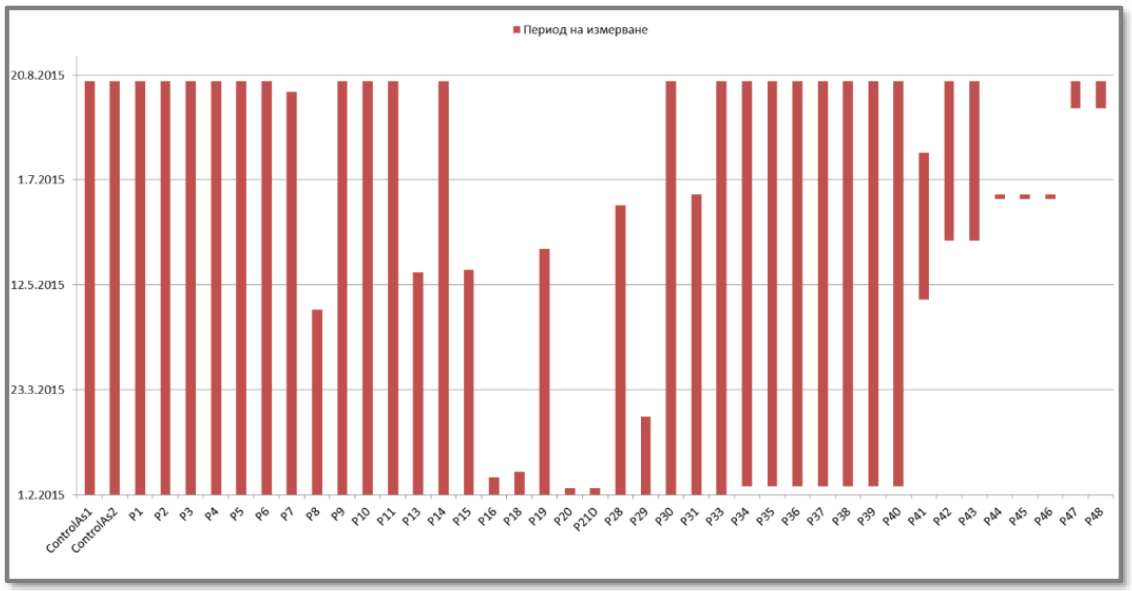
Върху източниците на грешки от третата група практически не може да се влияе. Затова в повечето литературни източници и нормативни документи се поставя изискването за извършване на измерванията при условия, когато тяхното влияние е минимално.

Извършването на високоточни измервания не се препоръчва/позволява при валежи, мъгла, значителна разлика в температурата на станцията и наблюдаваната точка, влажността и запрашеността на различните атмосферни слоеве, през които преминава лъча и др. Това ограничение в известна степен противоречи на идеята за непрекъснат мониторинг.

Целта на анализа е установяване фактическа точност на измерванията при използване на конкретния инструмент за конкретните условията на рудника. При анализа се отчита, че някои от разликите е възможно да се дължат на премествания на наблюдаваните точки, поради което основно се анализират **параметри, независещи от положението на точките** при различните цикли измервания. Такива например са индексната и колимачната грешки, както и разликите в разстоянията, които се получават при двете положения на зрителната тръба в един цикъл и които практически са извършени при едни и същи условия за относително кратко време.

На фигура 2 схематично са представени периодите от време на измерванията за всяка точка. Показатели за точността на ъгловите измервания, които не зависят от преместванията на наблюдаваните точки, са индексната и колимачната грешки. Те характеризират точността на ъгловите измервания при всеки гирус и теоретично се елиминират при осредняване на отчетите.

На фигура 3 са представени графики на стойностите им за всяка точка. По абсцисата на тези графики е средното разстояние от наблюдаваната точка до станцията. Графиките не показват съществена зависимост на колимачната и индексните грешки от разстоянието. Аналитичната оценка за това са корелационните коефициенти, които за средната стойност и ср.кв.грешки са 0.48 и 0.64 за колимачните грешки и съответно 0.68 и 0.38 за индексните грешки. Най-големи са средните квадратни грешки на индексната и колимачната грешки при най-късите визури (15-20 m) към точки ControlAs1 и ControlAs2. Те са предвидени да бъдат контролни при бъдещата реализация на мониторинговата система, но поради твърде малките разстояния, противоречащи на инструкционните изисквания, са отпаднали.



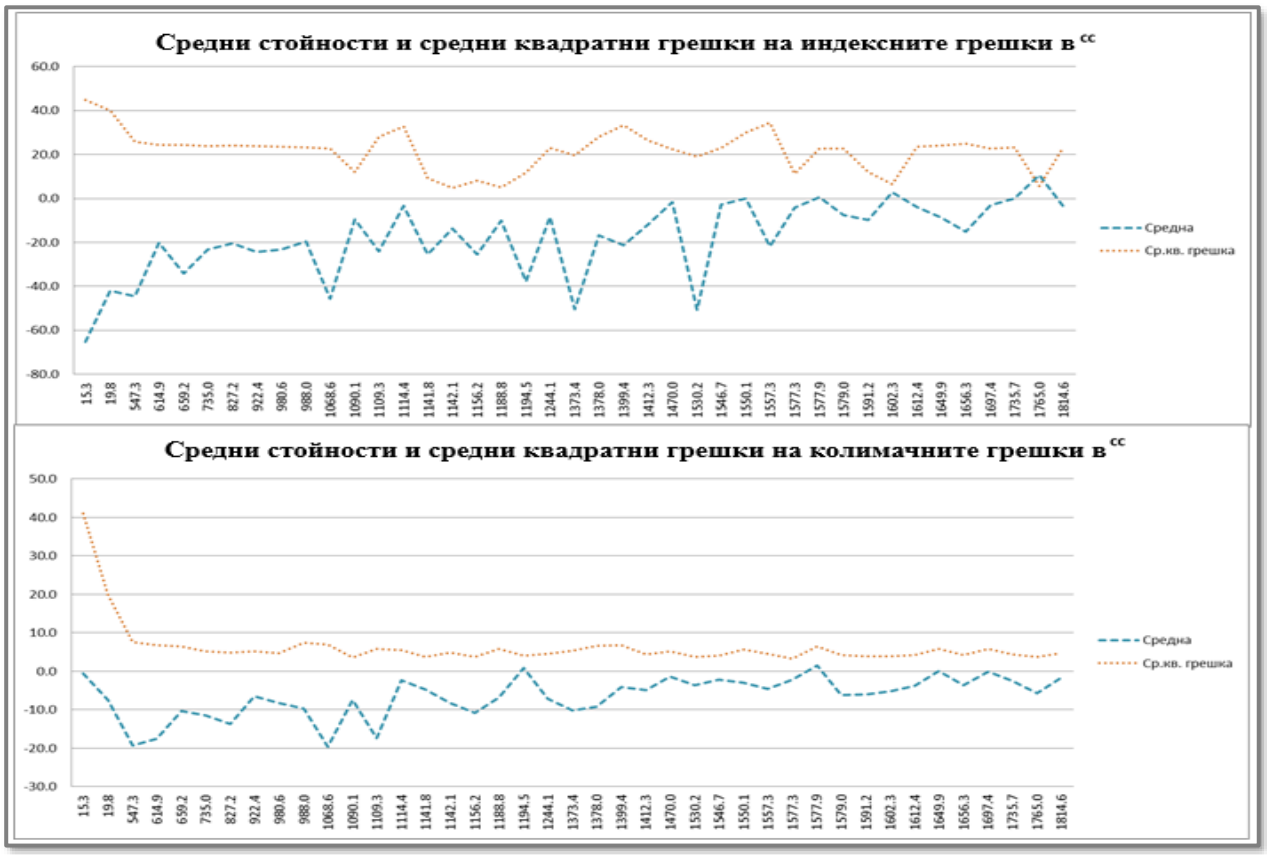
Фиг. 2 Период на измерване за призмите

Анализът на резултатите за измерените дължини е извършен по наблюдавани точки, като общо са обработени 439386 дължини или средно 10717 на наблюдавана точка.

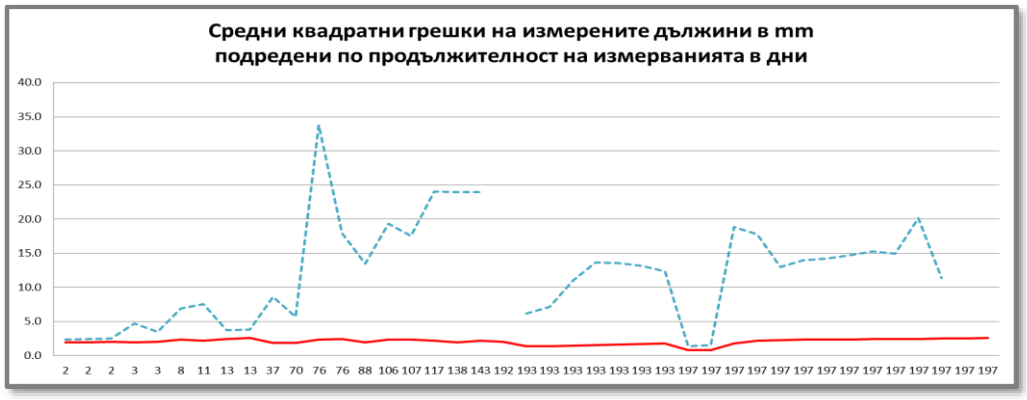
Средната квадратна грешка на измерена дължина е 17.2 mm. Тя зависи както от техническите параметри на далекомера, така и от положението в пространството на точките. Графика на изменението на средните квадратни грешки на измерените дължини (без тези на точки P4 и P7) е представена на фигура 4, в която по абсцисата са наблюдаваните точки подредени по разстояния. На нея с червен цвят е представена техническата точност при съответните разстояния. Значително по-големите стойности на ср. кв. грешки от тези представени в техническата спецификация на инструмента се дължат на преместванията на наблюдаваните точки.

Върху точността на определянето в пространството на наблюдаваната точка влияят не само точностите, а и стойностите на измерените разстояния и ъгли. Ако се приеме паспортната точност на измерените ъгли (3^{cc}), то грешката в превишението (респ. котата) при среден зенитен ъгъл е 6.1 mm. Същата такава неточност при определяне на превишението би се получила при грешка в определеното разстояние от 580 mm. Ако вместо паспортната точност се използва определената от измерванията, чак грешка в измереното разстояние от 2000 mm би повлияла със същата стойност както точността на измерването на ъглите.

За средни разстояния и зенитен ъгъл към наблюдаваните точки в рудник "Асарел" **точност на измерените разстояния 1-2 m не влияе върху определянето на котите** повече от точността на определянето на зенитните ъгли.



Фиг. 3 Средни показатели за ъгловите измервания



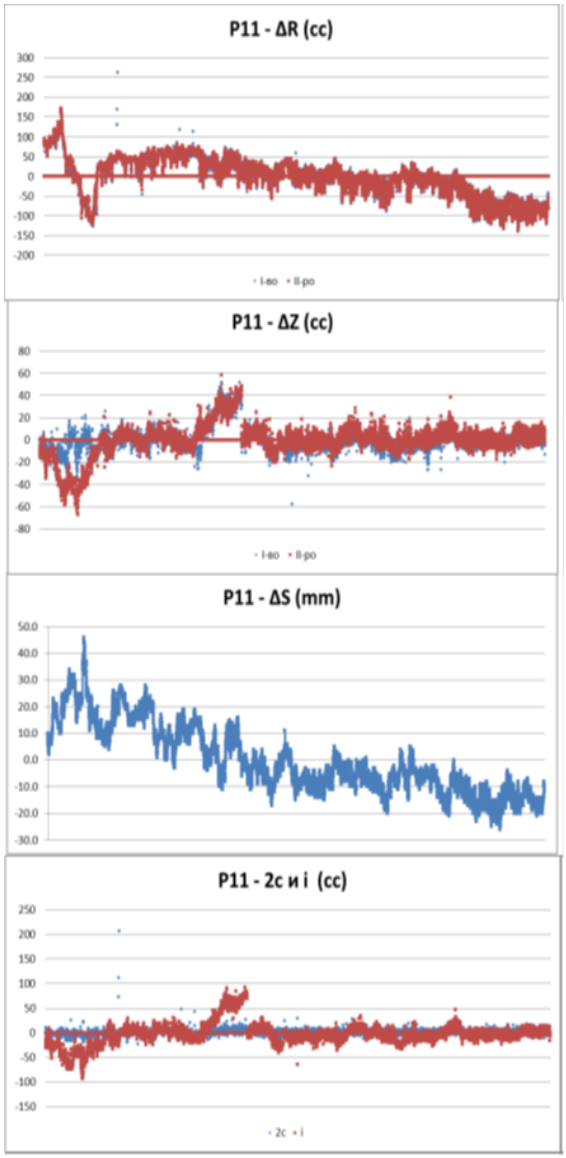
Фиг. 4 Средни квадратни грешки на измерените дължини

Обработката на данните от измерванията е извършена по точки, в които е визирано. Предварително данните с измерванията към всяка точка са подредени по време и I-во и II-ро положение на зрителната тръба в гируса. На база на получените стойности за измерените посоки, зенитни ъгли, колимачна и индексна грешка, са изработени по четири графики за всяка точка (фиг. 5). И в четирите графики абсцисата е времето на измерването, а отгоре на всяка от графиките е посочен номера на наблюдаваната точка и съответната характеристика.

На първите три графики са показани съответно отклоненията на измерените хоризонтални посоки, зенитни ъгли и хоризонтални разстояния от техните средни стойности, а на последната - индексната и колимачна грешки, което дава възможност да се оценят измерванията независимо от това дали има движения при наблюдаваната точка

Първо положение е представено със син цвят, а второ – с червен, но поради дребния мащаб по-голяма част от данните се припокриват, при което се визуализират основно данните от II положение.

Групирането на ъгловите измервания по периоди от няколко дни неколкократно намалява стойностите им във времевите интервали. Това показва, че възможна причина за по-големите стойности на грешките са премествания на наблюдаваните точки.



Фиг. 5 Обработка на данните от измерванията (за т. P11)

Рязката промяна в някои от времевите интервали (напр. около полунощ на 25.04.2015 г.) показва, че освен преместването на наблюдаваните точки, причина могат да са технически проблеми на измервателната апаратура или коригирането на работата на инструмента чрез промяна в настройките му, вследствие на извършеното автоматично калибриране. Големите стойности на индексната грешка преди калибрирането на инструмента поставят под въпрос надеждността на направените изводи. Това налага детайлен анализ на първичните данни от измерванията преди използването им при последващи обработки (например координатни изчисления) и анализи. Някои от *по-съществените изводи*, които могат да се направят са:

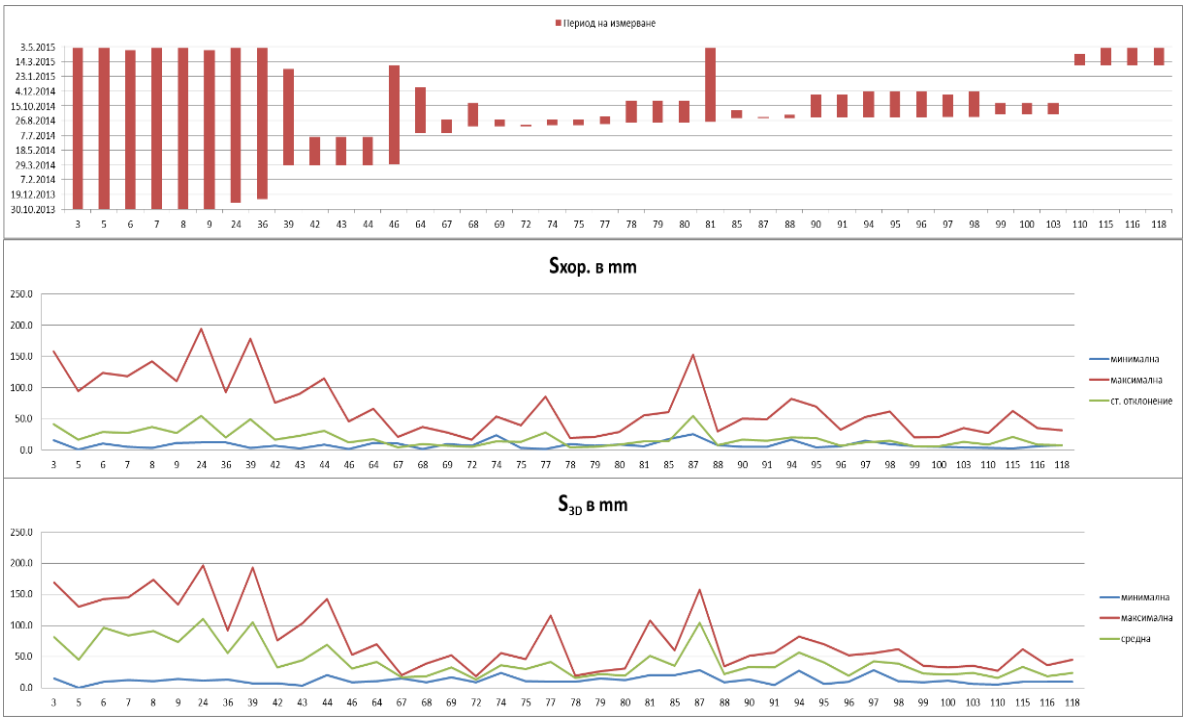
- индексната и колимачната грешки не зависят съществено от дължините на визурите, при големи разстояния между станцията и наблюдаваните точки (средно 1240 m);
- индексните грешки са около 4 пъти по-големи от колимачните, а ай-вероятна причина за това е значителното влияние на вертикалната рефракция;
- основно влияние върху точността на определяне на наблюдаваните точки в план оказва точността на измерените посоки, а върху котите – на зенитните ъгли;
- влиянието на индексната грешка при определянето на пространственото положението е значително - около 4 пъти по-голямо от това на колимачната грешка и резултатите от измервания с по-големи индексни и колимачни грешки не следва да участват в обработката;
- поставянето на мониторинговите станции в направление на очакваните деформации (една от координатните оси на условната координатна система), повишава точността на определянето на преместванията на точките и др.

4 АНАЛИЗ НА ДАННИТЕ ОТ ПЕРИОДИЧНИ ИЗМЕРВАНИЯ, ПОЛУЧЕНИ ЧРЕЗ ИЗПОЛЗВАНЕ НА ГНСС

Определяне на преместванията на част от наблюдаваните точки, чрез използване на ГННС, е на база измервания, извършени с приемник Trimble R6 в режим RTK.. Данни за постигната точност на измерванията не са налични, а уточненията сочат, че при измерванията щокът с приемника е държан “на ръка“, без използване на различни устройства за придържане, например “биподи“, “щипки“ и др. Не са използвани и устройства за принудително центриране. Като разположение всички точки (репери) се намират в източната част на котлована, групирани в две зони – едната на югоизток, а другата - в североизточната част.

От всички данни от измерванията (60 точки), са обработени само за 42 от наблюдаваните точки, тъй като за останалите 18 от тях има по няколко измервания. Общият брой на обработените измервания е 1195 или средно 29 на точка. Повече от половината от измерванията (704) са извършени в 8 точки, т.е. средно около 90 измервания във всяка от тях.

Графично интервалите от време, за които са извършвани измервания за съответните точки са представени на фиг. 6, където са показани и двумерния и тримерен вектор на преместване с минималните и максимални стойности, и стандартни отклонения.



Фиг. 6 Времеви интервали и вектори на преместване

За всяка от точките е извършена обработка и са изчертани по три графики (фиг.7). Първата илюстрира преместването на наблюдаваната точка спрямо първото измерване по направления на координатните оси X, Y и H, това са съответно ΔX, ΔY и ΔH, както и преместването в план Sхор. и в пространството - Sобщо (или 3D). На тази графика по абсцисата е отразено времето на измерване, а по ординатата – съответното преместване в mm.

Втората графика представя преместванията на наблюдаваната точка в план спрямо началното положение, като абсцисата е преместването в посока изток в mm, а ординатата преместването в посока север в mm.

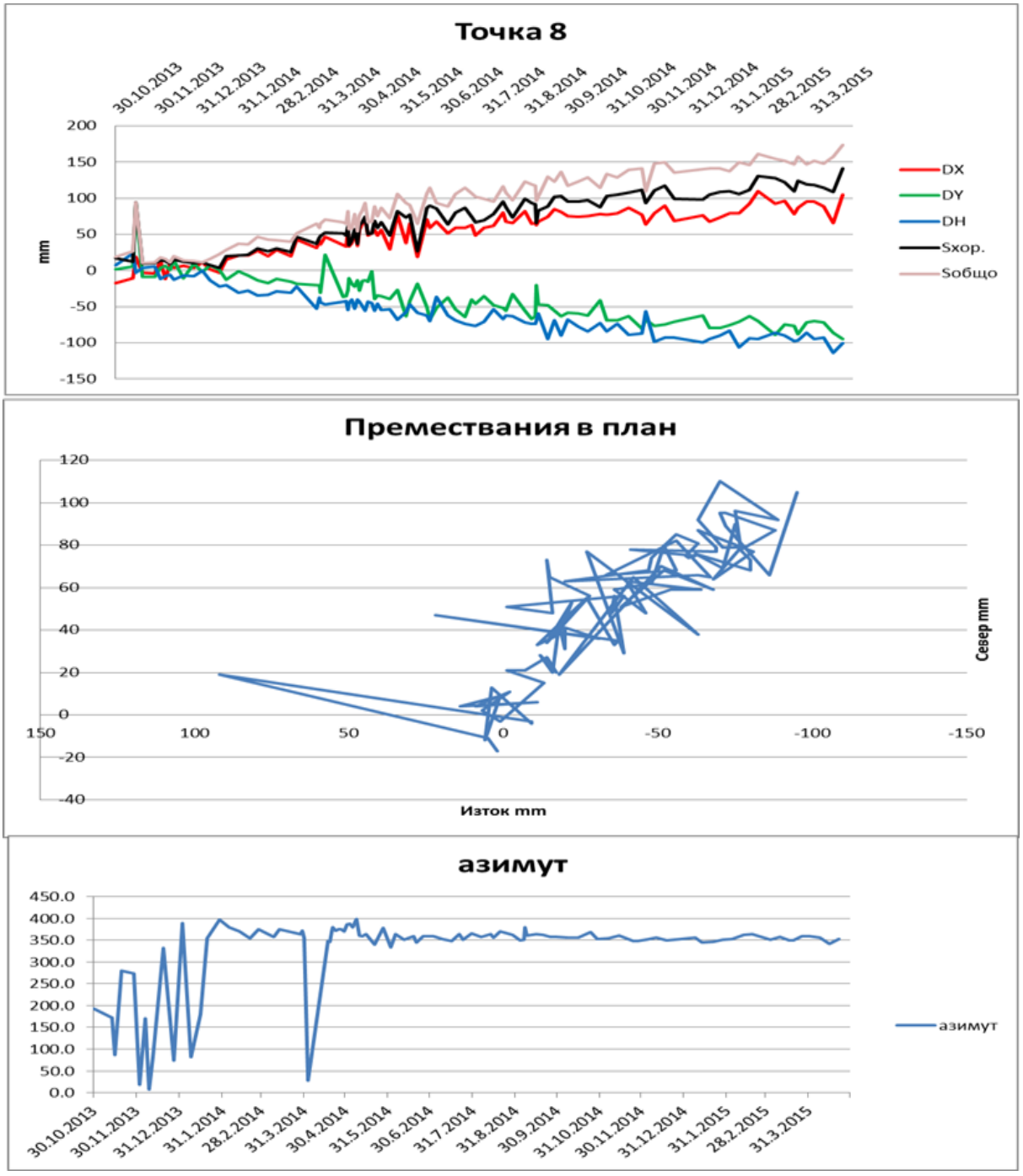
Третата графика отразява посоката на преместването чрез азимута на вектора на преместването. На нея по абсцисата е времето на измерването (момента като дата), а по ординатата стойността на азимута в гради.

Като показател за точността на измерванията може да се използват средните стойности на преместванията от всички измервания, които са съответно $\Delta X_{ср.}$= -5.3 mm, $\Delta Y_{ср.}$= -4.6 mm и $\Delta H_{ср.}$= -3.4 mm, както и стандартните им отклонения, които за всички измервания са $\sigma_{\Delta X}$= ±48.5 mm, $\sigma_{\Delta Y}$= ±30.3 mm и $\sigma_{\Delta H}$= ±27.4 mm. Тези стойности не отразяват реалната точност на измерванията и са значително завишени, понеже при тяхното определяне участват и премествания, които се дължат на деформационни процеси, а не са вследствие точността на измерванията

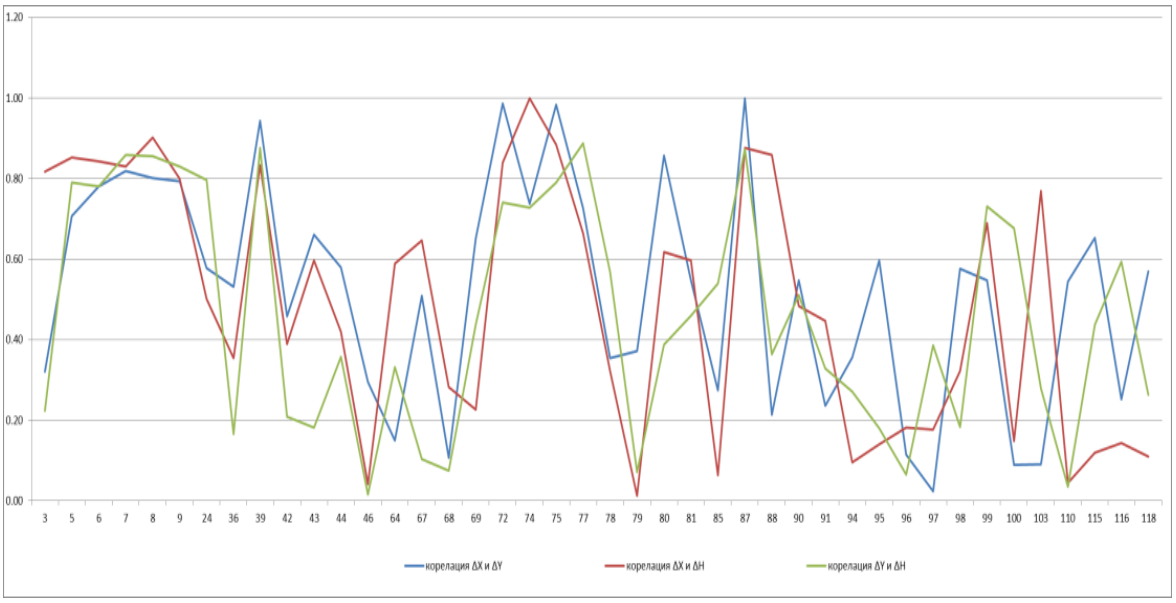
Прилагането на ГНСС технологията при изследване на деформации и постигането на точност под 1 cm или даже 3 до 5 mm в положението на точките се постига при определени условия на измерванията, което за откритите рудници не винаги е възможно.

За илюстриране на зависимостите между преместванията по трите координатни оси са изготвените графики (фиг. 8) на корелационните коефициенти на връзките между преместванията в северна и източна посоки, в северна и по височина, и в източна и по

височина. За повечето наблюдавани точки стойностите на трите коефициента са приблизително еднакви. За отбелязване е, че при точките с по-продължителни измервания корелацията е умерена или значителна до висока, а за единични точки и много висока. За точките с по-малък период на измервания тя е умерена до слаба. По-високата корелация показва еднакви и равномерни премествания в план и височина, а по-слабата – по-големи премествания в определено направление.



Фиг. 7 Премествания на наблюдаваните точки (за т. 8)



Фиг.8 Корелация между преместванията по трите направления

Основни изводи за резултатите от измерванията в реално време (RTK) са:

- точността на измерванията не зависи от метеорологичните условия и се определя основно от метода, който се прилага, начина на центриране на приемника над наблюдаваната точка, конфигурацията и броя на спътниците;
- анализът на данните показва, че точността на определяне на положениетона наблюдаваните точки чрез ГННС е по-голяма от точността на определянето на положението им с моторизирана тотална станция Trimble S8;
- за повечето точки се наблюдава движение в северозападна или югозападнапосока, стойността на което зависи до голяма степен от продължителността на измерванията;
- оценката на точността е налична по време на самите измервания и при необходимост могат да се извършат допълнителни такива;
- непрекъснат мониторинг чрез ГНСС в рудник “Асарел“ е неприложим, поради големият брой наблюдавани точки (завишени разходи) и трудности при самото придвижване.

5 ЗАКЛЮЧЕНИЕ

Сигурната и безопасна експлоатация на откритите рудници е пряко свързана с установяване на промени в състоянието на масива от една страна. От друга страна изследването на пространствено-времеви зависимости между компонентите на деформационното поле позволява евентуална корекция в техните параметри.

Наличието на многобройни измервания, извършени при различни условия, дефинирането на преместванията, като реакция на масива към изменението на първичното му напрегнато-деформирано състояние, отчитане влиянието на екзогенните фактори са в

основата на коректността на изводите и препоръките. Анализът на първичните измервания гарантира и една надеждна статистическа обработка и обективност на оценките.

ЛИТЕРАТУРА:

[1] Димитров, Д. Инженерна геодезия, София, Техника, **1989**. 418, 235-238.
[2] Изграждане на мониторингова геодезична система от призми за рудник Асарел за автоматично следене на деформации посредством роботизирана тотална станция, GNSS референтни станции и интеграция на данните в софтуерен продукт Trimble 4D Control, Работен проект, „Солитех“ АД, **2015**.
[3] Инструкция за изследване на деформациите на сгради и съоръжения чрез геодезически методи, София, Главно управление по геодезия, картография и кадастър, **1980**.
[4] Инструкция за опазване на обектите и съоръженията от вредното влияние на минните работи във въглищните басейни, М - во на енергетиката, София, **1983**.
[5] Маждраков, М. Маркшайдерство. Методика на маркшайдерските работи в откритите рудници, Университетско издателство „СВ. Климент Охридски“, София, **2007.** 192, 150-157.

Име на автор: инж. Ясен Трифонов Прокопов
Месторабота: докторант към катедра “Маркшайдерство и геодезия” на МГУ “Св. Иван Рилски”, гр. София
E-mail: jasen_prokopov@abv.bg , тел. 0888671383

ASSESSMENT OF THE POSSIBILITY OF PRACTICAL USE OF AN UNMANNED AERIAL SYSTEM IN 3D TERRAIN-LEVEL MODELLING

KIRIL F. YANCHEV
KRASIMIRA K. KIRILOVA

ABSTRACT: *The report looked at the capabilities of unmanned aerial vehicle equipped with new modules and systems. A real experiment evaluated the accuracy of photogrametric survey for the practical use of an unmanned aerial system in three-dimensional terrain field modeling. An analysis has been carried out and the possibilities for their use for the creation of a field area of large areas are justified.*

KEYWORDS: *GNSS, PPK, VTOL, WingtraOne, 3D modelling*

ОЦЕНКА НА ВЪЗМОЖНОСТТА ЗА ПРАКТИЧЕСКО ИЗПОЛЗВАНЕ НА БЕЗПИЛОТНА ЛЕТАТЕЛНА СИСТЕМА ПРИ ТРИИЗМЕРНО МОДЕЛИРАНЕ НА ТЕРЕННА ПОВЪРХНИНА[1]

Кирил Ф. Янчев
Красимира К. Кирилова

АБСТРАКТ: *В доклада са разгледани възможностите на снабдените с нови модули и системи безпилотни летателни апарани (БЛА). Чрез реален експеримент е направена оценка на точностите на фотограметричното заснемане за практическо използване на безпилотна летателна система (БЛС) при триизмерно моделиране на теренна повърхнина. Извършен е анализ и са обосновани възможностите при тяхното използване за създаване на теренна повърхнина на големи площи.*

1. Въведение

Понастоящем платформите на безпилотните летателни апарати (БЛА) са ценен източник на данни за проучване, наблюдение, картографиране и 3D моделиране. Тъй като безпилотните летателни апарати могат да се разглеждат като евтина алтернатива на класическата пилотирана въздушна фотограметрия, се въвеждат нови приложения в обсега на късите и близки разстояния (*short- and close-range domain*). След един типичен фотограметричен работен процес, могат да се произвеждат 3D резултати като дигитална повърхнина или модели на терен, контури, текстурирани 3D модели, векторна информация и др.

2. Обект и цел на изследването.

Обект на настоящото изследване е незастроен имот в урбанизираната територия на гр. Благоевград, общ. Благоевград, обл. Благоевград. Имота се намира в промишлената зона на града, граничи с голям пътен възел, железопътна линия и складова база. Целта на настоящото изследване е да се провери възможността за използване на БЛС от ново поколение за създаване на панорамна снимка и 3D модел на терана. За постигане на поставената цел е

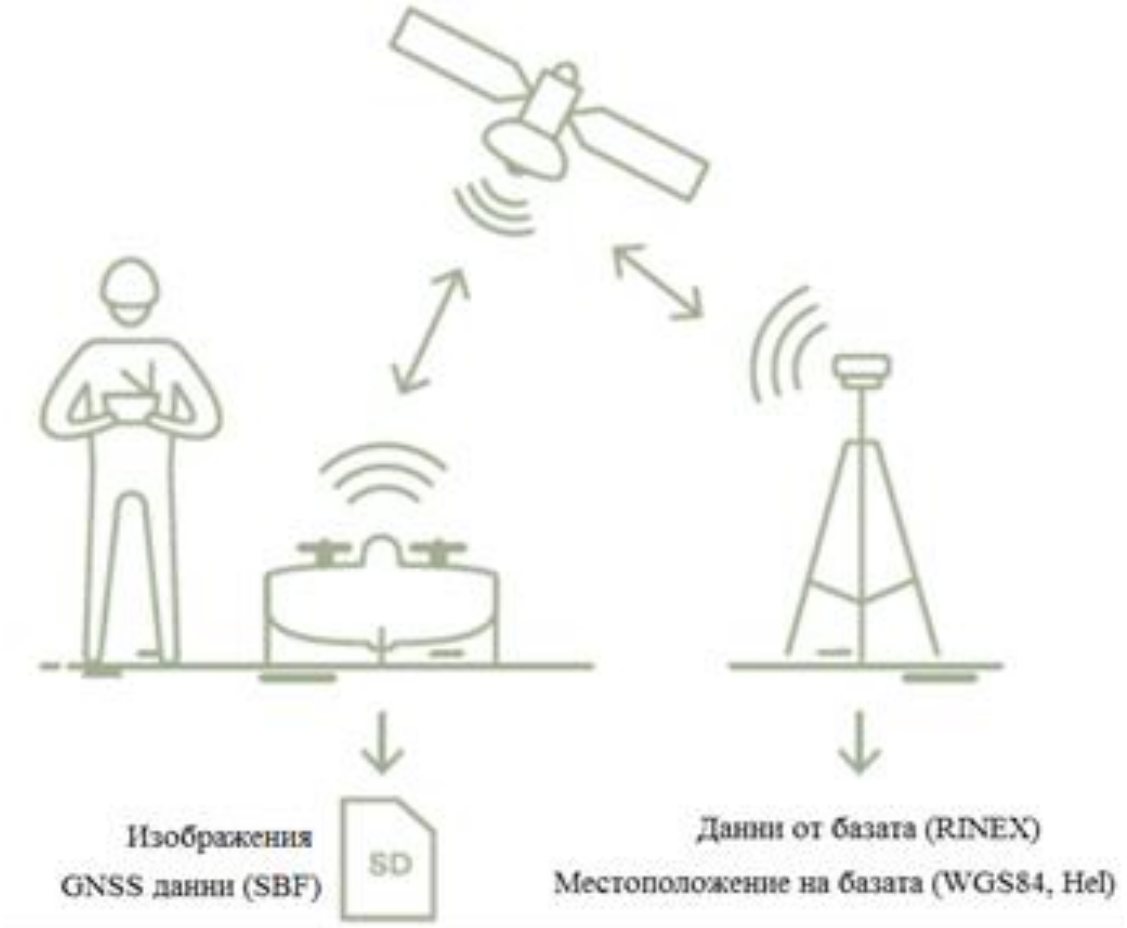
[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

направено въздушното фотограметрично заснемане и подробна полярна геодезична снимка [8].

3. Полски геодезически дейностти.

За оценка на възможността за практическо използване на безпилотна летателна система (БЛС) при триизмерно моделиране на теренна повърхнина се използва дрон WingtraOne PPK (Post Processed Kinematics). Кинематика за последваща обработка (PPK), използва корекционни данни от базова GNSS станция на земята, за да коригира GNSS данните на WingtraOne от полета. Тя позволява присвояване на сантиметрови прецизни геотагове към получените изображения. Този процес на географско маркиране се обработва в приложението на Windows - WingtraHub след извършване на полета (фиг. 1) [1], [4]. Използват се следните данни:

- Изображения от камерата WingtraOne;
- GNSS данни от PPK модула WingtraOne;
- Базови файлове (RINEX) от вашата базова станция;
- Базово местоположение на базовата GNSS станция в базирана на ITRF координатна система с елипсоидна височина.



Фиг.1. Кинематика за последваща обработка (PPK)

Базовата GNSS станция може да бъде както потребителска, така и базова станция от изградената инфраструктурна GNSS мрежа. Кинематика за последваща обработка позволява да се постигне висока точност без да се маркират и координират наземни опорни (контролни) точки (ground control points - GCP) [5], [6]. БЛС WingtraOne е оборудван с 42MP камера Sony RX1RII която гарантира висока резолюция на изображенията. На обекта са поставени шест контролни маркера които са координирани с двучестотни GNSS приемници Topcon HiPer Pro с продължителност на измерванията 30 min. По същото време са проведени и преки геодезически измервания с тотална станция Topcon GPT 3005LN. Обработката на резултатите от преките геодезически измервания е направена с програмен продукт Tplan.

4. Обработка на резултатите от полските геодезически дейностти.

Обработката на резултатите от геодезическите GNSS измервания е извършена с програмен продукт Topcon Tools v.8.2.3.

Резултатите от преките геодезически измервания са обработени с програмен продукт Tplan.

Въздушното фотограметрично заснемане е проведено с един полет на височина 100 m над терена, през месец Юни 2019 г. Обработката на изображенията е извършена по два начина:

- със софуера WingtraHub и използване на потребителска базова станция. Резюме на обработката на резултатите са представени в таблица 1.

Обработени резултати със софтуер WingtraHub **Таблица 1**

Output coordinate system	Geodetic ellipsoidal height (WGS84)
PPK processed	Yes
Base file(s)	log0166i.19O log0166i.19G
Base	blg22
Base location	Cartesian ECEF (WGS84) 4367012.36000 m, 1862114.63700 m, 4245723.36600 m
Base antenna offset	Not specified.
Detected base antenna type	TPSHIPER_PRO
Matching	867 images tagged.
PPK fix	98.85%
Mean accuracy	0.04 m horizontal, 0.06 m vertical
Warnings	None

- със софтуера Pix4Dmapper version 4.4.12, като в обработката са включени шестте контролни маркера. Резюме на обработката на резултатите са представени в таблица 2.

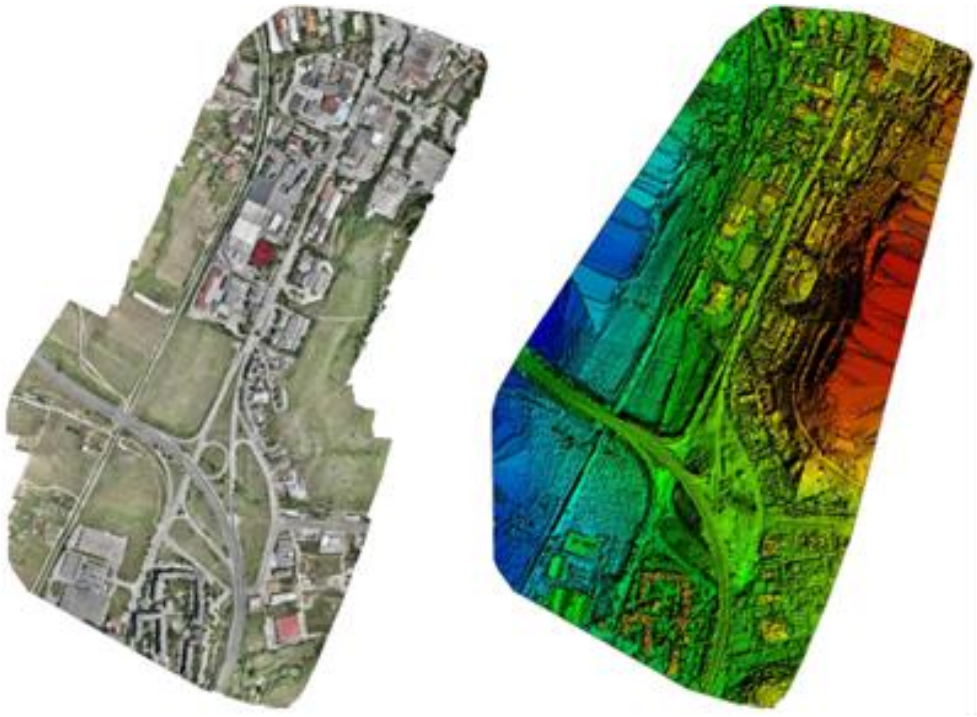
Обработени резултати със софтуера Pix4Dmapper version 4.4.12 **Таблица 2**

Project	BlgTOPCON2
Processed	2019-06-18 19:19:41
Camera Model Name(s)	DSC-RX1RM2_35.0_7952x5304 (RGB)
Average Ground Sampling Distance (GSD)	1.61 cm / 0.63 in
Area Covered	0.986 km^2 / 98.5891 ha / 0.38 sq. mi. / 243.7451 acres
Time for Initial Processing (without report)	01h:52m:30s

Images	median of 30709 keypoints per image	✓
Dataset	867 out of 867 images calibrated (100%), all images enabled	✓
Camera Optimization	0.06% relative difference between initial and optimized internal camera parameters	✓
Matching	median of 12579.2 matches per calibrated image	✓
Georeferencing	yes, no 3D GCP	⚠

Number of Generated Tiles	9
Number of 3D Densified Points	275636962
Average Density (per m^3)	644.79

Получената ортофото мозайка и съответния първичен цифров модел на повърхността (DSM) са показани на фигура 2.



Фиг.2. Ортофото мозайка и съответния първичен цифров модел на повърхността

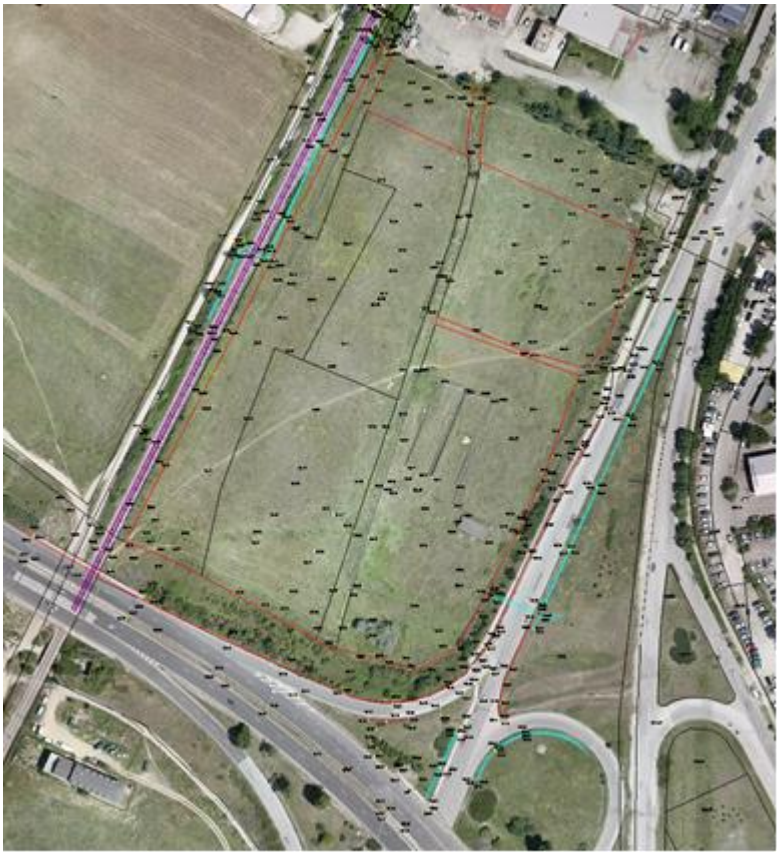
5. Сравнителен анализ на получените резултати.

От краткото изложение на получените резултати от обработката на въздушното фотограметрично заснемане по два начина, е видно че абсолютната дисперсия на геолокацията на ортофото мозайката е в едни и същи интервали (Таблица 3).

Абсолютна дисперсия на геолокацията на ортофото мозайката **Таблица 3**

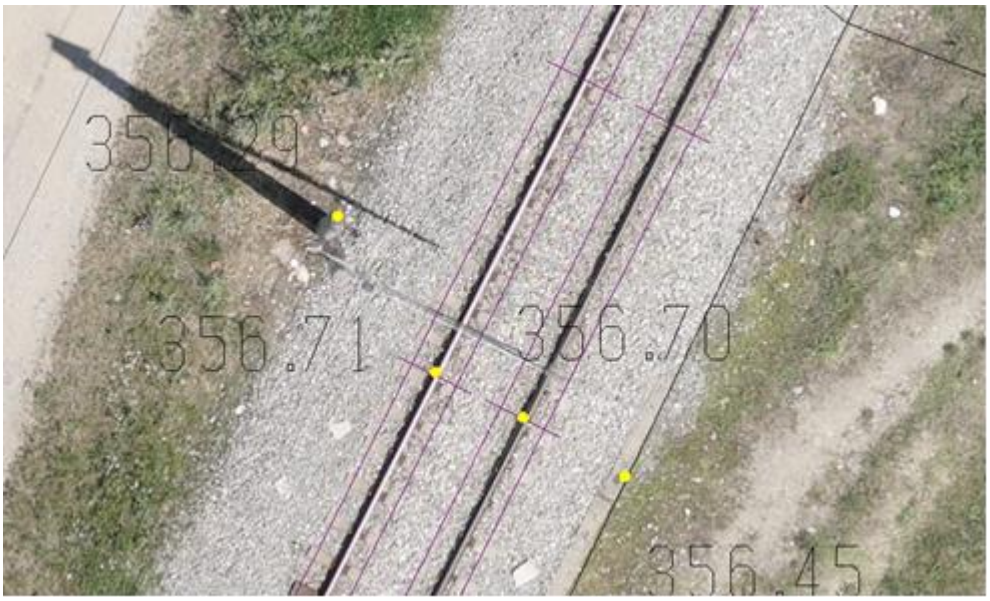
Min Error [m]	Max Error [m]	Geolocation Error X [%]	Geolocation Error Y [%]	Geolocation Error Z [%]
-	-0.80	0.00	0.00	0.00
-0.80	-0.64	0.00	0.00	0.00
-0.64	-0.48	0.00	0.00	0.00
-0.48	-0.32	0.00	0.00	0.00
-0.32	-0.16	0.00	0.00	1.15
-0.16	0.00	50.52	51.21	52.36
0.00	0.16	49.48	47.64	46.48
0.16	0.32	0.00	1.15	0.00
0.32	0.48	0.00	0.00	0.00
0.48	0.64	0.00	0.00	0.00
0.64	0.80	0.00	0.00	0.00
0.80	-	0.00	0.00	0.00
Mean [m]		0.000120	0.002967	-0.002908
Sigma [m]		0.012610	0.031090	0.028948
RMS Error [m]		0.012611	0.031232	0.029094

За сравнителния анализ чрез програмен продукт AutoCAD Civil 3D, са обединени ортофото мозайката и точките от преките геодезически измервания фиг. 3.



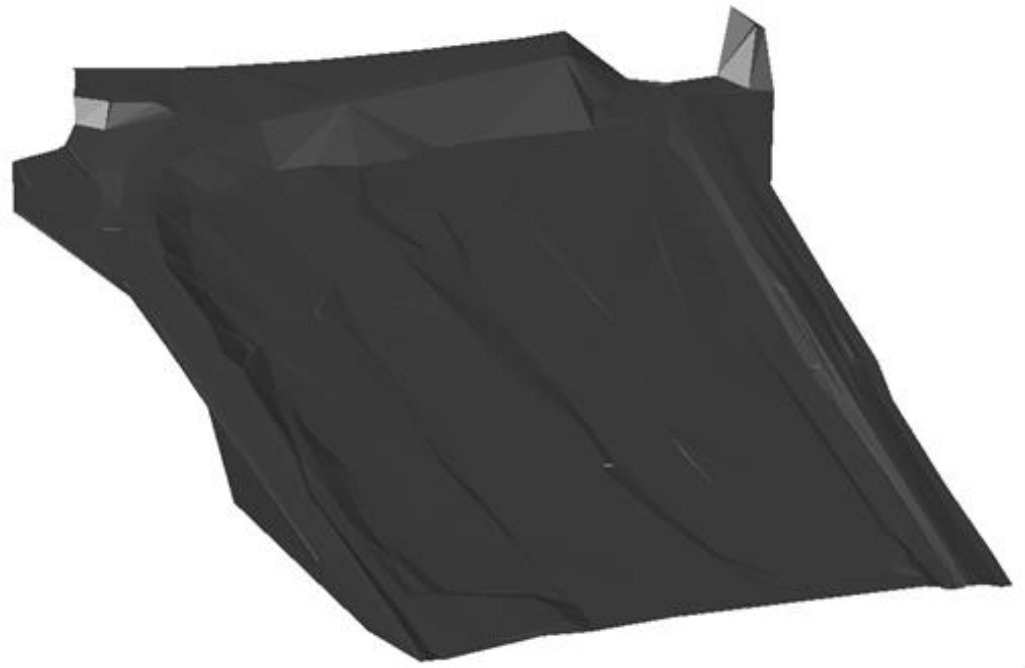
Фиг.3. Обединен модел на получените резултати

Точността на ортофото мозайката в планово полжение е визуализирана чрез обединениео и с точките от преки геодезически измервания на фигура 4.

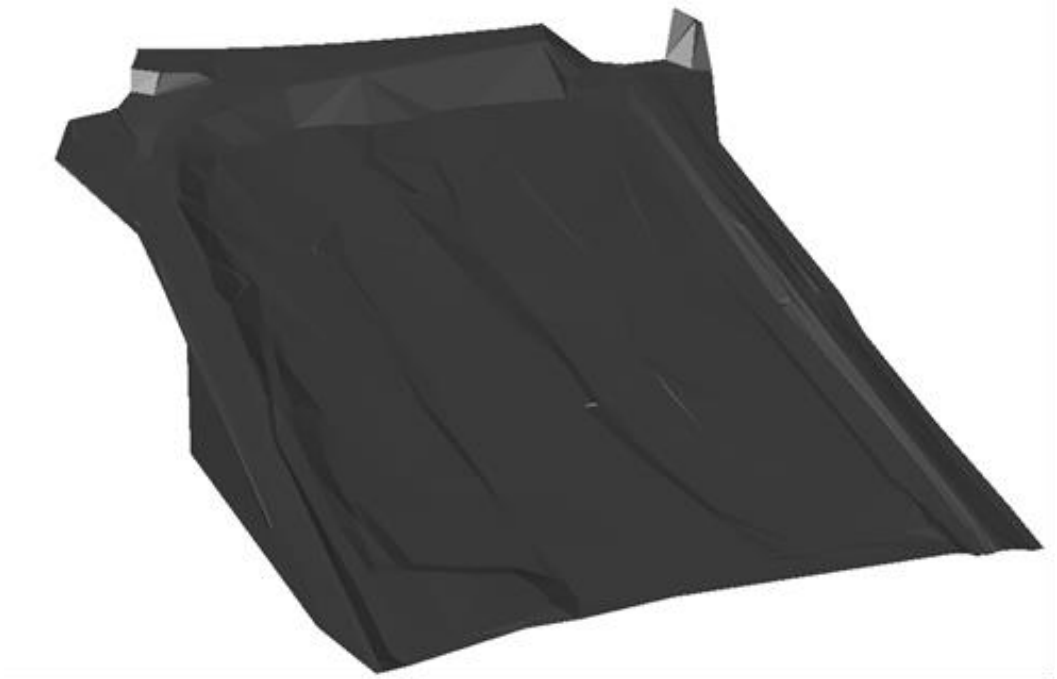


Фиг. 4. Точки от преки геодезически измервания нанесени върху ортофото мозайка

Триизмерното моделиране на теренна повърхнина е извършено с програмния продукт AutoCAD Civil 3D, като за срвнителния анализ са създадени две повърхнини. За създаването на първата са използвани точките от преки геодезически измервания (фиг. 5), а за втората идентични точки с коти отчетени от ортофото мозайката (фиг. 6).



Фиг. 5. Теренна повърхнина създадена от точки от преки геодезически измервания



Фиг. 6. Теренна повърхнина създадена чрез точки отчетени от ортофото мозайка

Стойтости на част от точките с отчетената височина от двата модела са показани в таблица 4.

Таблица 4

№ на точка	Коорд. С-ма UTM-35		преки измервания	ортофото мозайка	разлика
	X (m)	Y (m)	Hel (m)	Hel (m)	(4 - 5)
1	2	3	4	5	6
1	4656964.870	176437.042	413.784	412.580	1.204
2	4657864.696	176572.975	417.610	416.480	1.130
3	4657262.841	176294.456	412.220	411.020	1.200
4	4657242.372	175938.638	406.957	405.770	1.187
5	4656921.192	176139.541	402.394	401.210	1.184
6	4656667.848	176299.558	411.167	409.970	1.197

Заключение:

Обект на изследването е оценка на възможността за практическо използване на БЛС при триизмерно моделиране на теренна повърхнина. Сравнението на двете повърхнини показва, че разликата в отчетените височини е в интервал от 1.13 - 1.21 m, което може да се приеме за константна величина.

Направените сравнителни анализи на преките геодезически измервания и въздушното фотограметрично заснемане с дрон WingtraOne PPK потвърждава възможността за триизмерно моделиране на теренна повърхнина с необходимата точност. Привързването на създадената повърхнина към съответната височинна система може да се извърши чрез височинна транслация.

Ортофото мазайката позволява отчитането на коти в характерни точки от релефа в открити пространства и е особено полезна за съставяне на теренни повърхнини на големи площи [2], [3], [7].

Извършването на дейности по въздушното фотограметрично заснемане и обработката на изображенията с използването на БЛС оборудвана с PPK модул и технологията VTOL (vertical take-off and landing), значително съкращава разходите, времето и необходимия брой специалисти при създаване на триизмерен модел на теренна повърхнина.

ЛИТЕРАТУРА:

[1] Стойков, Е., Иванов, С., Михайлова, М.,Стоянова, Р. Използване на безпилотни летателни апарати в областта на геодезията. MATTEX 2018: Сборник научни трудове. Том 2. Част 2. Шумен: Университетско издателство "Епископ Константин Преславски", ISSN 1314-3921 (2018).

[2] Стоянов, Б.С., Стоянов, Е.С. Използване на локални цифрови филтри в съвременните геодезични методи. Втора научна конференция с международно участие - ТУ Варна, 26.09-27.09.2014г., Списание "КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ", Година XII, Брой 1/2014, с.158-163.

[3] Стоянов, Б.С., Стоянов, Е.С. Приложение на стеганографията за нуждите на геодезията и цифровата фотограметрия. MATTEX 2012, Университетско издателство ШУ "Еп. К. Преславски", том 2, стр. 176-184, ISSN 1314-3921

[4] Стоянов, Б.С., Стоянов, Е.С. Приложимост и оценка на точността на фотограметричен метод за цифровизиране на исторически архитектурни паметници. Специализирано научно издание "Дигитализация на културно-историческото наследство" - 2019 г. на НАЦИОНАЛЕН ЦЕНТЪР ЗА ДИГИТАЛИЗАЦИЯ към ННЕК – ЮНЕСКО, в печат.

[5] Bedzheva, M., Denev, D. Experimental exploration of the factors influencing on the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019).

[6] Bedzheva, M., Dobrev, S. Estimating the area of the irregular dung-hills in Shumen municipality by using unmanned aerial vehicles. Annual of Konstantin Preslavsky University of Shumen, vol. VIII E, ISSN 1311-834X, Konstantin Preslavsky University Press (2018).

[7] Bedzheva, M., Ignatova, T. Analysis of the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019).

[8] https://knowledge.wingtra.com/wingtraone-ppk

Име на автор(ите): гл. ас. д-р Кирил Янчев
Месторабота: Факултет по технически науки на Шуменски университет „Еп. Константин Преславски“, катедра „Геодезия“, България
E-mail: k.yanchev@shu.bg
Име на автор(ите): гл. ас. д-р Красимира Кирилова
Месторабота: Факултет по технически науки на Шуменски университет „Еп. Константин Преславски“, катедра „Геодезия“, България
E-mail: k.kirilova@shu.bg

REDEFINING THE CAPABILITIES OF THE UNMANNED AERIAL SYSTEM FOR THE NEEDS OF THE CADASTRE

KRASIMIRA K. KIRILOVA
KIRIL F. YANCHEV

ABSTRACT: *The report examines the capabilities of unmanned aerial vehicles equipped with new modules and systems. A real experiment evaluated the accuracy of photogrammetric surveying for geodetic activities. An analysis has been made and the possibilities for their use for creating and checking cadastral maps have been substantiated.*

KEYWORDS: *GNSS, PPK, VTOL, WingtraOne*

ПРЕДЕФИНИРАНЕ НА ВЪЗМОЖНОСТИТЕ НА БЕЗПИЛОТНАТА ЛЕТАТЕЛНА СИСТЕМА ЗА НУЖДИТЕ НА КАДАСТЪРА[1]

КРАСИМИРА К. КИРИЛОВА
КИРИЛ Ф. ЯНЧЕВ

АБСТРАКТ: *Докладът изследва възможностите на безпилотните летателни апарати, оборудвани с нови модули и системи. Реален експеримент оцени точността на фотограметричното заснемане за геодезически дейности. Направен е кратък анализ и са обосновани възможностите за тяхното използване за създаване и проверка на кадастрални карти.*

1. Въведение

Сливането на пространствени технологии като GPS и появата на достъпни платформи за пренос на тези технологии отвори нови възможности за картографиране и моделиране на кадастралните граници. Изображенията с висока резолюция от безпилотните летателни системи (БЛС) вече могат да се използват за оптимизиране на количеството на полевите нужди и предлага по-ефективно и по-богато решение за нуждите на кадастъра.

Картиращият безпилотен самолет WingtraOne VTOL (vertical take-off and landing) е способен да извърши бързи въздушни изследвания в широки или труднодостъпни области, да създава надеждни карти с несравнима разделителна способност и точност.

2. Професионални резултати и дискусия

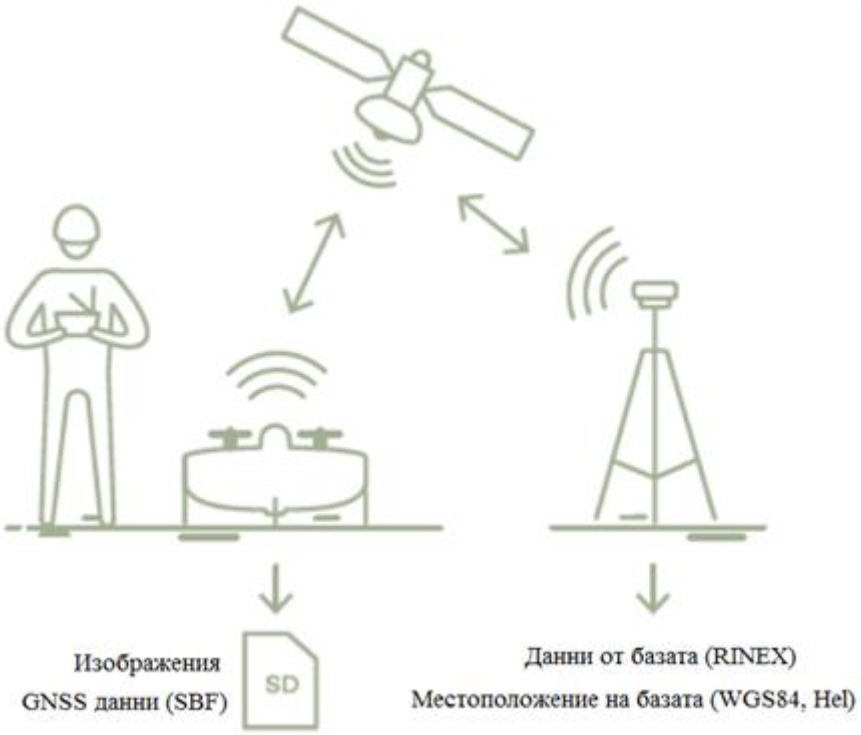
2.1. Професионалната безпилотна летателна система (БЛС) на Wingtra.

Изследването на възможността за проверка на кадастрална карта (КК) чрез използването на БЛС е извършено с дрон WingtraOne PPK (Post Processed Kinematics). Кинематика за последваща обработка (PPK), използва корекционни данни от базова GNSS станция на земята, за да коригира GNSS данните на WingtraOne от полета. Тя позволява присвояване на сантиметрови прецизни геотагове към получените изображения. Този

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

процес на географско маркиране се обработва в приложението на Windows - WingtraHub след извършване на полета (фиг. 1) [7]. Използват се следните данни:

- Изображения от камерата WingtraOne;
- GNSS данни от PPK модула WingtraOne;
- Базови файлове (RINEX) от вашата базова станция;
- Базово местоположение на базовата GNSS станция в базирана на ITRF координатна система с елипсоидна височина.



Фиг.1. Кинематика за последваща обработка (PPK)

Базовата GNSS станция може да бъде както потребителска, така и базова станция от изградената инфраструктурна GNSS мрежа. Кинематика за последваща обработка позволява да се постигне висока точност без да се маркират и координират наземни опорни (контролни) точки (ground control points - GCP). БЛС WingtraOne е оборудвана с 42MP камера Sony RX1RII, която гарантира висока резолюция на изображенията и при по-голяма височина на полета.

2.2. Обект на изследването

Обект на настоящото изследване е урбанизираната територия на село Покровник, общ. Благоевград, обл. Благоевград (фиг. 2). Селото се намира на 3 km западно от гр. Благоевград и е гъсто застроено с еднофамилни къщи с височна до 10 m. През селото преминават две малки реки и по-голямата част от улиците са асфалтирани. За населеното място на село Покровник е обявена процедура за изработване на кадастрална карта и кадастрални регистри (КККР), като за същото съществуват различни цифрови модели,

създадени чрез оцифряване на съществуващи кадастрални планове, което обуславя настоящото изследване [3], [6].

Фиг. 2. Областта на изследване - с. Покровник, общ. Благоевград, обл. Благоевград

2.3. Провеждане на измервания и обработка на резултатите.

Въздушното фотограметрично заснемане е извършено през месец Февруари 2019 г., като са проведени два последователни полета на височина 200 m. Обработката на изображенията е извършена със софуера WingtraHub поотделно за двата полета. Резюме на обработката на резултатите от първия полет са представени в таблица 1, а от втория в таблица 2.

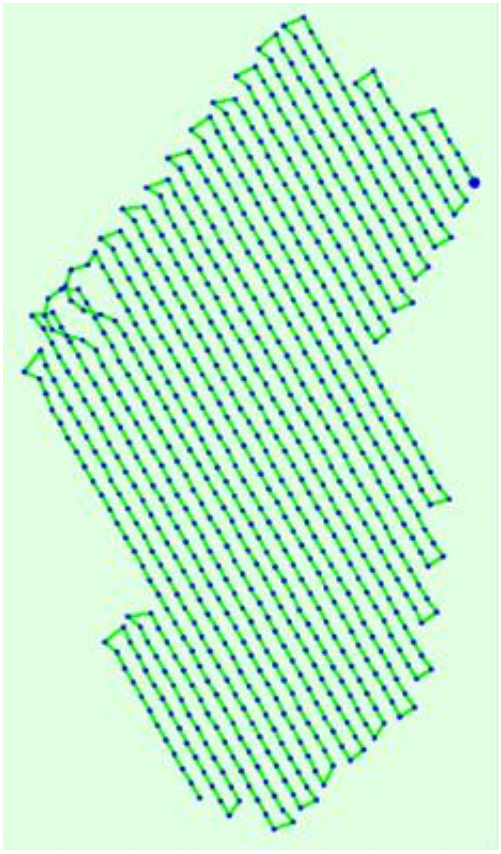
Резюме на резултатите от обработката от първия полет **Таблица 1**

Output coordinate system	Geodetic ellipsoidal height (WGS84)
PPK processed	Yes
Base file(s)	Bazz.19o
Base	PokrovnikBlagoevgrad
Base location	Cartesian ECEF (WGS84) 4368887.81500 m, 1859589.53400 m, 4244838.96600 m
Base antenna offset	East: 0.00000 m, North: 0.00000 m, Up: 0.21700 m
Detected base antenna type	HITRTK5
Matching	556 images tagged.
PPK fix	100.00%
Mean accuracy	0.03 m horizontal, 0.08 m vertical
Warnings	None

Резултати от проведените фотограметрични измервания от втория полет **Таблица 2**

Output coordinate system	Geodetic ellipsoidal height (WGS84)
PPK processed	Yes
Base file(s)	Bazz.19o
Base	PokrovnikBlagoevgrad
Base location	Cartesian ECEF (WGS84) 4368887.81500 m, 1859589.53400 m, 4244838.96600 m
Base antenna offset	East: 0.00000 m, North: 0.00000 m, Up: 0.21700 m
Detected base antenna type	HITRTK5
Matching	298 images tagged.
PPK fix	100.00%
Mean accuracy	0.03 m horizontal, 0.06 m vertical
Warnings	None

Заснетата площ е 190 ha, а траекторията на полетите е показана на фиг. 3.

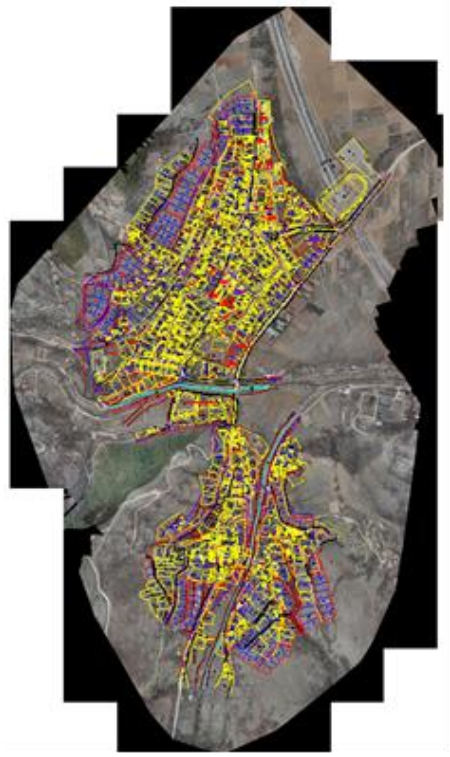


Фиг. 3. Траектория на полетите

По същото време са проведени и преки геодезически измервания с тотална станция Topcon GPT 3005LN. Обработката на резултатите от преките геодезически измервания е извършена с приложна програма за автоматизирана обработка на измерванията за геодезични мрежи и геодезични снимки – TPLAN [4], [5].

2.4. Сравнителен анализ на получените резултати.

За сравнителния анализ са обединени с програмен продукт Mkad for Windows, съществуващия оцифрен кадастрален план с жълт цвят, съществуващия оцифрен регулационен план със син и червен цвят, ортофото мозайката и точките от преките геодезически измервания (фиг. 4).



Фиг. 4. Обединен модел на получените резултати и съществуващи модели

Чрез точките от преките геодезически измервания е извършрн контрол на фотограметричното заснемане. За контролни точки са заснети капаци на шахти в различни краища на района като същите са разпознати на ортофото мозайката фиг. 5.

Фиг.5. Контролни точки

Разликата в абсолютното положение на 28 заснети и 28 разпознати контролни точки е в инервала 3 – 5 cm, което напълно отговаря на средната точност на обработените

изображения. От обединените цифрови модели и ортофото мозайката е анализирано съответствието на имотните граници и сградите от цифровия модел и съществуващите на място. От графиката ясно се виждат несъответствията на имотни граници, проложени регулационни граници, както и нови сгради, пристройки, допълващо застрояване и вече несъществуващи такива фиг. 6., фиг. 7.

Фиг. 6. Обединени цифрови модели и ортофото мозайка

Фиг. 7. Обединени цифрови модели и ортофото мозайка

Заключение:

Обект на изследването е възможността за проверка на кадастрална карта чрез използването на БЛС [1], [2], [7]. Направените сравнителни анализи на преки геодезически измервания и въздушното фотограметрично заснемане с мултикоптер (дрон) WingtraOne PPK се потвърждава възможността за нанасяне на разпознати имотни граници в КК с необходимата точност.

Ортофото мазайката е особено полезна за нансяне на вътрешни имотни граници, които са трудни за заснемане с преки геодезически измервания, отнемат значително време и са ангажирани сравнително голям брой специалисти [5]. Налага се поставянето на операционни точки, което от своя страна понижава точността на определяне в планово и височнно положение на точките.

Чрез обединяването на цифровите модели и ортофото мозайката е възможно да се направи пълен подробен анализ на изходните данни за създаване на КК. Това дава възможност максимално да се оптимизира разчета на техниката, необходимите специалисти, точното местоположение и времето, необходими за извършване на допълнителни полски дейности по създаване на КК.

Дейностите по въздушното фотограметрично заснемане и обработката на изображенията на обеката с площ от 180 ha, предмет на настоящото изследване, са извършени от един специалист в рамките на един работен ден, което значително съкращава времето и разходите на полските работи по създаване на КК, както и за проверка на изготвени кадастрални карти.

Оборудването на БЛС с PPK модул и технологията VTOL (vertical take-off and landing) предефинира възможностите на въздушното картографиране и го отвежда към съвсем нов етап в неговото развитие.

ЛИТЕРАТУРА:

[1] Стоянов, Б.С., Стоянов, Е.С. Използване на локални цифрови филтри в съвременните геодезични методи. Втора научна конференция с международно участие - ТУ Варна, 26.09-27.09.2014г., Списание "КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ", Година XII, Брой 1/2014, с.158-163.

[2] Стоянов, Б.С., Стоянов, Е.С. Приложение на стеганографията за нуждите на геодезията и цифровата фотограметрия. MATTEX 2012, Университетско издателство ШУ "Еп. К. Преславски", том 2, стр. 176-184, ISSN 1314-3921

[3] Стоянов, Б.С., Стоянов, Е.С. Приложимост и оценка на точността на фотограметричен метод за цифровизиране на исторически архитектурни паметници. Специализирано научно издание "Дигитализация на културно-историческото наследство" - 2019 г. на НАЦИОНАЛЕН ЦЕНТЪР ЗА ДИГИТАЛИЗАЦИЯ към ННЕК – ЮНЕСКО, в печат.

[4] Bedzheva, M., Denev, D. Experimental exploration of the factors influencing on the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019).

[5] Bedzheva, M., Dobrev, S. Estimating the area of the irregular dung-hills in Shumen municipality by using unmanned aerial vehicles. Annual of Konstantin Preslavsky University of Shumen, vol. VIII E, ISSN 1311-834X, Konstantin Preslavsky University Press (2018)

[6] Bedzheva, M., Ignatova, T. Analysis of the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019)

[7] https://knowledge.wingtra.com/wingtraone-ppk

Име на автор(ите): гл. ас. д-р Красимира Кирилова
Месторабота: Факултет по технически науки на Шуменски университе „Еп. Константин Преславски“, катедра „Геодезия“, България
E-mail: k.kirilova@shu.bg
Име на автор(ите): гл. ас. д-р Кирил Янчев
Месторабота: Факултет по технически науки на Шуменски университе „Еп. Константин Преславски“, катедра „Геодезия“, България
E-mail: k.yanchev@shu.bg

CARTOGRAPHIC APPLICATIONS FROM REMOTE METHODS

SABIN I. IVANOV

ABSTRACT: *The report looked at cartographic applications derived from remote methods, relief modelling methods, stereophotogrammetric techniques using aerial photographs, and the application of thematic cartography*

KEYWORDS: *remote, digital model, relief, thematically*

КАРТОГРАФСКИ ПРИЛОЖЕНИЯ ОТ ДИСТАНЦИОННИ МЕТОДИ[1]

СЪБИН И. ИВАНОВ

АБСТРАКТ: *В доклада са разгледани картографските приложения, получени от дистанционните методи, начините за моделиране на релефа, стереофотограметричните техники, използващи въздушни снимки, както и приложението на тематичната картография..*

1 Въведение

Картографирането е неразделна част от процеса на управление на земните ресурси. Картографираната информация често е резултат от анализ на данни, получени от сензори за дистанционно наблюдение на земната повърхност. Платформите за дистанционни сензори може да бъдат разположени на земята, на самолет или на космически кораб или спътник извън Земята.

2 Изложение

Картографските приложения, получени от дистанционно наблюдение, включват следното:

1.планове;

2.цифрови модели на релефа (DEM);

3.основни тематични и топографски карти.

• Планове

Плановете са мащабни изображения, които идентифицират и определят местоположението на обекти от земната покривка (например гора, блато) и антропогенни особености (например градска инфраструктура, транспортни мрежи) в двумерната равнина (x, y). Планиметричната информация обикновено е необходима за едромащабни

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

приложения за градско картографиране, управление на съоръженията, военно разузнаване и обща информация за ландшафтната покривка.

Геодезичните методи, напоследък придружени с използването на ГНСС се използват за постигане на прецизни изисквания за точност. Ограниченията на геодезичните измервания са свързани с ефективност на разходите и трудности при картографиране на големи или отдалечени райони. Дистанционното изследване осигурява средство за идентификация и набавяне на планиметрични данни по бърз, удобен и по-ефикасен начин. Изображенията могат да са в различни мащаби, за да отговарят на изискванията на различни потребители.

• Цифров модел на релефа

Цифровият модел на релефа (ЦМР) съдържа надморските височини на равномерно разпределени по земната повърхност точки. Съществуват редица начини за генериране на цифрови модели на релефа. Най-често числените стойности на височините се получават чрез преки геодезични измервания на точки от терена, които след провеждане на интерполационни процеси формират т.н TIN (Triangulate irregular network) или GRID (Global Resource Information Database) модели. Тези две групи модели създават продукти наречени цифрови модели на релефа или Digital Elevation Models (DEMs). По нататък чрез тях се моделира релефа, който представя характера на земната повърхнина посредством линейни знаци: профили, перспективни линии и изолинии (хоризонтали). Профилите, перспективните линии и изолиниите се получават при мисленно пресичане на повърхнината със серия от успоредни равнини, еднакво отстоящи една от друга. Сеченията определят линии, които проектираме върху приетата за картата “изходна” равнина. Най-използваният картографски метод за изобразяване на повърхнина е методът на изолиниите, особено в традиционните топографски карти.

Описания по-горе начин за моделиране на релефа, получен от мрежа от точки в които са извършени измервания за определяне на тяхното местоположение x и y и третата координата - надморската височина, отнема изключително много време и усилия.

Генерирането на ЦМР от сензорни данни, получени с прилагане на дистанционни методи може да бъде рентабилно и ефективно. През последните години са налични различни сензори и методологии за генериране на такива модели и са доказани картографски приложения. Два основни метода се използват за създаване на ЦМР с данни за надморски височини (Canada Centre for Remote Sensing, Fundamentals of Remote Sensing, 2017):

- ❖ стереофотограметрични техники, използващи въздушни снимки (фотограметрия) или радарни данни (радаргграметрия);
- ❖ радарна интерферометрия.

Стереофотограметрията включва извличане на информация за височините от припокриващи се стереоизображения, обикновено от въздушни снимки, SPOT или радарни изображения. Хоризонталите (линии с една и съща височина) могат да бъдат проследени по изображенията чрез оператори, които постоянно поддържат изображенията в стерео ефект.

Интерферометрията включва събиране на точни данни за надморските височини с помощта на последователни космически или въздушни повторни SAR (Synthetic Aperture Radar) преминавания над заснемената зона или се използват две пространствено разделени антени.

SAR системите са радиолокационни системи, установени на борда на космически апарат, които излъчват електромагнитни вълни към земната повърхност и регистрират амплитудата и времето на задържане или фазата на отразените сигнали, за да се формира радиохолограма на наблюдаваната повърхност (Атанасова, М. 2011). Интерферометричната преработка се базира на използването на разликите в нивото на сигналите, излъчвани от спътника и отразени от повърхността на Земята. Генерира се цифров височинен модел на терена (DEM- Digital elevation model) за всяка снимка.

- **Топографско и тематично картографиране**

В последните години на информационния век все повече нараства търсенето на цифрови бази данни с топографска и тематична информация. Топографските карти съдържат релефа, представен с хоризонтали, които представят надморските височини и ситуационни подробности в разнообразни мащаби.Те служат главно като обща основна информация за граждански и военни цели.

Основното тематично картографиране интегрира спътникови изображения, земеползване, земна покривка и топографски данни в цифров вид. Тази нова концепция за тематичното картографиране е разработена, за да се възползваме от цифровата обработка и интегриране на пространствена информация от множество източници на данни чрез широкото използване на географски информационни системи за синтезиране на информация, извършване на анализи от потребителя и възможността за представяне на данните в картографска форма.

Данните за основните тематични карти са съставени от топографска база данни и добавяне на инфраструктурни бази данни, данни за земна покривка, климата, население и други данни. Подходящата тематична информация се наслагва върху базова карта, като се предоставя конкретна информация за конкретни крайни потребители. Различни комбинации от тематична информация могат да бъдат показани, за да се състави карта за специфични приложни цели.

3 Заключение

Основните тематични и топографските карти, получени с помощта на дистанционните методи са от съществено значение за планиране, оценка и мониторинг, за военни или граждански цели или управление на земеползването, особено ако информацията е цифрово интегрирана в географски информационна система като информационна база. Интегрирането на информацията с височини е от решаващо значение за много приложения и често е ключът към потенциалния успех на съвременните програми за картографиране.

ЛИТЕРАТУРА:

[1] Добрев, С. Анализ на геодезическите методи за изследване деформациите на хидротехнически обекти. Научна конференция с международно участие МАТТЕХ 2018, гр. Шумен (2018).

[2] Казаков Ст., „Resources and organization of processes in logistics engineering“, International scientific refereed online journal with impact factor, ISSUE 69 MAY 2020, ISSN 2367-5721.

[3] Михайлов Пл., Стойков Е., "Измервания с GPS и обработка – анализ на получените резултати", научна сесия с международно участие МАТТЕХ, ШУ “Епископ Константин Преславски” (2012).

[4] Стойков Е., Ниязи М., Райнова П., "Съвременни информационни и GPS технологии - аспекти и последици от тяхното приложение", научна конференция с международно участие МАТТЕХ 2014, ШУ "Епископ Константин Преславски" (2014).

[5] Kirilova K. "Methodology for establish a local model of geoid (quasigeoid) in mountain and high mountain areas" Годишник на ШУ "Еп. К. Преславски" Технически науки. Том IX E, Шумен, Университетско издателство "Епископ Константин Преславски", стр. 86-91, ISSN: 1311-834X.

[6] Yankova-Yordanova, Y., Innovative methods for improving transport forwarding service. SocioBrains, www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva, Bulgaria, Issue 70, June 2020, pp. 76-80, ISSN 2367-5721.

[7] Yanchev K. Methods for presenting, processing and interpreting the results of geodetic observations of geodynamic processes, Годишник на ШУ "Еп. К. Преславски" Технически науки. Том IX E, Шумен, Университетско издателство "Епископ Константин Преславски", стр. 55-60, ISSN: 1311-834X.

Име на автор: Събин Иванов
Месторабота: ШУ „Еп. К. Преславски“
E-mail: s.ivanov@shu.bg

DIGITIZATION RULES

SABIN I. IVANOV

ABSTRACT: *The report highlights some basic principles in digitisation, especially those related to how to avoid errors during the digitisation process.*

KEYWORDS: *digitisation, Identify, Attributes, vector data*

ПРАВИЛА ПРИ ДИГИТАЛИЗИРАНЕ[1]

СЪБИН И. ИВАНОВ

АБСТРАКТ: *В доклада са подчертани някои основни принципи при дигитализирането, особено тези свързани с това как да се избегнат грешките по време на процеса на дигитализиране.*

1 Въведение

Дигитализирането е монотонна работа и по тази причина въвеждането на една карта става по-скоро на части отколкото наведнъж. Това изисква ясна дефиниция за планиране на процеса на дигитализиране и да се разработи метод за идетифициране на отделните части на картата. Тук ще подчертаем някои основни принципи при дигитализирането, особено тези свързани с това как да се избегнат грешките по време на процеса на дигитализиране. Първото правило естествено е свързано с избора на подходящите данни за въвеждане в базата данни. От картографска гледна точка, главният фактор при проектиране на една карта е да се дефинира целта на картата и намерението на потребителя. Те ще са определящите фактори за избора на приоритетните бази данни. Второто правило е свързано с точността на изходните карти, което изисква да се използват най-точните данни, необходими за създаване на ГИС базата данни. Дори за много специфични цели има много начини за получаване на пространствена информация, включително най-новата ГНСС технология. При наличие на традиционни източници с достатъчна за целите точност е добре да се разчита на тях. Въпросът със сложността на информацията при моделиране на обектите формулира третото правило. При векторните ГИС всяка въведена линия може да съдържа криви. При очертаване на по-сложни обекти, едно просто правило е да се дигитализират повече точки. Например, за да се очертае точно копие на крива линия се дигитализират отделни линейни сегменти. Местоположението на сегмента (права линия) може да бъде определен само с две точки, по една в началото и в края. Този процес много прилича на картографската генерализация.

2 Изложение

- **Правила при векторен метод на дигитализиране**

Методът на дигитализиране е свързан със структурата на данните. Правилата са различни за различните софтуерни пакети. При едни се изисква да се покаже

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

местоположението на възлите, а при други не, някои изискват да се построи топология след построяване на базата данни, други да се кодират топологичните данни по време на дигитализирането и т.н. При векторните ГИС, атрибутите най-често се въвеждат с клавиатурата на компютъра. Добра практика е атрибутите да се проверяват в момента на въвеждането им.

- **Правила при растерен метод на дигитализиране**

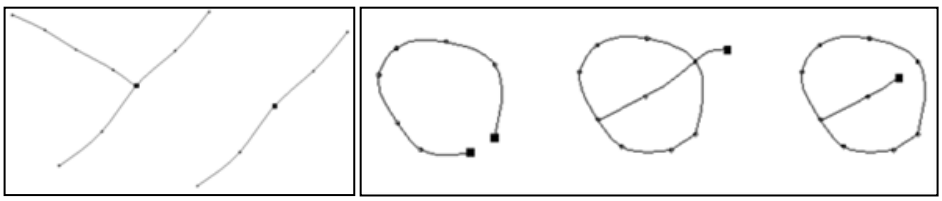
Съдържанието на информацията при растерните данни се основава на правилото: по-малките обекти се моделират с по-малки grid клетки (DeMers, 1992). Този принцип често определя избора на размера на клетките (резолюцията) при въвеждане на растерни данни. И в двата случая, при векторните и растерните ГИС, моделирането е зависимо от обхвата на картографираната територия и въведените данни за нея.

- **Грешки при дигитализиране**
  - ❖ **Графични грешки**

Много грешки се допускат при дигитализиране, особено при грешно натискане на бутоните. Основно, грешките се класифицират като графични и атрибутни. Други грешки са основани на средата в която се извършва процеса на дигитализиране. Те също могат да се ограничат до минимум и предимно са свързани с условията за климатизиране на помещенията. Повечето ГИС софтуерни продукти осигуряват възможности за идентифициране и поправяне на грешките от дигитализирането.

По нататък, ще представим някои от най-често срещаните видове грешки при дигитализирането и възможностите за тяхното отстраняване. Първият тип грешки са свързани с неточно дигитализиране на точкови обекти. Възможни са два случая на грешки – допускане на псевдовъзли и висящи възли. Известно е, че във векторните модели възлите са специфични точки, които свързват две линии, формирани от множество линейни сегменти. Тук трябва да се подчертае, че линейните сегменти са съставени от свързване на точкови обекти, наречени върхове.

Подходящ пример за възел е пресечната точка на две реки, съставени от множество линейни сегменти. Обикновено появата на псевдовъзел се допуска при натискане на грешен бутон.



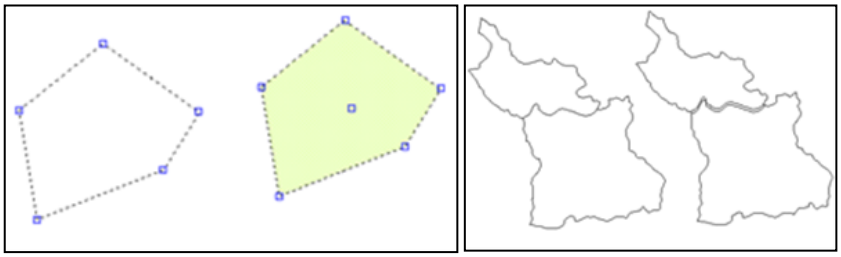
Фигура 1. Грешки при дигитализиране на точкови обекти

а) нормален възел; б)псевдовъзел; в) висящ възел формиращ: 1) незатворен полигон; 2) пресичане на линия; 3) недостигане до линия

Коригирането се извършва лесно чрез изтриване на грешните псевдовъзли и добавяне на други на правилните места. Друга подобна грешка е допускане на висящи възли, които причиняват следните резултати: незатворени полигони, пресичане на линия или

недостигане до линия. Тези грешки са в резултат на недостатъчно прецизно “прихващане” на точки от линиите. В резултат се получават незатворени полигони. За незатворени полигони се разбира по броя на създадените такива в базата данни. Ако техният брой е по-малък от броя на дигитализираните, означава, че имаме незатворени полигони. По трудно се откриват грешките свързани с пресичане на линии или недостигане на една линия до друга, макар че редактирането се извършва лесно. При отворен полигон трябва само да се премести едната точка до другата; ако имаме недостигане на една линия до друга или да се премести точката, така че да се свърже с другата линия; и ако имаме пресичане на линия, тя се отрязва в точката на пресичане. За извършване на редактиране на всички тези случаи, грешките се забелязват при увеличен визуален мащаб. Разбира се, за идентифицирането им преди това се използват възможностите на софтуера. Тези грешки са показани на фиг.1.

Другата категория грешки са свързани с дигитализиране на полигоните (фиг.2). Известно е, че местоположението на полигонов обект се характеризира с контура определен от ограждащите го точки, а информацията за него с етикетна точка, чието местоположение е в околността на полигона. Често се случва да липсва или да има повече от една етикетна точка. В такъв случай или няма възможност да се “прикачи” атрибутна информация за този полигон или тя ще се дублира. Редактирането е просто – в зависимост от случая или се добавя, или се изтриват излишните етикетни точки.



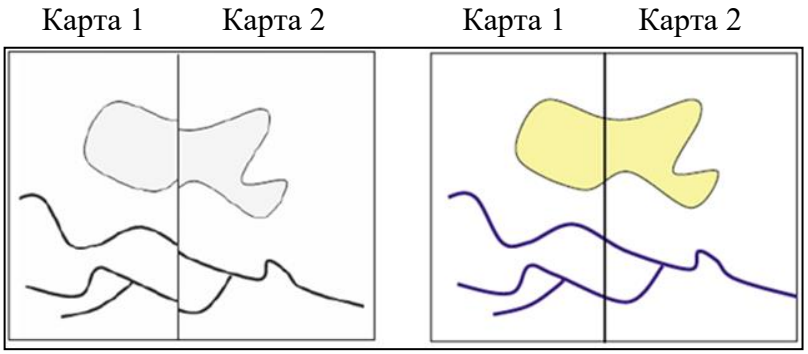
а) б) в) г)

Фигура 2. Дигитализиране на полигони

а) без етикетна точка;б) с етикетна точка; в) правилна обща граница; г) неправилна дигитализирана обща граница

Други грешки при дигитализиране на полигоните, които често се получават е, когато се дигитализират едни и същи линии на съседни полигони. Например, ако се дигитализират държавни граници и за да се формират отделни полигони за две съседни държави, общата граница трябва да се дигитализира два пъти. При повтаряне на границата почти е невъзможно да се “прихванат” същите точки от първото дигитализиране и резултатът е получаване на прекалено тесен полигон между идентичните линии. Много трудно се откриват такива полигони. За отстраняването на такава грешка в повечето случаи има софтуерно решение със специална функция, която проследява първоначално дигитализираната линия.

Други грешки, които могат да се появят при дигитализирането са когато се съединяват картните листи (фиг.3). Грешките от разтеглянето на хартиените карти се поправят чрез трансформационни процедури преди процеса на дигитализиране. Тази операция в софтуерните продукти е наречена rubber sheeting или метод на гумената лента.



Фигура 3. Пример за сходка на картни листи

❖ **Атрибутни грешки**

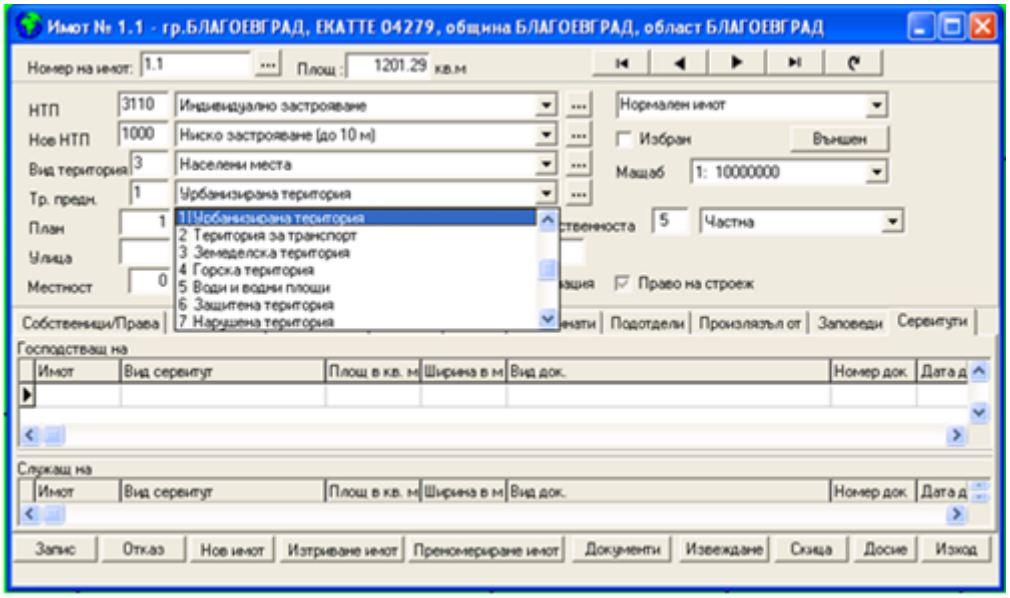
Няма правила по които ГИС може да извърши проверка на точността на атрибутите, тъй като не е известно кои от тях са верни и кои не са. Като цяло атрибутните грешки могат да се разделят на две групи: пропуснати атрибути и неправилно въведени атрибутни стойности. При векторните и растерните данни атрибутите значително се различават, поради което откриването на грешките също ще е различно.

Пропуснатите атрибутни стойности при растерите най - често се представят като изпуснат ред или колона, които се причиняват от кодиране на клетките. Ако се използва софтуер за написване на кодовете, ГИС подсказва редът, като данните се въвеждат ред по ред. Ако те се въвеждат без помощта на софтуер, възможността за изпускане на стойностите се увеличава. Пропуснатите атрибутни стойности при векторните данни просто представляват невключени атрибути за точкови, линейни или полигонови обекти в атрибутните таблици.

Неправилно въведените атрибутни стойности са трудно откриваеми, както при растерните, така и при векторните данни. При единичен случай на сгрешен ред или колона при растерите, грешката най-често се дължи на грешно въведена атрибутна стойност. В случай на неправилно въведени стойности за голяма територия, те най-вероятно са резултат от неправилно въведени стойности по време на дигитализиране. Неправилните стойности при векторните данни са по-трудно откриваеми, отколкото при растерните. Обикновено се използва кодираща система, която свързва кодове с действителните имена на въвежданите точкови, линейни или полигонови обекти. На фиг.4 е показано въвеждането на данни за имоти с български програмен продукт, съгласно Закона за кадастъра и имотния регистър в България.

Примерът показва избор на територията по предназначение за полигонов обект (имот). В случая от падащото меню се избира “урбанизирана територия”, което означава, че имотът е в населеното място. Допускането на грешка в кодирането трудно ще се забележи в атрибутната таблица, но в картата грешката е забележима.

В нашия пример, при избран код “1” имотът трябва да бъде в населеното място. Ако сме сгрешили и сме написали код “2” за земеделска територия, картографският знак ще съответства на площна територия оцветена в жълто. При визуализация с картографския си знак, съответстващ на дадения му код “2”, имотът значително ще се отличава от съседните имоти, също принадлежащи на урбанизираните територии.



Фигура 4. С падащо меню се избират кодове, отговарящи на територии с различно предназначение

ЛИТЕРАТУРА:

[1] Добрев, С. Анализ на геодезическите методи за изследване деформациите на хидротехнически обекти. Научна конференция с международно участие МАТТЕХ 2018, гр. Шумен (2018).

[2] Казаков Ст., „Resources and organization of processes in logistics engineering“, International scientific refereed online journal with impact factor, ISSUE 69 MAY 2020, ISSN 2367-5721.

[3] Михайлов Пл., Стойков Е., "Измервания с GPS и обработка – анализ на получените резултати", научна сесия с международно участие МАТТЕХ, ШУ “Епископ Константин Преславски” (2012).

[4] Стойков Е., Ниязи М., Райнова П., "Съвременни информационни и GPS технологии - аспекти и последици от тяхното приложение", научна конференция с международно участие МАТТЕХ 2014, ШУ “Епископ Константин Преславски” (2014).

[5] Kirilova K. "Methodology for establish a local model of geoid (quasigeoid) in mountain and high mountain areas" Годишник на ШУ "Еп. К. Преславски" Технически науки. Том IX Е, Шумен, Университетско издателство "Епископ Константин Преславски", стр. 86-91, ISSN: 1311-834X.

[6] Yanchev K. Methods for presenting, processing and interpreting the results of geodetic observations of geodynamic processes, Годишник на ШУ "Еп. К. Преславски" Технически науки. Том IX Е, Шумен, Университетско издателство "Епископ Константин Преславски", стр. 55-60, ISSN: 1311-834X.

[7] Yankova-Yordanova, Y., E. Konstantinova, Ts. Tsankov, Forecasting logistics systems through models. SocioBrains, www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva, Bulgaria, Issue 68, April 2020, pp. 105-109, ISSN 2367-5721

Име на автор: Събин Иванов
Месторабота: ШУ „Еп. К. Преславски“
E-mail: s.ivanov@shu.bg

SEA MAPS - HISTORY AND FUTURE

EVGENI G. STOYKOV

ABSTRACT: *Prior to the founding of the hydrographic organizations, the captains were responsible for the supply of sea maps. This means that ships often sailed with non-compliant information for safe navigation and that when new waters were found, information often did not reach everyone who needed it.*

KEYWORDS: *Hydrographic study, Sea map, Navigation*

МОРСКИ КАРТИ – ИСТОРИЯ И БЪДЕЩЕ[1]

ЕВГЕНИ Г. СТОЙКОВ

АБСТРАКТ: *Преди основаването на хидрографските организации капитаните били отговорни за снабдяването с морски карти. Това означава, че често корабите плавали с несъответстващи информация за безопасно навигиране и че при откриването на нови води често информацията не стигала до всички, които се нуждаели от нея.*

1 Въведение

Първите опити за създаване на морски карти принадлежат на хората от тихоокеанските острови. Такава карта е запазена от Маршаловите острови (около 2000 г. пр.н.е.), в която няколко раковини, изобразяващи острови, са заплетени в мрежа от пръчки.

Възникването на географията е една от предпоставките за създаване на точни карти. Древногръцките учени (Ератостен, Хипарх, II в. пр. н.е.) разкриват сферичната форма на Земята, въвеждат понятията за координати (географска ширина и дължина) и съставят първите карти на света на районите, които са познавали, т.е. Средиземно море и прилежащите му части от Европа, Азия и Африка (Фиг.1).

Фиг.1

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

От най-дълбока древност са формулирани основните посоки на света – север, юг, изток и запад, обосновани с видимото движение на Слънцето. Древногръцките моряци се опитват да създадат точна система за определяне на посоките, по-известна като морска роза. Една от първите е морската роза, построена с център остров Родос, която разделя хоризонта на 12 части. През средните векове тази система се създава с все повече деления, които са назовани румбове.

2 Изложение

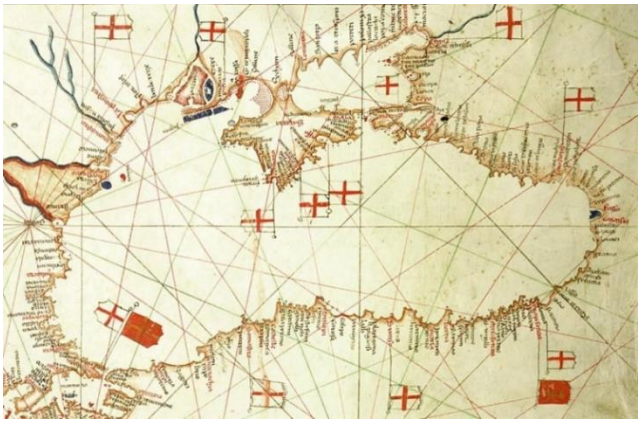
Първият създаден инструмент за навигационни измервания е компасът. Първообразът му е изобретен от китайците, вероятно преди новата ера, и може само да определя посоката север. През XI в. италианецът Джойя изработва компас, удобен за използване при корабоплаване. Развитието на морския компас го превръща в прибор за измерване на всички посоки, които са формулирани като азимути или курсове, а повишаването на точността му довежда до утвърждаването на градуса като мерна единица за ъгъл в навигацията. Морската роза е преименувана на „компасна“ и е начертана на компаса, а след това и на морските карти.

През древността в Близкия изток се изучават звездите и са очертани съзвездията. Особено внимание се отделя на Полярната звезда, която се използва за ориентиране, а след изобретяването на астролабията (II век пр.н.е., която представлява астрономически уред) – и за определяне на географската ширина.

През Ранното средновековие в Европа се превеждат и изучават книгите на арабските и древногръцките учени, а също така започва и изработването на компаси и астролабии. Европейците строят все по-големи и сигурни кораби, като важен етап е построяването на ветроходни кораби, които могат да се движат и срещу вятъра. С развитието на западноевропейските страни се стига до нови икономически възможности и търсения, включително Великите географски открития. Тези открития са извършени след продължителни и опасни плавания, за което свидетелства големият процент на загубени хора и кораби. В навигационно отношение рискът е особено голям: в повечето случаи мореплавателите нямат карти, пълноценното определяне на координатите все още е невъзможно, състоянието на времето се оценява на око и прогнози се правят на основата само на наблюдаваните местни признаци. В днешно време е трудно да си представим, че великият мореплавател Колумб стига до отчаяние, когато на връщане от Америка попада в буря и губи представа за своето място и най-вече за географската дължина, т.е. какво разстояние му остава до брега. Първите карти „портолани“ са изработени през XIII в. (фиг.2), и показват бреговата линия с много детайли. Те са били особено полезни при опознаването на брега. Отличителен белег на портолана е розетката от прави линии, които се използват за определяне на посоката към желания краен пункт. Но и тези карти са неточни и не дават координатите на обектите. Те са изработвани на ръка и са били скъпи и редки.

Бързото развитие на картографията създава различни типове представяния на земната повърхност върху равнината на картата, наречени проекции. Специфичните изисквания на навигацията в най-голяма степен удовлетворява проекцията, създадена от холандеца Г. Меркатор през 1569 г. На картите, създадени от Меркатор, меридианите са успоредни вертикални прави, а паралелите – успоредни хоризонтални прави. При еднаква разлика в координатите, например 10^0, разстоянията между меридианите са еднакви, а между паралелите нарастват от екватора към полюса. Курсът на кораба, сключващ постоянен ъгъл с меридиана, е права линия. Лесното начертаване на курсовете и пеленгите, както и лесното

преминаване от проплавани разстояния към координати на крайната точка, са основните предимства на меркаторската карта. Тя е най-разпространената морска карта и днес (фиг.3).



Фиг.2. Портолан от 1489 г. Показан е районът на Черно море

Фиг.3

Според Международната хидрографска организация (International Hydrographic Organization – IHO) [1]: *Хидрографията е отрасълът на приложните науки, който се занимава с измерването и описанието на физическите характеристики на океаните, моретата, крайбрежните зони, езерата и реките, както и с прогнозирането на тяхната промяна с течение на времето, с основна цел безопасността на навигацията и в подкрепа на всички други морски дейности, включително икономическо развитие, сигурност и отбрана, научни изследвания и опазване на околната среда.*

Произходът на хидрографията лежи в направата на помощни карти за корабна навигация от отделни моряци, които плавали в непознати води. Картите обикновено били частна собственост, понякога съдържащи тайни, на хора, които ги използвали за комерсиални или военни изгоди. С разрастването на трансокеанската търговия хидрографските проучвания започват да се извършват редовно, а изследванията се правят все повече от правителствата и специални хидрографски служби. Националните организации, особено военноморските сили, осъзнават, че събирането, систематизирането и разпространението на тези знания дават големи организационни и военни преимущества. В тази връзка се раждат специалните национални хидрографски организации за събиране, организация и разпространение на хидрографска информация, включвана в карти и

плавателни инструкции. Хидрографските изследвания в Западна Европа започват към края на XVII и началото на XVIII век. През 1805 г. контраадмирал Франсис Бофорт създава едноименната скала, а по-късно въвежда и първите официални приливни таблици.

Едромащабната хидрография обикновено се предприема от национални или международни организации, които спонсорират събирането на данни чрез точни изследвания и публикуват карти и описващи документи за навигационни цели. Океанографията частично възниква вследствие на хидрографията. В много отношения данните са взаимозаменяеми, но все пак морските хидрографски данни се използват специално за морска навигация. Морските изследвания за ресурси, особено въглеводороди, представляват значителна част от приложенията на хидрографията.

Хидрографските измервания включват информация за приливи и отливи, океански течения, информация за вълните и измервания на океанското дъно, с акцент върху тези географски особености, които могат да представляват опасност за корабоплаването (например скали, рифове, плитчини и други). Дънните изследвания включват събирането на дънна флора и фауна, тъй като те имат отношение към ефективното закотвяне. За разлика от океанографията, хидрографията включва още характеристики на бреговете – естествени и създадени от човека, които биха помогнали на корабната навигация. Следователно хидрографските изследвания могат да включват точното местоположение на скали, планини, фарове и кули, които биха помогнали за определянето на позицията на плавателния съд.

Поради причини за сигурност хидрографията е приела редица конвенции, които засягат изразяването на данните на морските карти. Например хидрографските карти се изработват така, че да изобразяват това, което е безопасно за корабоплаване, и затова обикновено показват най-малката възможна дълбочина, а понякога пренебрегват реалната подводна топография, която се описва чрез батиметрични карти. Докато първите карти служат на моряците, за да избегнат инциденти, вторите карти служат на учените за изследвания с реални числа. С времето разликите между двата вида карти постепенно се размиват. В днешно време морските изследвания често събират различни данни едновременно, така че едни и същи данни да могат да бъдат използвани едновременно за хидрографски и батиметрични изображения.

Въпреки че хидрографските данни в някои части на света са достатъчно, за да изобразяват детайлно релефа на дъното, те показват дълбочинна информация по отношение на безопасното корабоплаване и не следва да се считат за продукт, който точно изобразява формата на дъното. Рядкостта на точната дълбочинна информация също засяга безопасната навигация. В изолирани райони единствената дълбочинна информация е събрана чрез оловни пръти. Този метод включва спускането на оловни пръти от плавателен съд до дъното на определени времеви интервали. Няма данни за дълбочината между две измервания.

Измерванията на теченията включват информация за коритото на течението, анализ на водата и заобикалящата суша. Хидрографията за водосборните басейни обръща специално внимание на реките и питейната вода. Все пак ако данните не служат за корабоплаване, а за научно ползване, тогава става дума за хидрология. Хидрографията на реки и потоци е важна част от управлението на водите. Използват се ръчни и брегово монтирани устройства, за да се отчете дебитът на водата през даден участък.

3 Заключение

Хидрографията е ключът към напредъка по всички морски дейности, които обикновено са с голямо национално икономическо значение. В тази връзка трябва да се обърне адекватно внимание на области като [1]:

- Безопасно и ефективно управление на морския трафик;
- Управление на крайбрежните зони;
- Проучване и използване на морските ресурси;
- Опазване на околната среда;
- Морска отбрана.

За тази цел е създадена хидрографската служба. Хидрографската служба чрез системно събиране на данни, извършвани на брега и в морето, произвежда и разпространява информация в помощ на морската навигационна безопасност, опазването на морската среда и отбраната.

ЛИТЕРАТУРА:

[1] International Hydrographic Organization, Manual on Hydrography, Publication C-13, May 2005, (Corrections to February 2011), Chapter 1, 2 and 3.

[2] Стойков, Е. "Технически средства и системи при извършване на хидрографски измервания", Университетско издателство "Епископ Константин Преславски", 177 стр., ISBN 978-619-201-334-9

[3] Ivanov, S. "Determination of visibility between card points". Journal scientific and applied research, Volume 13, 36 -40 стр, ISSN: 1314-6289. Лицензирано в EBSCO , USA. 2018 г.

[4] Добрев, С. Анализ на геодезическите методи за изследване деформациите на хидротехнически обекти. Научна конференция с международно участие МАТТЕХ 2018, гр. Шумен (2018).

[5] Иванов, С. "Определяне на точката на стоене по топографска карта". МАТТЕХ 2018: Сборник научни трудове. Том 2. Част 2. Шумен: Университетско издателство "Епископ Константин Преславски", 134 - 140 стр. ISSN: 1314-3921. 2018 г.

[6] Stoyanov, B., Stoyanov, E.,"The usage of new technologies for collecting spatial data and ways of application in archeoastronomy", Publications of the Astronomical Society of Bulgaria (PASB), 2016. , available at: http://astro.shu-bg.net/pasb/index_files/Papers/2016/Stoyanov.pdf , retrieved on 01.12.2016.

[7] Стоянов, Б., Стоянов, Е., Използване на локални цифрови филтри в съвременните геодезични методи, Втора научна конференция с международно участие - ТУ Варна, 26.09-27.09.2014г., Списание "КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ", Година XII, Брой 1/2014, с.158-163.

[8] Стоянов, Е., Стоянов, Б., „Приложение на стеганографията за нуждите на геодезията и цифровата фотограметрия", МАТТЕХ 2012, 22.11-24.11.2012, ШУ "Еп. К. Преславски",том 2, ISSN: 1314-3921. 2012 г.

[9] Bedzheva, M., Dobrev, S. „Estimating the area of the irregular dung-hills in Shumen municipality by using unmanned aerial vehicles", Annual of Konstantin Preslavsky University of Shumen, vol. VIII E, ISSN: 1311-834X, pp. 166-173, Konstantin Preslavsky University Press 2018 г.

[10] Казаков, С., "Систематизиране на информационни потоци в логистиката" е от НВУ в Годишна университетска научна конференция 2020 В. Търново.

[11] Казаков, С., Йорданова, Йо., "Typology of risks in RFID", Journal scientific And Applied Research 2017.

Име на автора: Евгени Гришев Стойков
Месторабота: ШУ „Епископ Константин Преславски"
E-mail: e.stoykov@shu.bg

BASIC PRINCIPLES OF HYDROGRAPHIC RESEARCH

EVGENI G. STOYKOV

ABSTRACT: *The main objective of most hydrographic studies is to obtain basic data for the compilation of navigation maps with a focus on characteristics that may affect safe navigation. The sea map is the final product of hydrographic exploration. Its accuracy and consistency depend on the quality of the data collected during the studies.*

KEYWORDS: *Hydrographic study, Sea map, Navigation*

ОСНОВНИ ПРИНЦИПИ НА ХИДРОГРАФСКИТЕ ИЗСЛЕДВАНИЯ[1]

ЕВГЕНИ Г. СТОЙКОВ

АБСТРАКТ: *Основната цел на повечето хидрографски проучвания е да се получат основни данни за съставянето на навигационни карти с акцент върху характеристиките, които могат да засегнат безопасната навигация. Морската карта е крайният продукт на хидрографското проучване. Точността и съответствието й зависят от качеството на данните, събрани по време на проучванията.*

1 Въведение

Хидрографското проучване разглежда конфигурацията на дъното и съседните земни площи на океани, езера, реки, пристанища и други водни форми на Земята. В строгия смисъл на думата то се определя само като геодезия на водна площ, но в съвременната употреба може да включва голямо разнообразие от други цели като измерване на приливите, теченията, гравитацията, земния магнетизъм и определянето на физичните и химичните свойства на водата. Основната цел на повечето хидрографски проучвания е да се получат основни данни за съставянето на навигационни карти с акцент върху характеристиките, които могат да засегнат безопасната навигация. Другите цели включват придобиване на необходимата информация за свързани морски навигационни продукти и за управление на крайбрежните зони, инженеринг и наука.

2 Изложение

Целта на хидрографското проучване е:

❖ Да събира със систематични наблюдения в морето, по крайбрежието, язовирите, реките и във вътрешността георeферентни данни, свързани с:

- Конфигурация на бреговата линия, включително човешка инфраструктура за морско и речно корабоплаване, т.е. всички тези функции на брега, които представляват интерес за моряците;
- Дълбочини в района на корабоплаване (включително всички потенциални опасности за корабоплаването и други водни дейности);

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

- Състав на морското и речно дъно;
- Приливи и отливи;
- Физични свойства на водния стълб.

❖ Да обработва събраната информация, за да създаде организирани бази от данни, способни да осигурят създаването на тематични карти, морски карти, речни карти и други видове документи, използвани най-често за:

- Морска и речна навигация и управление на трафика;
- Военноморски операции;
- Управление на крайбрежните зони;
- Опазване на морската, язовирната и речната среда;
- Експлоатация на морски и речни ресурси, полагане на подводна инфраструктура (кабели, тръбопроводи и др.);
- Определяне на морските (прилагане на правото на море), язовирните и речните граници.
- Научни изследвания.

Морската, язовирната или речна карта е крайният продукт на хидрографското проучване. Точността и съответствието й зависят от качеството на данните, събрани по време на проучванията. Морската (язовирна, речна) карта е графично изображение на водната среда, показваща естеството и формата на брега, дълбочините на водата и общия характер и конфигурация на морското (язовирното, речното) дъно, местата на опасностите за навигацията, повишението и спадането на приливите и характеристиките на магнитните свойства на Земята. Действителният вид на морската (язовирната, речната) карта може да варира от традиционна хартия до електронна карта. Електронната карта не е просто цифрова версия на хартиената, тя въвежда нова навигационна методология с възможности и ограничения, които са много различни от хартиените карти. Електронната морска (язовирна, речна) карта се превърна в юридически еквивалент на хартиената карта, одобрена от Международната морска организация. Те доведоха до публикуването на различни карти от "ново поколение". Батиметричните морски карти, разработени от цифрови данни или създадени от многоцветни звукови данни, позволяват подводният релеф да бъде визуализиран чрез различни сини оттенъци и изобати. По същия начин са били публикувани сонарни мозайки за странично сканиране под формата на карти или атласи, за да се характеризират големите геоморфологични структури. Тези карти вече нямат за цел безопасността на корабоплаването, а по-скоро дават знания за околната среда, необходими за подводната навигация, океанографските проучвания или промишлените приложения, като например полагане на кабели, добив на морското дъно и експлоатация на нефт.

Хидрографската геодезия претърпява фундаментални промени в измервателната технология. Многобройните акустични и въздушни лазерни системи осигуряват почти цялостно покритие и измерване на морското дъно в сравнение с по-ранното вземане на проби от батиметрични профили. Способността за точно позициониране на данните в хоризонталната равнина е увеличена значително от наличието на системи за сателитно позициониране особено когато се увеличава с диференциални техники [1].

1. **Планиране на изследванията**

Планирането на проучванията обхваща широк спектър от дейности от разработването на идея за проучване в рамките на хидрографската служба и последващото ѝ издаване като Инструкции за проекта / Хидрографски инструкции (HI – Hydrographic Instructions), за подробно планиране и организиране на геодезичен кораб за изпълнение на практическа задача.

Планирането обхваща междуведомствената връзка на правителствено ниво, дипломатическото сътрудничество и разпределението на многобройни скъпи ресурси. Планирането на изследването включва смесване на дейности в съгласуван модел, насочен към постигането на конкретна задача.

Проучването започва много преди началото на събирането на данни. Някои задачи, които трябва да бъдат решени, са:

- Точна област на проучването;
- Вид на проучването и мащаб за изпълнение на стандартите на морската (язовирната или речна) карта, която трябва да бъде съставена;
- Обхват на изследването (краткосрочно или дългосрочно);
- Налични платформи (кораби, катери, самолети, наети плавателни съдове, споразумения за сътрудничество);
- Помощ при работа (въздушна или сателитна фотограметрия, геодезия, приливи и отливи);
- Ограничителни фактори (бюджетни, политически или оперативни ограничения, ограничения на системите за позициониране, логистика).

2. **Продължаване на планираните проучвания**

След като бъдат решени горните въпроси, се извършва преразглеждане на цялата налична информация в района на конкретното проучване. Това включва въздушна фотограметрия, сателитни данни, топографски карти, съществуващи навигационни карти, геодезическа информация, информация за приливите и всичко останало, което засяга изследването. Подробностите, дадени в инструкциите за проекта, могат да включват някои или всички от изброените по-долу, в зависимост от вида на дадено проучване:

- Ограничения на изследванията;
- Изисквания за данни и резолюция;
- Метод на позиционния контрол, заедно с очакваната точност;
- Използване на сонар;
- Как се изготвя докладът за проучването;
- Общо и подробно описание на причините за приоритетите на изследването, методи, които трябва да се използват, конкретни наблюдения и други подходящи насоки или инструкции;

Освен това приложенията към хидрографските инструкции дават подробни указания за следното:

- Каква координатна система и проекция да се използва;
- Останки от разбити кораби в изследваната област;
- Необходими данни за приливите;

- Специални инструкции относно събирането на данни по отношение на океанография, геофизика, инструкции за ветроходство, въздушна фотограметрия и др.

Разработването на общ план за проучване и последващите планове за специфични за обекта проучвания създава по-ефективно проучване. Общият план за проучване разглежда начина, по който се планират, извършват и обработват проучванията. Този план трябва да бъде добре обмислен и надежден, за да отчете възможно най-много непредвидени обстоятелства. Този план включва обучение, софтуер, поддръжка и обновяване на оборудването, изчисления, всички изисквания за данни, график, безопасност и време. Планът за специфично проучване на дадено място разглежда местните съобщения, предходни измервания и данни, плътност на данните и специфично оборудване и персонал, които ще отговарят на изискванията на общия план на изследването. Някои от изискванията са:

- Обучението на геодезисти следва да се извършва по време на измервания, за да се гарантира, че се поддържат подходящи компетенции;
- Софтуерът за регистриране и обработка на данни е от решаващо значение за проучването. Той трябва да е лесен за ползване;
- Следва да се избере подходяща платформа за проучване и оборудване. От първостепенно значение е да се направи правилен подбор;
- Целта на проучването обикновено ще диктува изискването за данните (гъстота/плътност, покритие и точност);
- Графикът често е критичен елемент в хидрографското проучване. Данните обикновено имат определена конкретна дата на предаване, така че събирането и обработката на данните от изследването да се извършват в много специфична времева рамка. Като се има предвид това, важно е да се планират и анализират всички аспекти на общия план за проучване с възможност да се изпълни графикът като основен елемент;
- Безопасността е основното съображение. Задължение на отговорното лице е да оцени всяка ситуация за възможни опасности. Ако има установена опасност, трябва да се обърне внимание, преди да се продължи с дейността;
- Своевременно уведомяване на местните власти;
- Проучвателните линии (промерите) с множество изследвания трябва да следват контурите на дъното. Това ще помогне при определянето на промените в подводния релеф. Многобройните линии на изследване също трябва да бъдат разположени така, че да се постигне подходящо количество припокриване или плътност на данните, за да отговарят на стандарта за проучване;
- Неразделна част от данните от проучването е използваната референтна система. Координатната система WGS-84 е подходяща, понеже се използва в цял свят;
- Плътността на данните ще варира според метода на проучването, дълбочината на водата и необходимостта. Методът на проучването се определя от наличното оборудването, квалифицирания персонал и условията на обекта на изследването [1].

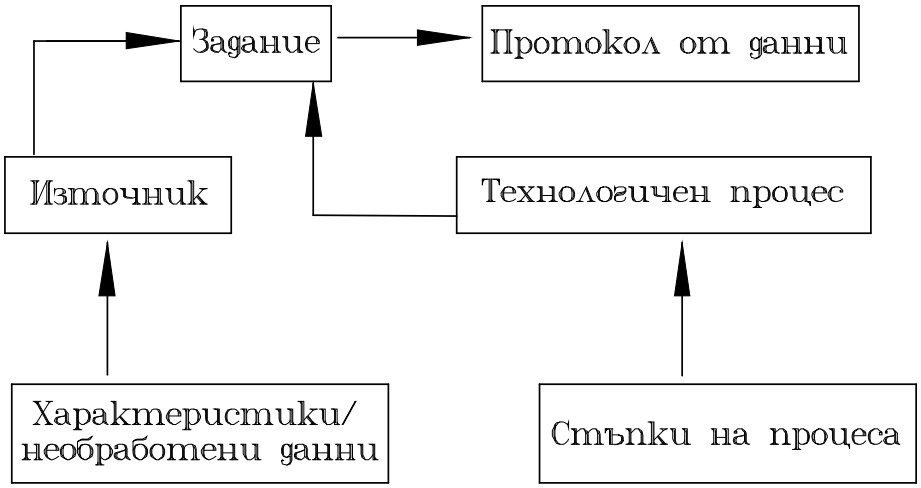
3. **Събиране на данни**

Събирането на данни зависи от различни фактори. Изискванията за проучването, наличната платформа и оборудване, както и времето, определено за определена задача, определят количеството данни, които трябва да бъдат събрани. Голяма част от данните могат да бъдат събрани, като се използват най-новите хидрографски софтуер и инструменти.

Трябва да се отбележи, че съкращаването на данните и плътността (гъстотата) на данните не са едно и също нещо. Плътността на данните е броят на измерените дълбочини на единица площ, докато съкращаването на данните се отнася до припокриване на данни или данни, събрани в различно време на едно и също място. Типът на изследването дефинира дублиране на данни или изисквания за припокриване на данни. Проучванията за пълно покритие се занимават повече с плътността на данните, което гарантира, че всички подводни характеристики на релефа (препятствия) са изобразени.

4. **Обработка на данни**

Обработката на данните трябва да се извършва при строги критерии за контрол на качеството. Хидрографските данни се събират чрез автоматизирани системи или се преобразуват в автоматизиран формат. Окончателното обработване на данните и картите се извършват чрез използване на бордови или офис-базирани компютърни системи. Събраните данни се обработват и впоследствие се проследяват пропуските и областите със съмнителни данни. Повечето от хидрографските системи са в състояние да изпълняват "довършителни" операции, при които данните от изследванията се събират, обработват, изчертават и анализират на полето. Необходимо е цялостно планиране на проучването за интегриран подход, който генерира базовата линия за цялата операция в реално време и последваща обработка със системата.



Фиг. 1 Модел за обработка на данни

Основното изискване за обработката на данни е генерирането на валидни данни, които са достатъчно обработени, т.е. преминали през различни процедури на различни етапи или представени така, че да може да се направи оценка. Тези процедури / етапи на обработка могат да се прилагат в реално време или по време на последваща обработка, но те трябва да

гарантират, че крайният продукт отговаря на стандартите и спецификациите, определени от IHO.

Трябва да се гарантира, че всички грешки са елиминирани и необходимите корекции нанесени, например коефициенти на калибриране на системата и компенсации на сензорите или променливи стойности, като например профили на скорост на звука и стойности на приливите за намаляване на измерените дълбочини. Обработката трябва да се стреми да използва всички налични източници на информация, за да потвърди наличието на навигационно значими дълбочини и качествени данни [1].

5. **Анализ на данните**

Точността на получените резултати от конкретно изследване трябва винаги да бъде цитирана, за да покаже колко са добри или надеждни. Тъй като никое оборудване не е напълно без грешки, затова във всички измервания се внасят грешки. Освен това грешките се въвеждат в изчисленията чрез приближения, използвани във формули, или чрез закръгляване на числата. Наблюдателните техники са предназначени да отстранят всички грешки, но има малки, случайни грешки, които след това могат да бъдат анализирани чрез строги техники за количествено определяне на точността на наблюденията.

Постоянните, систематичните и периодичните грешки често се разглеждат заедно като "систематични грешки". Постоянните и систематичните грешки са натрупващи се и поради това не могат да бъдат намалени чрез повторение. Случайни грешки присъстват във всички наблюдения, като резултатът никога не може да бъде "точен". Тези грешки могат да бъдат положителни или отрицателни и по-вероятно да бъдат с малки размери.

3 Заключение

Целта на дадено проучване обикновено диктува изискването за данните (плътност на данните, покритие и точност на данните). Възможно е да се събират повече данни по време на теренното проучване, ако няма увеличаване на разходите и графика за изпълнение на конкретна задача. Събирането на данни се извършва по методичен начин, започвайки от едната страна на областта, и завършващо на друга.

ЛИТЕРАТУРА:

[1] International Hydrographic Organization, Manual on Hydrography, Publication C-13, May 2005, (Corrections to February 2011), Chapter 1, 2 and 3.

[2] Добрев, С. Анализ на геодезическите методи за изследване деформациите на хидротехнически обекти. Научна конференция с международно участие MATTEX 2018, гр. Шумен (2018).

[3] Стойков, Е. "Технически средства и системи при извършване на хидрографски измервания", Университетско издателство "Епископ Константин Преславски", 177 стр., ISBN 978-619-201-334-9

[4] Ivanov, S. "Determination of visibility between card points". Journal scientific and applied research, Volume 13, 36 -40 стр, ISSN: 1314-6289. Лицензирано в EBSCO , USA. 2018 г.

[5] Иванов, С. "Определяне на точката на стоене по топографска карта". MATTEX 2018: Сборник научни трудове. Том 2. Част 2. Шумен: Университетско издателство "Епископ Константин Преславски", 134 - 140 стр. ISSN: 1314-3921. 2018 г.

[6] Stoyanov, B., Stoyanov, E.,“The usage of new technologies for collecting spatial data and ways of application in archeoastronomy“, Publications of the Astronomical Society of Bulgaria (PASB), 2016. , available at: http://astro.shu-bg.net/pasb/index_files/Papers/2016/Stoyanov.pdf , retrieved on 01.12.2016.

[7] Стоянов, Б., Стоянов, Е., Използване на локални цифрови филтри в съвременните геодезични методи, Втора научна конференция с международно участие - ТУ Варна, 26.09-27.09.2014г., Списание "КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ", Година XII, Брой 1/2014, с.158-163.

[8] Стоянов, Е., Стоянов, Б., „Приложение на стеганографията за нуждите на геодезията и цифровата фотограметрия“, MATTEX 2012, 22.11-24.11.2012, ШУ "Еп. К. Преславски",том 2, ISSN: 1314-3921. 2012 г.

[9] Bedzheva, M., Dobrev, S. „Estimating the area of the irregular dung-hills in Shumen municipality by using unmanned aerial vehicles“, Annual of Konstantin Preslavsky University of Shumen, vol. VIII E, ISSN: 1311-834X, pp. 166-173, Konstantin Preslavsky University Press 2018 г.

[10] Казаков, С., "Систематизиране на информационни потоци в логистиката" е от НВУ в Годишна университетска научна конференция 2020 В. Търново.

[11] Казаков, С., Йорданова, Йо., "Typology of risks in RFID", Journal scientific And Applied Research 2017.

Име на автора: Евгени Гришев Стойков
Месторабота: ШУ „Епископ Константин Преславски“
E-mail: e.stoykov@shu.bg

SURVEYING COAST LINES OF LAKES WITH PHOTOGRAMERIC METHODS

STEFAN D. DOBREV

ABSTRACT: *Comparing the area of the coast line of "Shumensko ezero" from year 2000 to year 2019, using UAV photogrammetric methods.*

KEYWORDS: *Photogrammetry, UAV, Lakes.*

ИЗСЛЕДВАНЕ НА БРЕГОВАТА ИВИЦА НА ВОДОЕМИ С ФОТОГРАМЕТРИЧНИ МЕТОДИ[1]

СТЕФАН Д. ДОБРЕВ

АБСТРАКТ: *Сравнение на площта на контура на бреговата линия на Шуменското езеро за 2000 г. и 2019 г. с помощта на БЛА и чрез използването на фотограметрични методи.*

1 Въведение

Мониторинга и прогнозирането на обема на водата във водоемите, се превърна в необходимост, след зачистилите наводнения и аварии, на територията на България. Заливните терени около водоемите са хабитат на много животни и растения, които са под постоянна заплаха от антропогенните дейности на човека. Трудоемкостта от обследването на водоемите и скъпите съоръжения за мониторинг, са една от пречките за ефективно прогнозиране и правилната експлоатация на водоемите. Традиционните геодезически методи за заснимане на бреговата зона и заливните терени, са също много трудоемки, поради редица причини, като основната е трудната проходимост и недостъпност. Това прави въздушната фотограметрия един от предпочитаните методи за изследване на брега и водните басейни.

Използването на Безпилотни Летателни Апарати (БЛА), намира все по – голямо приложение в наши дни. С повишаване на точността и поевтиняването на БЛА (автономни дронове) и големия избор от софтуер за обработка на изображенията, приложението им расте непрекъснато. В статията се разглеждат проблемите свързани приложението на БЛА и фотограметрията в изследването на водоемите и прогнозирането на евентуални бедствия, аварии и катастрофи [1], [4].

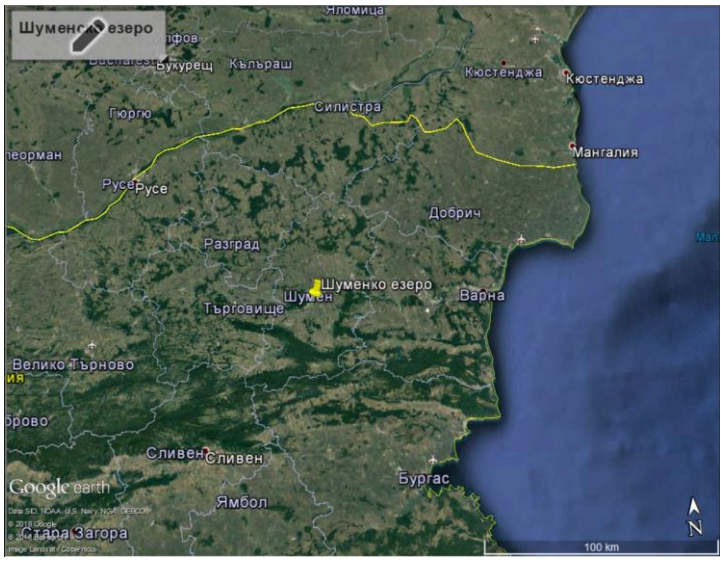
2 Изследвания

Чрез фотограметрични методи и с помощта на БЛА, можем бързо и ефективно да създадем модел на терена около всеки водоем, както и да изчислим площта на водното огледало или на бреговата линия. При наличието на базово (нулево) измерване, при което е изчислен обема на водоема, можем да изчисляваме спрямо площта на водното огледало и обема. Контура на водоемите е от значение за редица екологични и социални аспекти. При повишаването обема на даден водоем и не навременното вземане на съответни мерки, може

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

да доведе до заливането на терени, което от своя страна води до големи икономически загуби.

Обектът на нашето изследване е Шуменското езеро. То е разположено на около 6 км от град Шумен. Ограждащи езерото села са: село Дибич, село Васил Друмев, село Мараш, село Хан Крум и село Троица. Езерото е изкуствен инфраструктурен обект и буди голям интерес и впечатлява със заобикалящата го природа. То е подходяща дестинация за отдих, туризъм и риболов. Водоемът се стопанисва от „Напоителни Системи“ ЕАД и не се ползва за питейни нужди.



Фиг. 1 – Местоположение на Шуменското езеро

За начална епоха на изследването е използвано измерване на водното огледало (контура на бреговата линия) от 2000 год. извършено от проф. А. Андреев [2], [3]. Контура на бреговата линия от 2000 г. е наложено върху сателитни изображения на Google Earth от 2018 г.

Фиг. 2 – Измерване на бреговата линия от 2000 г.

С цел да се сравни как се изменил контура на бреговата линия е извършено фотограметричното заснимане на 17 октомври 2019 год., с дрон DJI Phantom 4 Pro. Камерата е FC6310S с дължина на фокуса от 8.8 mm. Заснимането е направено само по бреговете на водоема. Направени са 1 147 броя снимки (изображения) от които 1 129 броя са със задоволително качество и са годни за обработка. Височината на летене и заснимане е 100 метра над точката на излитане. Постигната резолюция е 2,14 cm на пиксел.

Използвани са 13 контролни точки ("GCP – ground control point" – контролна точка) за трансформация и точното георефериране на изображенията. Те са измерени с двучестотен ГНСС приемник EMLID REACH RS2 и използване на мрежата 1Yocto.

GNSS measurements are made at geodetic points that meet all the common requirements for site selection, the way to stabilize and benchmark, the visibility to other points, and native subjects stemming from applicable normative documents.[4], [5], [6].

Избраната координатната система е WGS84 зона N35, проекция UTM, с цел по – лесната софтуерна обработка. Височинната система в която са измерени точките е геодезическа (елипсоидни височини), като преди започване на обработката са трансформирани в нормална височинна система - Балтийска височинна система, с помощта на софтуерния продукт на Агенцията по Геодезия, Картография и Кадастър (АГКК) - BGS TRANS. Контролните точки са представени в таблица 1 с техните координати в координатен регистър на контролните точки.

Таблица 1

Координатен регистър на контролните точки

Координатна система: WGS84
Височинна система: Балтийска

Име на точка	***Географска ширина (дес. градуси)***	***Географска дължина (дес. градуси)***	***Надморска височина (m)***
GCP1	*43,25320468*	*26,95037708*	*194,306*
GCP2	*43,25086921*	*26,94853577*	*193,226*
GCP3	*43,25012383*	*26,94672273*	*191,606*
GCP4	*43,24640698*	*26,94081081*	*192,968*
GCP5	*43,24469034*	*26,94169517*	*195,710*
GCP6	*43,24321564*	*26,94659916*	*191,093*
GCP7	*43,24050436*	*26,95186636*	*189,527*
GCP8	*43,24210712*	*26,95376934*	*189,404*
GCP10	*43,24681005*	*26,95928837*	*189,518*
Gcp11	*43,24562398*	*26,95791456*	*189,422*
Gcp12	*43,24715332*	*26,95982197*	*190,729*
Gcp13	*43,24456854*	*26,95665725*	*189,409*
GCP14	*43,25167712*	*26,95291254*	*187,330*

Софтуерната обработка на получените изображения е извършена със софтуерен продукт AGISOFT, като постигната точност на георефериране на модела е 8,4 mm, или 0,32 pixel. В таблица 2 са представени грешките от контролните точки [7], [8], [9].

Таблица 2

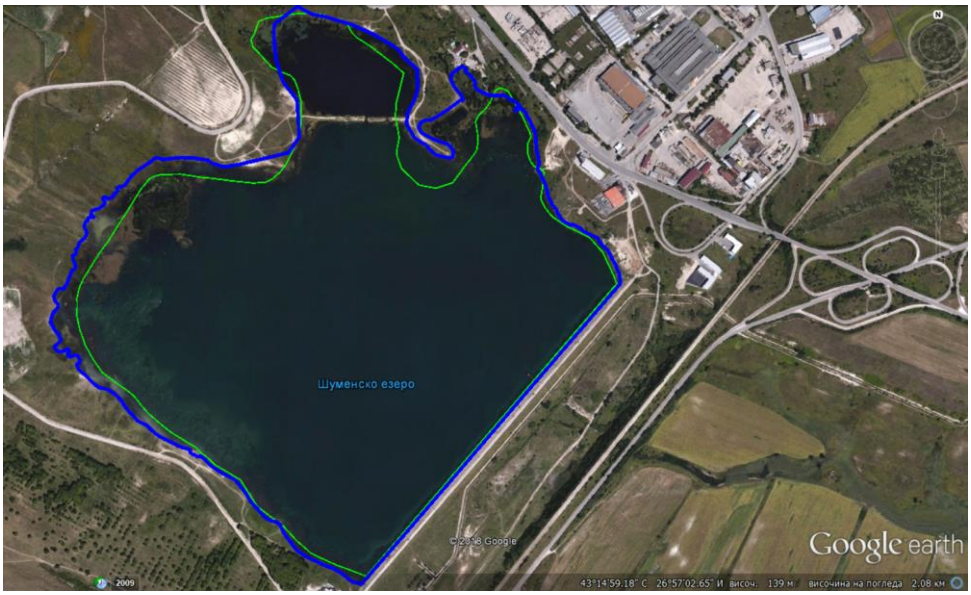
Грешки от контролните точки

Име	*Грешка в положение (m)*	*Грешка във височина (m)*	*Обща Грешка (m)*	*Брой проекции*	*Обща Грешка (pix)*
GCP1	*0,0018*	*-0,0003*	*0,0018*	*18*	*0,3800*
GCP2	*0,0020*	*0,0000*	*0,0020*	*22*	*0,3240*
GCP3	*0,0010*	*-0,0004*	*0,0011*	*5*	*0,2660*
GCP4	*0,0027*	*-0,0031*	*0,0041*	*10*	*0,2960*
GCP5	*0,0031*	*0,0032*	*0,0044*	*5*	*0,1860*
GCP6	*0,0014*	*-0,0022*	*0,0026*	*14*	*0,3480*
GCP7	*0,0006*	*-0,0007*	*0,0009*	*24*	*0,2950*
GCP8	*0,0020*	*0,0015*	*0,0025*	*15*	*0,3430*
GCP10	*0,0206*	*0,0034*	*0,0209*	*26*	*0,3410*
Gcp11	*0,0076*	*0,0001*	*0,0076*	*17*	*0,2770*
Gcp12	*0,0175*	*-0,0014*	*0,0175*	*30*	*0,3520*
Gcp13	*0,0074*	*-0,0017*	*0,0076*	*17*	*0,3640*
GCP14	*0,0012*	*0,0013*	*0,0018*	*18*	*0,1820*
ОБЩО:	***0,0082***	***0,0019***	***0,0084***		***0,3210***

3 Анализ на резултатите и интерпретация

След приключване на обработката на резултатите е начертан контура на бреговата линия по георефериранoто изображение. Площта на водното огледало е 931 559,6 кв. м или 93,16 ха. Контура измерен през 2000 г. от проф. А. Андреев е с площ от 838 808 кв. м или 83,88 ха. Разликата е близо 10 ха и от фигура 3 се вижда през 2019, кои терени за залети.

Със зелен цвят е представено измерването от 2000 г., а със син свят – измерването от 2019 г.



Фиг. 3 – Сравнение на контурите от 2000 г (зелен цвят). и 2019 г. (син цвят)

4 Заключения

Времето за реализирането на целия процес за получаването на контура, от измерването и поставянето на контролните точки, облитането с дрон, и обработката на изображенията е в рамките на един ден.

Навременния мониторинг на водоемите, може да доведе до превенцията на социално – икономически загуби, а фотограметричните методи в комбинация с ГНСС, могат бързо, лесно и точно да дадат представа за състоянието на даден водоем и за заливните терени, като се представи информацията върху актуална кадастрална карта.

.

ЛИТЕРАТУРА:

[1] Андреев А. Геоинформационни технологии за моделиране на сигурност при бедствия. Сборник научни трудове MATTEX 2012, ШУ ”Еп. К. Преславски” , том 2, стр. 105-117, ISSN:1314-3921 .

[2] Андреев А. Геопространствени данни от преки геодезически измервания на територии заети от водни течения.. Сборник научни трудове MATTEX , ШУ ”Еп. К. Преславски” 2012, том 2, стр. 161-168, ISSN:1314-3921

[3] Стойков, Е. Статистически анализ при сравняване на геодезически измервания, извършени по класически и ГНСС методи. MATTEX 2018: Сборник научни трудове. Том 2. Част 2. Шумен: Университетско издателство "Епископ Константин Преславски", ISSN 1314-3921 (2018).

[4] Стойков, Е. Установяване на стохастически връзки при сравняване на геодезически измервания извършени по класически и ГНСС методи“, MATTEX 2018: Сборник научни трудове. Том 2. Част 2. Шумен: Университетско издателство "Епископ Константин Преславски", ISSN 1314-3921 (2018).

[5] Bedzheva, M., Denev, D. Experimental exploration of the factors influencing on the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019).

[6] Bedzheva, M., Ignatova, T. Analysis of the accuracy of geodesical maps prepared by the means of UAVs. Proceedings of University of Ruse, vol. 58, book 3.2., ISSN 1311-3321 (2019)

[7] Assoc. Prof. Eng. Ilinka Metodieva Ivanova, Eng. Stefka Nikolova Spasova, “STATE AND MUNICIPAL PROPERTYIN THE CADASTRAL MAP AND CADASTRAL REGISTERSOF VELIKO TARNOVO”, ANNUAL OF KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN VOL. VI E, 2017, pp. 26.

[8] Evgeni Gr. Stoykov, “ANALYSIS AND EVALUATION OF GNSS METHODS IN GEODESY”, ANNUAL OF KONSTANTIN PRESLAVSKI UNIVERSITY OF SHUMEN VOL. VIII E, 2018, pp. 130.

[9] Стойков, Е. Methodology for surveying and tracing of objects by using GNSS. Годишник: Технически науки. Том IX E, Шумен, Университетско издателство "Епископ Константин Преславски", ISSN 1311-834X (2019).

Име на автора: ас. Стефан Д. Добрев
Месторабота: Факултет по технически науки, кат. Геодезия
E-mail: st.dobrev@shu.bg

SOURCES OF ERRORS IN THE INTEGRATED CADASTRAL MAP AND CADASTRAL REGISTERS

MIREM E. NIYAZI-YUSUF

ABSTRACT: *The errors in the integrated cadastral map and the cadastral registers result from errors in the geodetic basis, errors in the digitization of existing plans and maps, errors in performing geodetic measurements (including art. 36 and 38 of the LCPR).*
KEYWORDS: *cadastre, errors, map*

ИЗТОЧНИЦИ НА ГРЕШКИ В ИНТЕГРИРАНАТА КАДАСТРАЛНА КАРТА И КАДАСТРАЛНИТЕ РЕГИСТРИ[1]

МИРЕМ Е. НИЯЗИ-ЮСУФ

АБСТРАКТ: *Грешките в интрегрираната кадастрална карта и кадастралните регистри произтичат от грешки в геодезическата основа, грешки от дигитализирането на съществуващи планове и карти, грешки при извършване на геодезически измервания (включително чл. 36 и 38 от ЗКИР).*

1. Геодезическа основа – различни координатни системи

1.1. Геодезическа основа

Геодезическата и височинна системи на триангулачната мрежа на България 1877-1879 г. - Руската триангулация е първата триангулачна мрежа на България. Създадена е от Корпуса на руските военни топографи, по време на руско-турската освободителна за България война 1877 - 1878 години и следващата 1879 г.

Изградена е във формата на триангулачни вериги - общо 22 на брой. Съдържа 580 триангулачни точки II-ри ред, 637 триангулачни точки III-ти ред и 57 други точки.

Днес опорната геодезическа основа на България се състои от Държавната геодезическа мрежа (ДГМ) I – IV клас, Държавната нивелация I – III клас, геодезическите мрежи с местно предназначение V – VII клас, както и гравиметричната мрежа на страната. Тя е изграждана в продължение на дълъг период от време.

Държавната геодезическа мрежа включва около 6500 точки. Тя се поддържа чрез периодични проверки на терена, строителни и ремонтни работи от Министерството на отбраната и е в относително добро състояние.

Геодезическите мрежи с местно предназначение се състоят от над 60000 точки. Физическото състояние на тези мрежи не се поддържа и много от точките в интензивните райони са унищожени. В съвкупността си те образуват нехомогенна мрежа с различна плътност.

През 60-те и 70-те години ДГМ е модернизирана и преизчислена. Такава модернизация и преизчисления не са направени за геодезическите мрежи с местно предназначение.

Модернизирането на ДГМ на основата на ГНСС технологиите започна с включването на страната в изграждането на новата референтна система EUREF. През 1992/1993 г. са проведени международни ГНСС кампании и са определени 7 точки на територията на

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

страната като част от мрежата EUREF, както и 8 допълнителни точки. Тази съвкупност от 15 високоточно определени пространствени точки, наречена Булреф, няма непосредствено практическо значение, тъй като средното разстояние между точките е 93 км. Тя обаче има всички качества да бъде основа за радикално модернизиране на ДГМ [1].

Работната геодезическа основа се създава като планова и височинна мрежа, включена в точки от държавната геодезическа мрежа и геодезическите мрежи с местно предназначение [4, 6]. Тя се създава за урбанизираните територии, когато съществуващата РГО не отговаря на изискванията. За създаването на РГО се изработва проект, който се съгласува със службата по геодезия, картография и кадастър. В проекта се означават начините за определяне на точките от РГО като за създаването на кадастралната карта землищните граници се изобразяват в кадастралната карта така, както са отразени в плановете и картите, одобрени от Закона за собствеността и ползването на земеделските земи (ЗСПЗЗ), както и номерирането им.

Плътността на точките от РГО е най-малко 0,60 точки на един хектар за урбанизирани територии и най-малко 2 точки на един квадратен километър за неурбанизирани територии.

Точките от РГО се разполагат равномерно разпределени върху територията и на разстояние една от друга до 300 m в урбанизирани територии и на разстояние една от друга до 500 m в неурбанизирани територии. За връзки с точки от ДГМ и ГММП разстоянието е до 1000 m. От всяка една точка се осигурява видимост към най-малко две съседни точки [6].

1.2. Координатни системи

Координатните системи, в които е създадена РГО, и кадастралните планове са в локална координатна система, координатна система 1930 г., координатна система 1950 г. и координатна система 1970г.

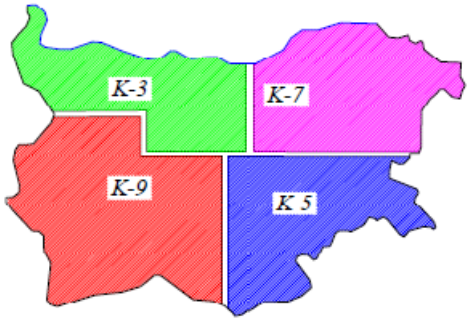
Координатна система 1930 година. За референтен елипсоид е използван елипсоида на Хейфорд. Ориентацията на координатната система върху елипсоида е с минимален брой астрономически измервания – изходна точка Черни връх и изходен азимут към точка Мечи камък. В тази система са дефинирани географски координати, а също и проекционни – Гаусова проекция с две триградусови зони, с осеви меридиани 24° и 27°. Мащабът на проекцията по меридиана е 0.9999. Ординатата Y се отчита от основния меридиан и е с положителен знак на изток, с отрицателен – на запад. Абсцисата X е с нулева точка на паралела с ширина 41° и нараства на север, т.е за цялата територия на нашата страна е положителна. От 1941 год. към абсцисите е прибавена мащабно намалената с 0.9999 меридианна дъга от екватора до 41-я паралел, а към ординатите се прибавя константата Yo = n.106+5.105, където n е номерът на зоната.

Координатна система 1950 година. Координатите на точките са трансформационен аналог на гаусовите проекционни координати на БГРС 1930 г., със следните променени значения на вторичните параметри: Първо, мащабът по основния меридиан на зоната става равен на единица и второ, наред с три градусовите зони, с основни меридиани 24 и 27 градуса, се въвеждат и шест градусови зони, с основни меридиани 21 и 27 градуса. Три градусовите зони са предназначени за създаване на едромащабната топографска карта (ЕТК) в мащаб 1:5000 и производен 1:10000, както и за плановете на населените места, в това число и кадастралните планове. Като цяло, това е “гражданската” геодезическа продукция. Шест градусовите зони се взаимствуват от съветската

геодезическа практика и са предназначени за създаване на военните топографски карти от целия мащабен ред.

За референтен елипсоид е приет елипсоидът на Красовски, едновременно с това са изменени и данните за изходната точка. Координатите на всички точки от държавната астрономо-геодезическа мрежа са трансформирани чрез диференциални формули от елипсоида на Хейфорд към елипсоида на Красовски.

Координатна система 1970 година. Тази система е дефинирана чрез координатна система 1950 година, като са въведени само нови проекционни координати с цел да се „прикрие" единната координатна система, използвана в Българската армия. Страната е разделена на четири зони със застъпване между тях от 10 km – северозападна (К-3), югоизточна (К-5), североизточна (К-7) и югозападна (К-9) (Фиг.1.1).



Фиг. 1.1. Разпределение на зоните върху територията на страната

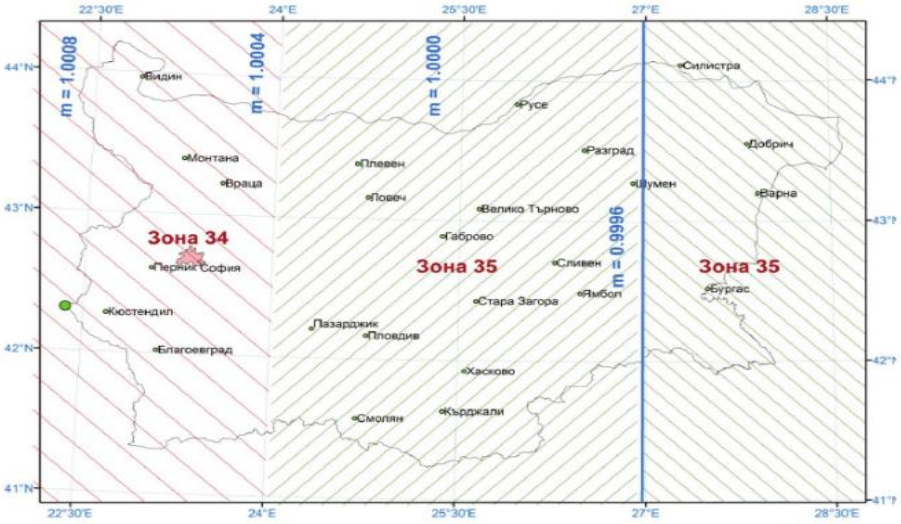
За всяка зона е въведена конична конформна проекция с един стандартен паралел и мащаб по допирателния паралел единица. Въведени са условни правоъгълни координати за централните точки на проекциите, а всяка проекция е завъртяна на малък ъгъл така, че да не се наруши конформността на изображението. За всяка от четирите зони са изчислени различни трансформационни параметри от система 1950 г. в система 1970 г. За целта е използвана полиномиална трансформация от трети ред, осигуряваща точност 1 mm.

Изброените геодезически референтни и координатни системи се наричат още класически. До момента на приемането на БГС2005 цялото геодезическо производство в страната се отнася към някоя от тях и най-вече към координатна система 1970 година (КС1970), но тази система е обвързана с 1950 год. (КС1950).

Българската геодезическа система 2005 (БГС 2005) е основана на геодезическата референтна система GRS80 (Geodetic Reference System). Тя включва геоцентричен еквипотенциален елипсоид GRS80, определена е към Европейската земна координатна система ETRS89 в епоха 2005.0. БГС 2005 включва за геодезическа проекция – Универсална напречна цилиндрична проекция на Меркатор (Universal Transverse Mercator – UTM) и въведената чрез нея система от проекционни (правоъгълни, равнинни) координати.UTM проекцията се използва за тясна част с ширина повече от от $\pm 3^{o}$ двете страни на централния меридиан. Тази особеност се дължи на изискването да се намали мащабната деформация. Като подходяща стойност за мащаба на централния меридиан е избрана 0.9996. Това означава, че мащабният фактор в проекцията се ограничава от 0.9996 по централния меридиан до 1.0010.

Тази проекция се използва като равнинна правоъгълна координатна система и е най-подходяща за територии, които са удължени в посока север – юг. Това е първият

критерий, по който UTM проекцията не е подходяща за географското разположение на нашата страна. Независимо от множеството написани критични материали за въвеждане на Българската геодезическа система (БГС) 2005, основана на UTM проекция, тя беше наложена от Министерството на отбраната. За всички е известно, че тази проекция е зонирана (каквато беше и Координатна система 1970 г.) и не може да се изгражда географска информационна система поради прекъснатост на данните. Другият проблем, който възниква, когато една страна е разположена в две или повече зони е, че при изграждане на ГИС се налага трансформиране на цифровия модел, т.е трансформиране на координатите от едната зона в другата. Това означава, че в трансформираната зона координатите ще са грешни, а това предполага измерване на грешни растояния, ъгли и площи. Трети проблем е промяната на площите, което е изключително важно за кадастъра. Именно тези проблеми наложиха впоследствие за кадастралните карти да се въведе т.н „Кадастрална координатна система". Всъщност, тази система е първоначално приетата БГС 2000, базирана на конична конформна проекция, която беше с подходящи параметри и осигуряваше минимални деформации. Въпреки това, Наредба №2 от 30 юли 2010 г. не е отменена и включва за геодезическа проекция UTM. Това е основание всички институции, които изграждат ГИС, да спазват тази наредба. Това са направили и по проекта „Интегрирано управление на водите в Република България" от проучвателен екип „Джайка", а именно: зона 34 е трансформирана към зона 35 (фиг.1.2)



Фиг. 1.2. Координатни зони в България в UTM проекция от [12]

Кадастралната координатна система 2005 е единна за територията на страната – проекционна пространствена координатна система и една от формите на координатна система БГС2005 [3]. Това означава, че между различните форми на координатна система 2005 (геоцентрична, елипсоидна и кадастрална) има взаимно еднозначно съответствие. При това условие, под „проекционна пространствена координатна система", следва да се разбира изображение на елипсоидната повърхност (на която е разположена страната) в проекционна равнина, като третата компонента е наделипсоидната (геодезическата) височина на точката. При това условие динамичните, ортометричните и нормалните височини остават (както и до сега) форми на височинната система, свързана с геоида, съответно квазигеоида.

Проекционната равнина е Ламбертово конично изображение на повърхнината на елипсоида с един основен паралел – с мащаб единица и равно отдалечен от най-южния и най-северния паралел на страната.

Координатното начало е пресечната точка на основния паралел и меридиана с дължина – равно отдалечен от най-западния и най-източния меридиан на сухоземната част от територията на страната.

Мащабният коефициент се определя по формулата на Крюгер , където е мащабният коефициент в края на зоната или е определен по критерия на Ейре, при който се минимизира квадрата на интегралната средна стойност на линейната деформация върху изобразяваната площ в проекционната равнина. Това е оправдано за дребномащабни топографски карти, когато отдалечението от основния паралел (меридиан) е над 200 км. Например, в края на 6 градусовите ивици мащабният коефициент достига 1.00077 за географската широчина на България. Това води до съществено увеличение на площите в края на зоната, както и площта на изображението като цяло.

2. Създаване на числени модели от съществуващи графични планове и карти (оцифряване на съществуващи планове и карти)

Кадастралните планове, одобрени по реда на отменения ЗЕКНРБ или отменения ЗТСУ, и на § 40 от преходните и заключителните разпоредби (ПЗР) на Закона за изменение и допълнение на ЗКИР [4, 11] са обикновено на традиционен носител (кадастрон с алуминиева вложка, подплатен с плат или само картон), поради което е необходимо преобразуването им в числен вид. Първите кадастрални планове бяха преобразувани от графичен в числен вид по **Приложение №11 към чл. 45, ал. 1, т. 3 от Наредба № 14 от 2001г. отм.**

Изработването на кадастралната карта от одобрени по реда на закон съществуващи планове и карти в графичен вид чрез преобразуване в цифров вид се извършва при спазване на следните изисквания:

1. Сканирането на планове и карти се извършва по зони. Използват се оригинали, контактно копирани оригинали и по изключение - копия от оригинали. Резолюцията на сканираното изображение трябва да бъде не по-малка от 300 dpi.

2. Трансформирането включва транслация, ротация и мащабиране на сканираното изображение в координатната система на кадастралната карта. Трансформирането се извършва чрез полиномна трансформация от първа степен (афинна трансформация) при най-малко шест идентични точки с известни координати в координатните системи на сканираното изображение и на кадастралната карта.

3. Трансформирането се извършва по зони не по-големи от 50 x 50 cm.

4. Точките за трансформация се разполагат равномерно в зоната. За трансформацията се използват координатни кръстове и/или точки от геодезическата основа на плана или картата.

5. Координатите на идентичните точки се трансформират от координатната система на плана или картата в координатната система на кадастралната карта с лицензиран софтуер от Агенцията по геодезия, картография и кадастър.

6. При липса на координатни кръстове и точки от геодезическата основа на плана за трансформация се използват трайно материализирани точки от границите на обекти на кадастъра с отчетени образни координати и определени с геодезически измервания координати в координатната система на кадастралната карта.

7. За определяне параметрите на трансформация образните координати на идентичните точки се определят с двукратно отчитане от сканираното изображение. След трансформацията линейната разлика между двукратните отчитания на една и съща точка не трябва да е по-голяма от 0.15*M в милиметри, където M е мащабното число на графичното изображение.

8. С параметрите на трансформация повторно се изчисляват координатите на идентичните точки. Най-голямата линейна разлика между изчислени и дадени или определени координати на идентичните точки не трябва да бъде по-голяма от 0.6*M в милиметри. Средната квадратна грешка, изчислена чрез линейните разлики на всички точки след трансформацията, не трябва да е по-голяма от 0.3*M в милиметри.

Кадастралните планове и карти се оцифряват ръчно (с дигитайзери) или полуавтоматично (със скенери). Най-често възникващите проблеми са:

- трудности при достъпа до картите;
- съдържанието им не винаги е актуално към момента на дигитализиране;
- недобрата съвместимост между картите, издадени през различни години;
- неточностите в картите;
- хартиените карти лесно се деформират (свиват или разтягат) и похабяват, което води до въвеждане на неточни координати на дигитализираните точки (фиг. 2.1);
- самите карти съдържат грешки, които автоматично се пренасят в техния цифров аналог;
- често трудно се съвместяват краищата на съседни картни листове.

Фиг. 2.1. Похабен кадастрален план от [11]

В процеса на дигитализиране операторите допускат редица грешки, най-типичните от които са следните:

- кръстосване на линиите;
- дублиране на обекти;
- несвързване на линиите;
- грешна регистрация и др.

След като се извърши дигитализирането на кадастралния и създаване на числен модел на регулационния план, в кадастралния план се нанасят промените в имотите, настъпили в резултат на приложената регулация; определят се кадастралните райони; дават се

идентификатори на поземлените имоти и сградите, като номерата на поземлените имоти е желателно да съвпадат с планоснимачните номера, съответно с номерата на имотите от картата на възстановената собственост; в кадастралните регистри планоснимачните номера се записват в колона „Стар идентификатор“, създава се сборна карта на землището, получена чрез обединяване на кадастралните планове и картите, изработени по реда на ЗСПЗЗ и ЗВСГЗГФ.

Сканирането, мащабирането и векторизирането на съществуващите планове и карти се извършва според Приложение № 9 към чл. 83, ал. 1 от **Наредба № РД-02-20-5 от 15 декември 2016 г.[6]. Контролът на тази дейност трябва да се извършва заедно с контрола на кадастралната карта. Съласно** Наредба № 19 от 28.12.2001 г. за контрол и приемане на кадастралната карта и кадастралните регистри [9], Службата по кадастър е длъжна да извършва проверката чрез повторно дигитализиране на част от кадастралния план.

3. Грешки от неспазване изискванията за означаване на имотните граници (чл. 36 и 38 от зкир)

Съгласно чл. 36 ЗКИР областният управител и кметът на общината са длъжни да осигурят означаването на границите на държавните и общинските имоти в срока, посочен в заповедта по чл. 35, ал. 1, и да предоставят на АГКК данни за недвижимите имоти от съответните регистри.

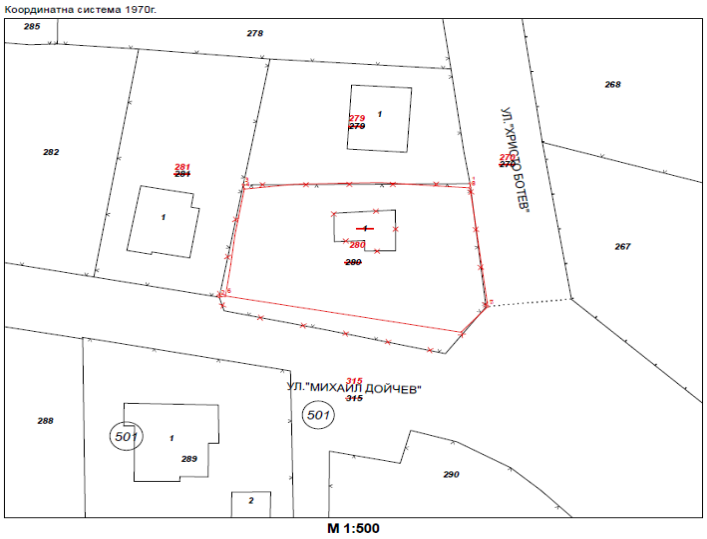
Съгласно чл. 38 ЗКИР собственикът, съответно носителят на друго вещно право, е длъжен:

1. да осигури свободен достъп в имота за извършване на работите по кадастъра;
2. да означи с трайни знаци границите на имота си и да опазва знаците от унищожаване;
3. да представи на служител от службата по геодезия, картография и кадастър при поискване акт, удостоверяващ правата му върху имота;
4. да опазва поставените в имота геодезически знаци.

В случай на повреждане или унищожаване на знаците собственикът, съответно носителят на друго вещно право, е длъжен незабавно да уведоми службата по геодезия, картография и кадастър. Когато поради строителни или монтажни работи възникне необходимост от унищожаване на геодезически знак, лицето е длъжно да уведоми службата по геодезия, картография и кадастър 7 дни преди започване на работите.

Неизпълнението на задълженията на собствениците и органите на изпълнителната власт води до значителни грешки в кадастралната карта, като:

- несъответствия в границите и очертанията на недвижимите имоти в кадастралната карта за урбанизирана територия спрямо действителното им състояние (фиг. 3.1);
- неправилното отразяване на правото на собственост;
- отсъствието или наличието на записи в кадастралния регистър;
- *записване на „стари“ актове за собственост;*
- нанесени граници по последния кадастрален план, без да бъдат отчетени промените в границите му в резултат например на делба, обединяване, поправяне на непълноти и грешки, в следствие на което е изменен регулационния план.



Фиг. 3.1. Несъответствие в границата на имота спрямо действителното ѝ състояние от [11]

4. Грешки при извършване на геодезически измервания

Изискванията за извършване на геодезически измервания при създаване на кадастрална карта и кадастрални регистри, съгласно Наредба № РД-02-20-5 от 15 декември 2016 г., са:

1. Геодезическите измервания се осъществяват чрез технологии, които осигуряват данни за определяне на геодезически координати на точки от граници, с точност, по-висока от определената в чл. 18, ал. 4, т. 1, буква "а", съответно - чл. 18, ал. 5, т. 1, буква "а" от Наредба № РД-02-20-5 от 15 декември 2016 г.[6], намалени три пъти.

2. Не са геодезически измервания технологиите за определяне на координати на точки чрез оцифряване (сканиране и векторизиране) на графични планове и карти, одобрени по реда на закон.

3. Геодезическите измервания могат да се извършат чрез:

а) тотални станции и технологии, осигуряващи висока точност;

б) ГНСС и технологии, осигуряващи точност, определена в Наредба № РД-02-20-5 от 15 декември 2016 г.;

в) фотограметрични технологии, осигуряващи достатъчно висока точност;

г) комбинации на изброените технологии.

4. Тоталните станции трябва да отговарят на изискванията определени в [6].

Изискванията към измерванията с тотална станция са регламентирани в [6].

5. Геодезическите измервания с ГНСС за определяне на геодезически координати на точки от граници се извършват в съответствие с изискванията на Инструкция № РД-02-20-25 от 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи [10].

6. За определяне на геодезически координати на точки от граници чрез фотограметрични технологии се прилагат изискванията на Наредба № РД-02-20-16 от 2011 г. [8].

Грешките при извършване на геодезически измервания са:

- имотът въобще не е бил заснет като самостоятелен поземлен имот в кадастралната карта;
- реална част от поземлен имот е грешно заснета в границите на друг поземлен имот;

- грешното заснемане в кадастралната карта на границите на един недвижим имот – поземлет имот, очертанията на сграда и самостоятелен обект.
- вследствие на предоставени стари документи за собственост, например преди делба, обединяване или отчуждителни процедури.

5. Грешки в кадастралния регистър могат да бъдат от:

- използване на неактуални кадастрални регистри;
- при създаването на кадастралната карта собствениците не са си предоставили документите за собственост – акт, установяващ правото на собственост или друго вещно право;
- правоспособното лице не е направило необходимото, за да събере данните за собственост;
- при промяна в идентификатора;
- дублиране на носителите на право на собственост;
- липсва информация за наследниците;
- при грешки в площта на поземлените имоти.

6. Заключение

В доклада са разгледани някои от източниците на грешки в интегрираната кадастрална карта и кадастрални регистри. От написаното до тук, можем да кажем, че:

1. В България е създадена многокласова геодезическа основа, като точността на всеки клас е различна и тя се отразява върху точността на всеки последващ клас. Това обстоятелство често го пренебрегваме.
2. Използването на различни координатни системи през годините оказва влияние върху точността на трансформираните кадастрални планове и карти от една координатна система в друга.
3. При дигитализирането на кадастралните планове се допускат груби грешки от операторите, които влияят върху точността на цифровия модел на кадастралната карта;
4. Неизпълнението на задълженията на изпълнителната власт и собствените води до непълноти и грешки в кадастралната карта.
5. При извършване на геодезическите измервания трябва да се използват вискоточни инструменти и не трябва да се допускат груби грешки.

ЛИТЕРАТУРА:

[1] Йовев Ил., Геодезическите мрежи на България и свързаните с тях референтни, координатни и височинни системи. Национален институт по геофизика, геодезия и география при БАН, София, 2010.

[2] Белчева, М. Следва ли при отстраняване на непълнота или грешка в кадастралната карта да се съставя акт за непълнота или грешка. Геомедия. 2015. 20 Ноември.

[3] Костадинов, К., Григоров, В., Кадастрална координатна система 2005. Статията е докладвана и публикувана на XXIII Международен симпозиум „Съвременните технологии, образованието и професионалната практика в геодезията и свързаните с нея области“ – 2013

[4] Закон за кадастър и имотен регистър. ДВ бр. 34, 2000

[5] Закон за собствеността. ДВ бр. 92, 1951

[6] Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри. ДВ. бр. 4, 2017

[7] Наредба № РД-02-20-3 от 29.09.2016 г. за структурата и съдържанието на идентификатора на недвижимия имот и на номера на зоната на ограничение в кадастъра. ДВ бр. 80, 2016.

[8] Наредба № РД-02-20-16 от 2011 г. за планирането, изпълнението, контролирането и приемането на аерозаснемане и на резултатите от различни дистанционни методи за сканиране и интерпретиране на земната повърхност. ДВ, бр. 65, 2011 г.

[9] Наредба № 19 от 28.12.2001 г. за контрол и приемане на кадастралната карта и кадастралните регистри. ДВ, бр. 2, 2002

[10] Инструкция № РД-02-20-25 от 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи, в сила от 11.10.2011 г., ДВ, бр. 79 от 2011.

[11] Ангелова, Е. Кадастрален план и кадастрална карта - съдържание, източници и данни от тях. Обжалване на кадастралната карта при създаването й. Непълнота или грешка в кадастралната карта и материално- правни спорове по ЗКИР. Съдебна геодезична експертиза. Установяване на местоположението на границите на поземлен имот – гражданскоправни и административноправни аспекти., София, февруари 2016.

[12] Кастрева, П., Безинска, Г., Грешки при трансформиране на графични данни от една координатна зона в друга, Списание „Геодезия, Картография, Земеустройство“ – 2015

[13] http://www.cadastre.bg/ - Агенция по геодезия, картография и кадастър

Име на автора: инж. Мирем Е. Ниязи-Юсуф
Месторабота: „Автомагистрали –Черно море“ АД, ШУ „Епископ Константин Преславски“
E-mail: mirem_1993@abv.bg

DESIGN AND MEASUREMENT OF A WORKING GEODETIC BASIS FOR THE SURVEY OF ROADS FOR REHABILITATION

PETYO P. SPASOV

ABSTRACT: *The linear objects are the connection between the settlements. They can be transport objects - roads, railways, subways, bicycle lanes, pedestrian lanes or communication objects – cable routes, plumbing, gas pipelines, heating pipelines and other routes for which it is necessary to prepare investment projects. In the present study will be considered precisely the accuracy and methodology in the design and measurement of working geodetic basis for the making of a geodetic survey in order to create projects for rehabilitation and subsequent tracing of road infrastructure. This article has a methodical and applied nature, does not claim to be exhaustive, but is focused on presenting basic knowledge.*

KEYWORDS: *linear objects, working geodetic basis, road infrastructure, measurement, roads*

ПРОЕКТИРАНЕ И ИЗМЕРВАНЕ НА РАБОТНА ГЕОДЕЗИЧЕСКА ОСНОВА ПРИ ЗАСНЕМАНЕТО НА ПЪТИЩА С ЦЕЛ РЕХАБИЛИТАЦИЯ [1]

ПЕТЬО П. СПАСОВ

АБСТРАКТ: *Линейните обекти са връзката между населените места. Те могат да бъдат транспортни - пътища, жп линии, метро, вело алеи, пешеходни алеи или комуникационни - кабелни, водопроводни, газопроводни, топлопроводни и други трасета, за които е необходимо да се изготвят инвестиционни проекти. В настоящата разработка ще се разгледа именно точността и методологията при проектиране и измерване на РГО за направата на геодезическа снимка, с цел създаване на проекти за рехабилитация и последващо трасиране на обекти от пътната инфраструктура. Настоящата статия има методически и приложен характер, няма претенции за изчерпателност, а е ориентирана към представяне на базови знания.*

Линейните обекти са връзката между населените места. Те могат да бъдат транспортни - пътища, жп линии, метро, вело алеи, пешеходни алеи или комуникационни - кабелни, водопроводни, газопроводни, топлопроводни и други трасета, за които е необходимо да се изготвят инвестиционни проекти. За изработването на един качествен инвестиционен проект, би трябвало проектантите да разполагат с добра изходна информация, ситуационни планове, карти, геодезически заснемания, нивелации, които са всъщност дело на инженери-геодезисти.

В настоящата разработка ще се разгледа именно точността и методологията при проектиране и измерване на РГО за направата на геодезическа снимка с цел създаване на проекти за рехабилитация и последващо трасиране на обекти от пътната инфраструктура. Комбинацията от инструменти, която се използва в представения вариант е ГНСС и дигитален нивелир. Известно е, че при изработването на инвестиционни проекти от този тип се изисква по-висока точност във вертикално отношение [3]. Това е така, защото при проектирането на пътища, пътнотранспортните инженери имат за задача да изчислят

[1] Настоящата статия е частично финансирана по проект №РД-08-82/27.01.2020 г.

работните разлики, нивелетите, дебелините на настилките, обемите на полагания материал (асфалтобетон). Ако проектантът не разполага с добра геодезическа снимка на местността, фактически няма да има възможността да направи качествен проект. Няма да може да изчисли коректно работните разлики, обемите, както и да даде добро решение за вертикално планиране. По-лошо от всичко е, че това се разбира едва, след като вече се започне работа по изпълнение на проекта. Затова една многозначителна задача е добрата изходна геодезическа основа.

Проектирането на РГО започва в канцеларски условия. Определят се предполагаемите места за стабилизиране на новите точки, видимостта между тях, изискваната точност от възложителя [3]. Изработва се предварителна схема – проект в подходящ мащаб, а след посещение на обекта и проучване на местността се вземат адекватни решения за позициониране на новите нивелачни репери. Окончателните схеми на мрежите се представят във вид определен с наредба [3].

„т. 1. схема на опорната мрежа - с изобразени изходни точки с червен цвят, новоопределени точки - син цвят, планови връзки между точките - черен цвят, и нивелачен ход между точките и реперите - тъмнозелен цвят със сплайн линия“ [3];

„чл. 267, ал. 5. Възложителят определя в заданието за проектиране на всеки конкретен обект изискванията си за гъстотата, начините на стабилизиране и точността на опорната мрежа - планово и височинно“ [3].

В нашия случай определената точност е ±50 mm в хоризонтално отношение и ± 2 mm във вертикално отношение и максимално разстояние между реперите не повече от 200m.

Координирането на новите точки става чрез ГНСС посредством референтна базова станция, станционирана на съществуващите в близост точки до обекта от държавната триангулачна мрежа, ГММП или РГО, като се взема под внимание тяхното състояние и точност.

Според инструкция №РД-02-20-25 [1] средната квадратна грешка на новоопределените точки от работната геодезическа основа не трябва да надвишава ±50 mm. В хоризонтално отношение това би било задоволително, но във височинно е недопустимо да се работи с подобна точност. Затова е необходимо да се направи геометрична нивелация чрез нивелир.

Нивелиране на редица от точки чрез включен нивелачен ход.

За определянето на надморските височини на един ред от точки (1, 2, 3 ...n), предварително означени на терена и координирани чрез ГНСС, посредством геометрична нивелация са възможни два случая:

- Нивелиране на редица от точки чрез нивелачен ход, при който надморските височини на началната точка на хода НР(А) и крайната точка НР(В) са дадени;
- Нивелиране на затворен нивелачен ход, при който е дадена надморската височина само на една точка (НР(А) ≡ НР(В)) [2].

Известно е, че и за двата варианта са приложими формулите [2]:

- Разликата от сумата от отчетите назад и сумата от отчетите напред –
  (1) $\sum a - \sum b = \Delta h'_{AB}$

- Разликата от височините на двата репера –
  (2) $\Delta h_{AB} = H_B - H_A$

- Несъвпадението –
  (3) $f_h = \Delta h'_{AB} - \Delta h_{AB}$

- Допустимото несъвпадение –
  (4) $f_{h.\text{доп.}} = \pm 30\sqrt{\sum D}$

- Поправката към превишенията –
  (5) $v_{i,k} = \frac{-f_h}{\sum D} D_{ik}$

- Определяне височините на новите точки –
  (6) $h_{i,k} = h'_{i,k} + v_{i,k}$,

  където:
  D_{ik} – разстояние.

По – добра практика е да се работи чрез затворения полигон, особено ако точността на дадените репери е ±50 mm. При изходни репери със споменатата точност е твърде вероятно да се натрупат грешки в новоопределените точки, които драстично повлияват на геодезическата снимка и пропорционалността на новоопределените точки една спрямо друга.

Нека се разгледа следният пример. Трябва да се направи нивелачен ход от НРА с H_A = 100.00 m, mh = ±50 mm до НРВ, с H_B = 115.10m, mh = ±50 mm, чрез който да се определят четири нови репера – (НР(1), НР(2), НР(3), НР(4)), като се приеме, че сумата от разстоянията между тях е $\sum D_{ik} = 1000$ m. Използван е нивелир с точност ±1 mm/km двойно пронивелирано разстояние.

- Разлика между сумата от отчет „напред“ и отчет „назад“:
  (1) $\Delta h'_{AB} = \sum a - \sum b$ = 14.999 m;

- Разликата от височините на двата репера:
  (2) $\Delta h_{AB} = H_B - H_A$ = 15.10 m;

- Несъвпадението:
  (3) $f_h = \Delta h'_{AB} - \Delta h_{AB}$ = - 0.101 m.

Ако се замести във формула (5) ще се установи, че трябва да нанесат поправки на новите репери пропорционално на разстоянието между тях. За да бъде по - нагледен примерът, новоопределените точки са точно през 200.00 m, което означава че всеки репер ще бъде поправен с + 20 mm. Видно е, че дори и да се направят точни измервания, чрез прецизна геометрична нивелация, ако не се разполага с надеждни изходни данни, не могат да се постигнат качествени резултати (фиг. 1).

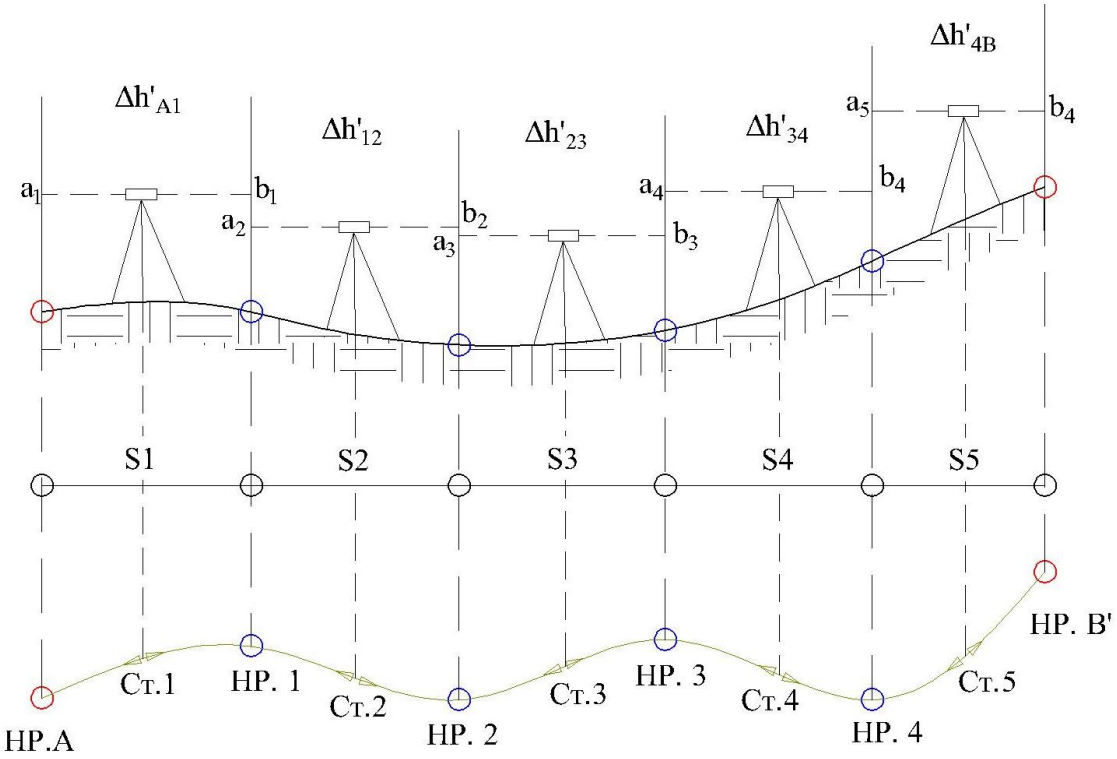
Друг пример, включващ двойно повече работа е измерването на нивелачен ход с единствен даден НР (А). Това означава да се направи нивелация от т. А до т. В’ и за да изчислим несъвпадението и да направим проверка се включваме отново в т. А (дадения репер).

Тогава за несъвпадението се явява:

Разликата между сумата от отчет „назад“ и отчет „напред“ -
(3) $f_h = \sum a - \sum b$ = -0.002 m;

По този начин новите репери ще останат пропорционални помежду си и няма да бъдат натоварени с грешката от втория изходен репер.

С така получените по положение ГНСС измервания в комбинация с геометрична нивелация с единствен изходен репер и двойно пронивелирано разстояние, би могло да се направи качествено заснемане на пътната настилка с цел рехабилитация на пътното платно.



Фиг. 1. Геометрична нивелация

ЛИТЕРАТУРА:

[1] Инструкция №РД-02-20-25 от 20 септември 2011 Г. За определяне на геодезически точки с помощта на глобални навигационни спътникови системи.

[2] доц. к. т. н. инж. Паско М. Бакалов, инж. Георги Н. Лазаров, доц. к. т. н. инж. Васил Г. Вълчанов, доц. к. т. н. инж. Иван Ц. Иванов, инж. Димитър Х. Димитров, инж. Радка Х. Янева, „Ръководство за упражнения по геодезия“, Техника, София (1991).

[3] Наредба № РД-02-20-2 от 28 август 2018г.за проектиране на пътища

Име на автор: Петьо П. Спасов
Месторабота: ШУ „Епископ Константин Преславски“
E-mail: p.spasov@shu.bg

PHOTOGRAMMETRIC APPROACH FOR PHOTOGRAPHY OF EPIGRAPHIC MONUMENTS

BOZHIDAR S. STOYANOV

ABSTRACT: *The methods for remote collection and processing of spatial information are applicable not only for large cultural and historical sites, whose location allows good visibility from the air. With the same success, they can be applied in the digital presentation of small artifacts that have been found in the study of cultural and historical sites and are currently part of the expositions of historical museums. This article proposes a methodology that is specially adapted to photogrammetric imaging of epigraphic monuments.*

KEYWORDS: *digital photogrammetry, epigraphic monuments.*

ФОТОГРАМЕТРИЧНО ЗАСНЕМАНЕ НА ЕПИГРАФСКИ ПАМЕТНИЦИ

БОЖИДАР С. СТОЯНОВ

АБСТРАКТ: *Методите за дистанционно събиране и обработване на пространствена информация са приложими не само за големите културно-исторически обекти, чието разположение позволява добра видимост от въздуха. Със същия успех, те могат да се прилагат и при цифровото представяне на дребни артефакти, които са намерени при проучванията на културно-историческите обекти и по настоящем са част от експозициите на историческите музеи. В настоящата статия се предлага методика, която е специално адаптирана към фотограметрично заснемане на епиграфски паметници.*

1 Особености на класическия подход.

Фотограметрията е научно направление, изучаващо способите за определяне на формата, размерите и пространственото положение на обектите в зададена координатна система по техни фотографски изображения [1]. Чрез фотограметричния подход се получават предимно количествени (*метрични*) характеристики на заснетите обекти.

Първоначално, методът е бил ограничен само до въздушно заснемане на части от земната повърхност с цел – картиране. За целта, са били използвани специално оборудвани самолети.В наши дни, въздушни снимки могат да бъдат получени и от малки безпилотни летателни средства (*БЛА*), наречени за по-кратко дронове. Класическият подход изисква върху терена, който ще се облита, предварително да бъдат маркирани точки с известни координати. Наречени са земни контролни точки – GCP (Ground Control Points). Те са видими на снимките и служат за пространственото привързване на модела. Друга особеност е, че заснемането се извършва от височина, която е съобразена с параметрите на аерофотокамерата и се гарантира желания мащаб на фотографските изображения. Полетът се осъществява по маршрут, разделен на ивици, който осигурява необходимите надлъжни и напречни застъпвания между съседните експонации [2]. При сложни, пресечени терени се налага облитането да се извършва по два маршрута с взаимно перпендикулярни ивици.

2 Методика за заснемане на епиграфски паметници.

Изброените по-горе особености са характерни за класическия подход, при който аерофотокамерата е ориентирана вертикално. Освен по този начин, възможно е фотокамерата да бъде ориентирана хоризонтално или да бъде поставена под перспективен

ъгъл. Въпреки посочените варианти има правила и изисквания, които не се променят и остават в сила без значение начина, по който се осъществява заснемането. Такива например са: главната оптична ос на фотокамерата да е перпендикулярна на повърхността, която се заснема и движението на фотокамерата да се осъществява в равнина, успоредна на повърхността, която се фотографира.

За представянето на малки по размер предмети в цифров вид отпада необходимостта от пространственото им привързване към местността. Отпада и необходимостта от заснемане с дрон. Вместо да бъдат георефериранн, получените модели трябва да се представят в действителен мащаб. Това е важно за да може върху тях да бъдат правени директни измервания и анализи. Заснемането може да се осъществи с бюджетна цифрова камера, закрепена на фотографски статив. Единствено обектива на камерата трябва да бъде със сведени до минимум оптични дисторзии и хроматични аберации.

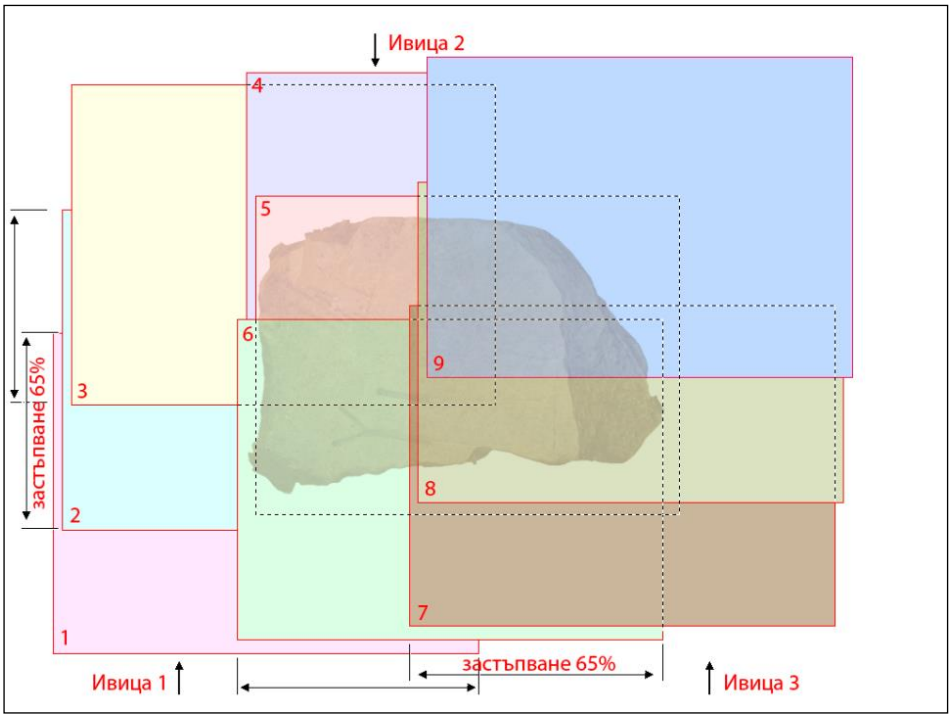
- **Планиране на заснемането.** Включва действията, предхождащи заснемането.

- Вземане на необходимите разрешителни за достъп до експонатите на съответните музеи и за всяко заснемане да се направи уговорка със служителите за деня и часа на посещението, в кое помещение и какви експонати да бъдат извадени и подготвени за заснемане. Достъпът до тях трябва да бъде свободен без наличието на преградни, алармени или защитни съоръжения.

- Дефиниране на локална координатна система. За да се гарантира, че цифровия модел ще бъде в действителен мащаб спрямо оригиналния предмет е необходимо обекта на фотографиране да се обвърже с конкретни метрични стойности, представени в подходяща координатна система. Метричната информация може да се получи чрез разграфяване на мястото, където ще бъде поставен предмета или чрез разполагане в непосредствена близост около него, на измерителни линийки, лати или разпънати рулетки. На (Фиг. 1.) е показано дефиниране на локална координатна система от планквадратната мрежа на топографска карта, поставена зад епиграфският паметник и ориентирана успоредно на лицевата му страна. Разстоянието между две съседни линии от квадратната мрежа е известно и следователно пространсвото зад епиграфският паметник е метрично определено.

Фиг. 1. Привързване на епиграфски паметник към локална метрична система

- Определяне на броя снимки, позицията на фотокамерата и застъпването между отделните експонации. С оглед, постигането на по-бързо заснемане на един епиграфски паметник и по-малко изчислително време за обработката на снимките е важно броят им да се сведе до оптималния минимум. Това се постига, чрез съобразяване на разстоянието, от което ще се фотографира с техническите параметри на цифровата камера (големина на сензора, брой точки в матрицата, фокусно разстояние на обектива и др.). На (Фиг. 2.) е предложена методика, която включва 9 снимки.



Фиг. 2. Схема, описваща методика за заснемане на епиграфски паметник с минимален брой снимки

Заснемането се реализира в три ивици, всяка с по 3 снимки. За да се гарантира добър резултат, трябва да бъдат спазени следните условия:

- надлъжното застъпване между стереодвойките във всяка ивица да бъде минимум 65%.
- странишното застъпване между ивиците също да бъде минимум 65%.
- фокусното разстояние на обектива и разстоянието на камерата от епиграфския паметник да бъдат подбрани така, че цялото лице на камъка да се вижда в снимка №5.
- ориентацията на камерата трябва да е по направление, перпендикулярно на лицето на епигравския паметник.
- придвижването на камерата до точките за експонация да се осъществява по две взаимно перпендикулярни оси, лежащи в равнина - успоредна на лицето на епиграфския паметник.

▪ **Същинско заснемане.** На този етап важен е въпросът за типът на осветлението и разположението на източниците на светлина. Досегашната практика при фотографиране на епиграфски паметници с цел – да се разчете посланието върху тях е включвала осветяване на лицевата страна на камъка под много малък страничен ъгъл (Фиг. 3.). Целта е била да се подчертаят драскотините чрез тяхното засенчване. Когато се прави фотограметрично заснемане сенките не са желани защото информацията в тях ще бъде безвъзвратно изгубена. Всяка точка от повърхността на лицевата страна на камъка трябва

да бъде равномерно и добре осветена. Следователно, източниците на светлина трябва да бъдат подбрани така, че техният брой, светлинната им мощност и разположението им около епиграфският паметник да гарантират дифузно осветление и равномерно разпределение на светлината във всяка точка.

Фиг. 3. Участък от повърхността на епиграфски паметник, заснет с осветяване под малък ъгъл. В плътните сенки има загуба на информация.

3 Заключение

Епиграфските паметници са неразделна част от световното културно-историческо наследство и цифровизирането им е важно за неговото съхранение. В публикацията е предложена методика за цифрово фотограметрично заснемане, основано на класическия подход, но посредством дефинирането на няколко нови правила методът е оптимизиран и настроен за прилагане конкретно върху епиграфски паметници. Условията по заснемане са прецизирани така, че броят на необходимите снимки е сведен до оптималният минимум, при който качеството на получените модели се запазва да бъде максимално, а времето за фотограметричната обработка се намалява значително. Направено е и предложение за равномерна осветеност по време на заснемането с дифузно разпределение на светлината.

ЛИТЕРАТУРА:

[1] Назаров, А. С. 2006, „Фотограмметрия. Учебное пособие для студентов вузов”, Минск, ТетраСистемс, ISBN 985-470-402-5

[2] B. Stoyanov, E. Stoyanov,THE USAGE OF NEW TECHNOLOGIES FOR COLLECTING SPATIAL DATA AND WAYS OF APPLICATION IN ARCHEOASTRONOMY, Publications of the Astronomical Society of Bulgaria (PASB), 2016. , available at: http://astro.shu-bg.net/pasb/index_files/Papers/2016/Stoyanov.pdf , retrieved on 01.12.2016.

Божидар Стоянов
ШУ „Еп. Константин Преславски”, Факултет по технически науки, катедра „Геодезия”
E-mail: b.stoyanov@shu.bg

CRITERIA FOR SELECTING COMPANY VEHICLES IN THE REPUBLIC OF BULGARIA

TSVETOSLAV S. TSANKOV, STANIMIRA TS. STANISLAVOVA

ABSTRACT: *The report advices recommended criteria which should be considered when purchasing company cars. Many manufacturers have introduced unnecessary conveniences in cars, thus losing practical functionality, economy and most importantly - reliability. All criteria that are recommended and are not intended to harm car manufacturers.*

KEYWORDS: *Automotive safety, Company vehicles, Fuel economy, Practical cars, Sport utility vehicle, Value-added tax.*

КРИТЕРИИ ЗА ИЗБОР НА СЛУЖЕБНИ АВТОМОБИЛИ ЗА ФИРМА В РЕПУБЛИКА БЪЛГАРИЯ

ЦВЕТОСЛАВ С. ЦАНКОВ, СТАНИМИРА Ц. СТАНИСЛАВОВА

АБСТРАКТ: *В доклада са дадени препоръчителни критерии, които могат да се вземат предвид при закупуването на служебни автомобили. Много производители са въвели излишни удобства в автомобилите, като по този начин се изгубват практичната функционалност, икономичността и най-важното – надеждността. Всички критерии са препоръчителни и не се цели ощетяването на автомобилните производители.*

Въведение

Големите и средни фирми в Република България използват служебни автомобили, освен тежката транспортна или селскостопанска техника. Тези служебни автомобили се използват, както за бързо придвижване на близки разстояния, така и за далечни командировки. Не е тайна, че една от най-честите им предназначения са за лични нужди – това се оказа проблем за данъчните власти, които направиха неуспешен опит да го предотвратят.

За избора на новите автомобили фирмите на първо място се водят от стойността. Когато автомобила отговаря на условията за приспадане на данъчен кредит, неговата цена значително намалява за фирмите, които са регистрирани по ДДС.

По същество тук са изброени най-важните критерии за избор на служебен автомобил. Всяка фирма разбира се може да има и допълнителни изисквания, които търговеца трябва да удовлетвори, за да се постигне сделка за закупуването и на повече автомобили.

Правото на приспадане на данъчен кредит

Това право не важи за леките автомобили, независимо от това, че се използват изцяло за нуждите на фирмата. Според допълнителните разпоредби в Закона за данъка върху добавената стойност, § 1, т. 18, „Лек автомобил“ е автомобил, в който броят на местата за сядане без мястото на водача не превишава 5. Не е лек автомобил, автомобил, който е предназначен за превоз на товари, или лек автомобил, който има трайно вградено допълнително техническо оборудване за целите на извършваната дейност от регистрираното лице.

Товарните автомобили с хомологация N1 са категория превозни средства, предназначени за превоз на товари, с технически допустима максимална маса не повече от 3,5 *t*. Те в болшинството случаи са с 1+1 места – за водач и пътник/помощник. Основното изискване към тези автомобили е полезният товар да бъде над 2 пъти по-голям от теглото на допустимия брой пътници. N1 версиите на автомобилите са идентични на пътническата им версия от категория M1. За да се спази условието за отношение полезен товар/тегло на пътниците, някои автомобили от категория N1 се произвеждат с 3+1 места (1 е за шофьора), вместо 4+1 при M1. Пример за такъв автомобил е новия Citroën C3 – PureTech 83 S&S BVM Feel /N1/ 3+1 места Euro 6.3 и версията му за лично ползване PureTech 83 S&S BVM Feel /M1/ 4+1 места Euro 6.3.

Право на приспадане на данъчен кредит имат и автомобилите с 6+1 места, т.к. според гореизложената т. 18 не са леки. Обикновено това е комби, на което седалките са: шофьор и пътник на първия ред седалки, трима пътника на втория ред, а в отсека, който е предназначен и за багаж са монтирани две лесно свалящи се, но удобни седалки и предпазни колани. Такъв е например автомобилът с повишена проходимост Audi Q7, който е от висок клас, а като по-евтин автомобил може да се посочи Dacia Lodgy.

Външен вид на автомобила

За ниска цена на автомобила, снежнобелият цвят на купето е най-евтин (фиг. 1). Белият цвят е много добър избор, т.к. прави автомобила лесно забележим, откроявайки се на пътя. Друго предимство е, че не може толкова много да сгорещи колата от слънцето в летните дни, както например кола с тъмносин или черен цвят. За добро съчетаване на повечето възможни рекламни надписи бялото покритие също е подходящо за фирмения автомобил.

Фиг. 1. Най-евтиният вариант за служебен автомобил

Светлосивият и близките до него цветове на колата са много по-неподходящи, от гледна точка на безопасността, т.к. в дадени условия правят автомобила слабо забележим. От този и редица други факти се наложи промяната в Правилника за прилагане на ЗДвП, задължаваща водачите целогодишно през светлата част на деня да управляват МПС с включени къси или дневни светлини. Във връзка с това правило е най-разумно новият автомобил да е оборудван с вградени светодиодни (LED) дневни светлини, т.к. те имат

ниска консумация на електрическа мощност, а това оказва влияние и върху разхода на гориво, особено доловима в градски условия на движение [5], [7].

Към евтината външност спадат черни брони и други външни пластмаси. Те също са голямо предимство, защото пластмасата на тези детайли е по-еластична. Броните позволяващи да бъдат боядисани в цвета на колата са по-твърди и чупливи, но и често с времето получават лош външен вид.

Прозорците на автомобила трябва да осигуряват отлична видимост на окръжаващата среда, като това трябва да се отнася не само за водача, а и за пътниците. Трябва да се избягват автомобили с малки прозорци, като и не са за предпочитане автомобилите с прекалено големи прозорци. Последните имат съществени недостатък – висока себестойност на стъклата, която не позволява да се произвеждат с по-голяма дебелина. Известно е, че челното стъкло придава устойчивост на предните колонки и предната част на покрива, но големият му размер влошава резултата от това свойство.

Двигател

Днес на пазара се предлагат разнообразни двигатели за автомобилите. Двигателите с вътрешно горене (ДВГ) може да бъдат по цикъл на Ото или по цикъл на Дизел. Първият вид могат да бъдат с горивата бензин, пропан-бутан или природен газ. Тези двигатели за среден клас автомобили са с малък работен обем, три цилиндъра и турбокомпресор, резултатът от които е отчитането на висока мощност, но недостатъчен въртящ момент, вследствие на което е лошата динамика и високия разход на гориво в градски условия.

Дизеловите двигатели са много по-икономични, благодарение на високия въртящ момент и много по-високия коефициент на полезно действие в сравнение с бензиновите. При тях проблем са нападките от политици и псевдоекологози, че дизеловите автомобили са големите замърсители на въздуха. Данните обаче показват друго – осезаемо по-ниски емисии на CO_2 и NO_x на дизеловия двигател, относно бензиновия за една и съща кола [9].

Тенденцията за отхвърляне на дизеловите двигатели, последвано от премахването на двигателите с вътрешно горене, не е в сила за товарните автомобили. Принуждават обикновения потребител да се откаже от дизеловия си автомобил, но не могат да задължат производителите да произвеждат големи бензинови двигатели за автобуси и товарни автомобили над 3,5 *t*. За превозите на товари могат да се използват комбинираните превози, но въпреки всички договорености, това не е така и големите товарни автомобили се движат по пътищата, като освен замърсяването, представляват огромна опасност за останалите пътни превозни средства [2], [11].

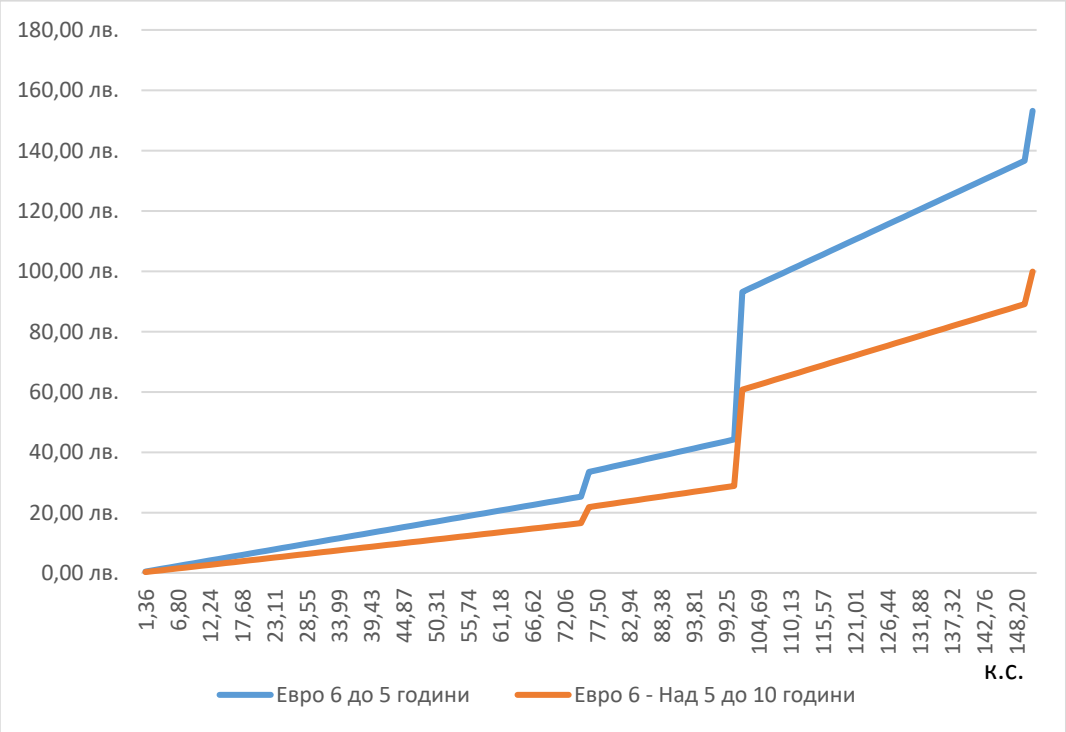
Електромобилите са особено перспективни, според проучвания, но поради високата си цена и неизвестностите относно експлоатационния живот на батериите, няма очаквания интерес и купувачи. Освен тях на пазара се вмъкват и хибридните автомобили, които също имат проблем с малкото живот на батериите, а от друга страна в реална среда при движение по нашите пътища, икономията на гориво е пренебрежимо малка в сравнение със сходна кола, която е само с бензинов двигател.

За да осигурява добра динамика на автомобил от среден клас, двигателят трябва да е с максимална мощност над 90 к.с. и максимален въртящ момент над 220 *Nm*, като повишаването на тези стойности е свързано и с по-голяма първоначална инвестиция, по-висок данък върху превозните средства, по-голям разход на гориво, особено при определени режими на работа [1], [6].

Данъкът върху превозните средства се определя от Закона за местните данъци и такси. В чл. 55 на този закон е уточнено, че за леки и товарни автомобили с технически допустима

максимална маса не повече от 3,5 *t* годишният данък се състои от два компонента – имуществен и екологичен. Имущественият компонент се определя в зависимост от мощността на двигателя, коригирана с коефициент в зависимост от годината на производство на автомобила. Екологичният компонент се определя от общинския съвет в зависимост от екологичната категория на автомобила.

При изпълнение на Наредбата за определяне размера на местните данъци на територията на община Шумен, размерът на данъка за автомобили с екологична категория Euro 6 и EEV, може да се оцени от графиката на фиг. 2.



Фиг. 2. Данък върху превозните средства с Euro 6 в община Шумен

Забелязват се няколко скока в размера на данъка, като най-важният е при мощност 74 *kW* (100,61 к.с.) и двойният му размер при 75 *kW* (101,97 к.с.). В тази връзка е и търговския трик с новия Citroën C3 – BlueHDi **<u>100</u>** S&S BVM Feel /N1/ 3+1 места, привидно 100 к.с. за малкия данък, но в действителност е 102 к.с. за двойния данък.

Произвеждат се автомобили с много по-мощни двигатели от препоръчителните 100 к.с. [10]. Високата стойност на автомобила, скъпото техническо обслужване и големият разход на гориво са проблеми, които не касаят никой друг, освен собственикът на превозното средство. Тук възникват двата големи проблема за човечеството и природата:

- автомобилите с голяма мощност са предвидени за движение с високи скорости, които никак не могат да се съобразят с максимално допустимите, като така се предизвикват водачите на тези автомобили да нарушават и да създават опасност за околните;
- голямата мощност се постига с голям разход на гориво, при завишени стойности на вредните емисии, като така просто се допуска по-голямо замърсяване на околната среда от един автомобил.

В последните години масово се произвеждат автомобили, които не позволяват стартирането на пусковия електродвигател без да е натиснат педала за съединителя. Това

разбира се е с цел предпазване от инциденти и се прилагаше дори и в много стари японски автомобили. Проблемът при това е, че при отцепването на съединителя се създава товар върху плъзгащите аксиални лагери на коляновия вал, а те първоначално работят в условията на сухо триене, поради липсата на налягане в маслената магистрала [3], [8].

Още една неудачна „екстра“ е Stop & Start. Тази система служи за изключване на двигателя, когато автомобила е в задръстване или изчакване на светофар. Когато педала на съединителя се натисне при автомобилите с ръчна скоростна кутия, или педала на спирачката се освободи при автомобилите с автоматична скоростна кутия, двигателя се включва. Това изглежда много полезно, когато е представено от търговеца, който продава автомобила, но в действителност води до намален живот на стартера, акумулатора, влошаване на температурния режим на двигателя и др.

Окачване, колела и трансмисия

Изборът на автомобил със задвижване само на предните колела, или на пълноприводен автомобил, трябва да бъде съобразен със условията в които ще се експлоатира. Автомобилите с повишена проходимост, най-известни с търговското си наименование 4×4 (колесната формула), са подходящи за сняг и лед, кал и други влошени пътни условия. Разбира се това предимство има своята цена при първоначалната инвестиция за закупуването на автомобила, повишена стойност на техническото обслужване, а като най-тежък разход може да се посочи високият разход на гориво. По последния недостатък се работи с въвеждането на новите технологии за хибридно задвижване с ДВГ и електродвигатели или хидромотори със свободен ход.

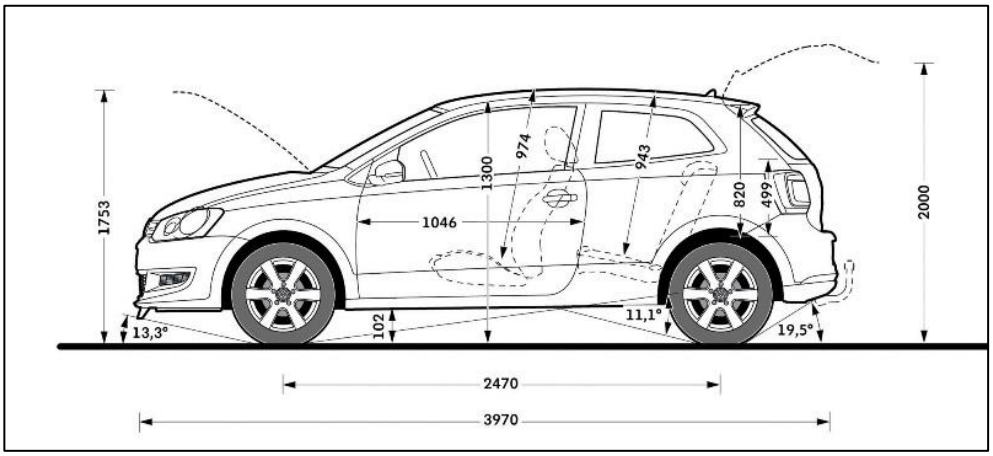
Силно увредените пътища, полските и горски пътища, могат да нанесат огромни поражения по шасито и двигателя на автомобила. За движението по такива пътища не са подходящи автомобили с малък пътен просвет (клиренс), каквито са повечето леки автомобили. Например Volkswagen Polo има пътен просвет 102 cm по спецификации от производителя (фиг. 3 а).

Пълноприводните автомобили с повишена проходимост обикновено имат особено голям пътен просвет, както и големи ъгли, определящи колко големи препятствия може да бъдат преминавани без да има сблъсък с тях. Един такъв завиден пример е актуалния и познат на пазара Dacia Duster / Renault Duster / Nissan Terrano (фиг. 3 б). Той е от т.н. SUV (sport utility vehicle – спортно превозно средство) и както много други от своя клас се предлага в евтин вариант със задвижване само на предните колела. Това е отличен компромисен вариант за безпроблемно движение по пътища с препятствия и без усложнена конструкция с повишен разход на гориво [13], [14].

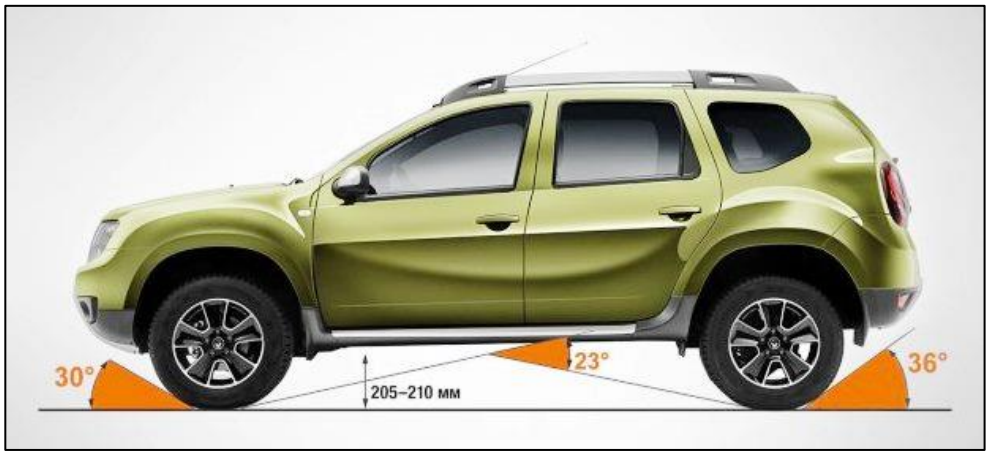
Поради особеностите на българските пътища възниква още една дилема: колелата да имат гуми с нисък или с висок профил. Безспорни са предимствата на нископрофилните гуми – по-голяма джанта с възможност за по-големи спирачни устройства, по-добра устойчивост в завой при високи скорости, но най-важен е пониженият разход на гориво. При ударите с неравностите по пътя обаче, ръбът на джантата срязва гумата, поради малкото разстояние, което позволява свиване на напомпаната гума [2], [3].

Гумите с висок профил са с по-ниска цена, когато са в комплект със стоманени джанти. Те осигуряват по-комфортното движение и намалената вероятност за срязване по обичайните пътища с неравности в Република България. Пътищата у нас никога няма да станат по-добри, а това се дължи на една очевидна преценка – увеличаващата се пътна мрежа с автомагистрали ще отнема все повече ресурс и средства за твърде скъпата им поддръжка. Автомагистралите са с приоритет при рехабилитацията на пътната

инфраструктура, следвани от първокласната пътна мрежа, а всички останали пътища ще се ремонтират некачествено и то само в краен случай.



а)



б)

Фиг. 3. Пътен просвет на автомобилите

За автомобилите с автоматична скоростна кутия е известно, че имат висок разход на гориво. Но те разбира се имат своите предимства при градско управление, както и за водачи с намалена работоспособност. Автомобилите с ръчно избираеми предавки са най-евтини и са доказали най-добър разход на гориво. Една сравнително нова конструкция предавателни кутии са т.н. DSG (direct-shift gearbox – предавателна кутия с директна смяна), които могат да се наредят по функционалност и характеристики между кутията с ръчно избираеми предавки и масовата автоматична скоростна кутия [1], [4], [12].

Предните спирачни механизми на предлаганите автомобили във всички случаи са дискови, докато на задните колела те могат да бъдат дискови или барабанни. От теорията е известно, че при спиране масата на автомобила се пренася към предните колела, поради което не е необходимо толкова голямо спирачно усилие за задните. Така единственото предимство на дисковите спирачки, че са по-силни, не е особено необходимо за задните спирачки, а дори и да са дискови, те са с много по-малки размери от предните.

Задните барабанни спирачки имат няколко предимства пред дисковите:

- затворени са и не са изложени на пряко замърсяване;
- при тях е много по-добра паркинг спирачката, без особено усложнение на конструкцията;

— много по-малка вероятност за задържане и излишно триене в сравнение с дисковите спирачки;
— по-ниската им цена.

Един от незабележимите детайли по автомобила, когато се избира за работа във фирмата, това е конструктивното изпълнение на окачването. Основни проблеми създава предното окачване, а колкото по-сложно е то – много по-скъпа ще бъде неговата поддръжка. Десетилетия наред, като най-достъпно и ефективно се доказва окачването Макферсон с един долен носач. Единственият проблем при него е, че много производители изработват шарнирния болт заедно с носача, а това се завежда като консуматив и има висока цена. Шарнирите, които имат възможност за демонтиране от носача имат много по-голям живот, поради възможността да бъдат закупени по-качествени, докато шарнир, който е изработен с носача, трябва да бъде много скъп и се подменя с нискокачествени заместители.

Интериор

Възможностите за удобства в интериора на автомобила в днешни дни са неизброими. За служебен автомобил разбира се трябва да се избягва лукса не само заради цената. Кожените тапицерии създават впечатлението за практичност, поради лесното почистване дори с обикновена гъба. Влошения комфорт и честите заболявания по кожата на човек обаче би трябвало да насочи купувача към обикновените тапицерии от плат, които въпреки всичко подлежат на успешно почистване дори и с обикновена перяща прахосмукачка. Тапицерията от плат по задната част на седалките е много по-устойчива на пробиване с ръбести предмети.

Автомобила трябва да осигурява лесно боравене с уредите, приборите и механизмите му. Всеки сам трябва да прецени доколко това условие удовлетворява самия него, защото освен всичко друго, от това ще зависи и безопасността на всички. Препоръчително е на контролното табло освен задължителния скоростомер да има термометър и нивомер за охлаждащата течност, индикация за налягането и нивото на маслото в картера на двигателя, т.к. всички те са изключително важни за предотвратяване на сериозни повреди по двигателя.

Заключение

Всички насоки в настоящия доклад са препоръчителни и по никакъв начин не трябва да повлияват на вече направен избор от потребителите. Много от нас вярват в компетентността на търговеца, но трябва да се знае, че неговата цел е преди всичко да продаде автомобил от марката на която е представител.

В днешни дни не може да се залага на марка автомобили, както това е било в миналото. Компании поглъщат други компании, японски автомобили се прикриват с емблеми на европейски автомобили и още редица съвместни производства могат да излъжат бъдещите собственици на нови автомобили.

Екологичните норми, които не могат да бъдат покрити след петата година от повечето автомобили, също ще станат голям проблем за фирмите потребители, които са заложили автомобилите си като актив за по-дълго време. Всевъзможни нови системи оскъпяват автомобилите, но така се изгубват практичност, икономичност, надеждност и дълговечност.

Голямата мощност дава самоувереност на водачите, поради което мощните автомобили стават твърде опасни за останалите участници в движението. Това разбира се е

взето предвид при изчисляването на данъци и застраховки, но това са само пари в хазната, които по никакъв начин не правят водача по-отговорен и не спасяват човешки живот.

ЛИТЕРАТУРА:

[1] Евтимов, И., Иванов, Р. Влияние на някои експлоатационни фактори върху разхода на гориво на автомобилите. Научни трудове на Русенския университет, том 54, серия 4, ISSN 1311-3321 (2015).

[2] Станева, Л.А. Методика за провеждане на експеримент за радиална еластичност. Научна конференция "30 год. Технически колеж - Ловеч", ISSN 2535-079X (2019).

[3] Станева, Л.А. Определяне на радиалната деформация за автомобилна пневматична гума. Научна конференция "30 год. Технически колеж - Ловеч", ISSN 2535-079X (2019).

[4] Bogdanov, A., Dyankov, P. Choosing a complete delivery circuit for multimodal transport operator. International scientific online journal SocioBrains, Issue 35, July (2017).

[5] Balevski, A., Balevski, I., Lyubenov, D. Investigation of the Speed of Running of Cars on Lipnik Blvd., Rousse. Proceedings of University of Ruse, Vol. 57, book 4.1, ISSN 1311-3321 (2018).

[6] Balevski, I., Lyubenov, D. Experimental Examination of an Active Safety System in the Vehicle. Proceedings of University of Ruse, Vol. 57, book 4.1, ISSN 1311-3321 (2018).

[7] Evtimov, I., Ivanov, R., Stahchev, H. Comparative analysis of air pollutions of eco-vehicles using flexible fuel. Proceedings of University of Ruse, Vol. 56, book 4, ISSN 1311-3321 (2017).

[8] Kadikyanov, G., Lyubenov, D., Evtimov, I., Ivanov Y. A Study of Pressures in Pneumatic Tyre Influence on Vehicles Braking Deceleration. INTERNATIONAL VURTUAL JOURNAL Machines, Technologies, Materials, Issue 7, ISSN 1313-0226 (2014).

[9] Kostadinov, S., Lyubenov, D. Balbuzanov, T. Comparative analysis of the methods for determining of the values of spare parts to cars. Proceedings of University of Ruse, Vol. 57, book 4, ISSN 1311-3321 (2018).

[10] Ivanov, R., Evtimov, I., Ivanov, Ya. A study and comparison of fuel consumption of a hybrid and a classic car in city motion. Proceedings of University of Ruse, Vol. 55, book 4, ISSN 1311-3321 (2016).

[11] https://www.dacia.bg/

[12] https://www.porsche.com/central-eastern-europe/en/_bulgaria_/

[13] http://www.ralpin.com/

[14] https://www.vw-lekotovarni.bg/virtualno-izlozhenie

Имена на авторите: доц. д-р инж. Цветослав Станиславов Цанков,
Месторабота: Шуменски университет „Епископ Константин Преславски“
E-mail: c.cankov@shu.bg

Станимира Цветославова Станиславова

STUDY OF TRIBOLOGICAL CHARACTERISTICS' INFLUENCE UPON PROJECTILE ANGULAR VELOCITY

YANA D. DIMITROVA, ANDREY I. BOGDANOV

ABSTRACT: *Due to bullet-rubber chopper wheel interaction phenomena, friction forces reveal which are caused by the tribological characteristics in contact between them. These friction forces alter the initial and angular velocity of projectile which result in bullet' trajectory change. An analytical model has been developed for the study of the problem, and the report presents the part of it related to the change of the angular velocity of the bullet (projectile).*

KEYWORDS: *projectile, bullet, angular velocity, tribological characteristics*

ИЗСЛЕДВАНЕ ВЛИЯНИЕТО НА ТРИБОЛОГИЧНИТЕ ХАРАКТЕРИСТИКИ ВЪРХУ ЪГЛОВАТА СКОРОСТ НА ПРОЕКТИЛ

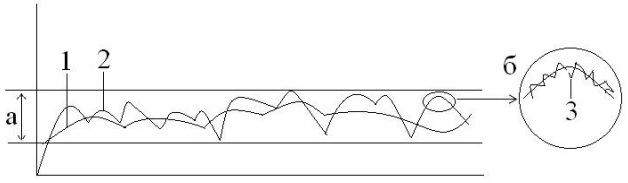
ЯНА Д. ДИМИТРОВА, АНДРЕЙ И БОГДАНОВ

АБСТРАКТ: *Преминаването на куршум (проектил) през гумен обтюратор е свързано с възникване на сили на триене породени от трибологичните характеристики на детайлите в контакта. Тези сили на триене изменят стойностите на постъпателната и ъгловата скорости на проектила, което от своя страна променя траекторията описвана от куршума. За изследването на проблема е разработен аналитичен модел, като доклада представя частта от него свързана с изменението на ъгловата скорост на куршума.*

1 Въведение

В трибологията телата се разглеждат като повърхностни слоеве с множество микро и макро грапавини (фиг. 1. – „2“ и „3“), които зависят от същността, точността и метода на обработка на детайлите. Характеристиките на повърхностните слоеве са от значение за повърхностното взаимодействие, защото оказват влияние върху реалната зона на контакт, триене, износване и смазване.

При движението на едно тяло спрямо друго, силата на триене се дължи на контакта на грапавините на материалите, където се образуват контактни петна (фиг. 1. – „б“).



Фиг. 1. Изображение на грапавините на повърхностните слоеве а – реална контактна зона; б – контактно петно; 1 – грапавост: 2 – макро-грапавини: 3 – микро-грапавини.

Контактните петна от своя страна образуват зоната на контакта (фиг. 1. – „а“), която се състои от грапавини с различна височина (фиг. 1. – „1“) и се образува по външните повърхнини на детайлите.

При явлението изстрел, проектила (куршума) получава определени стойности на въртеливо движение (ъглова скорост), което има за цел да му осигури стабилност по време на полета.

При използване на шумозаглушител камерен тип, проектиран с гумен обтюратор, в определен момент проектилът преминава през гумения обтюратор. Процесът на механичен контакт между проектила и гумения обтюратор е свързан с възникване на сили на триене в резултат от трибологични характеристики на контактната схема, която образуват двата детайла.

Трибологичните характеристики могат да бъдат определени като сили на триене проявяващи се в резултат от преминаването на проектила през гумения обтюратор на шумозаглушителя от камерен тип. Силата на триене е насочена в противоположна посока на силата пораждаща въртеливата скорост на куршума, в резултат на което тази скорост се изменя [4, 5, 6].

В резултат от анализа на движението на проектила през гумения обтюратор, като контактна схема, може да се заключи, че при този процес възникват следните сили на триене, породени от трибологичните характеристики на изследваната схема:

- сила на триене при плъзгане;
- сила на триене при въртене;
- сила на триене от течението на газовете;
- адхезионна сила на триене;

2 Цел

Целта на доклада е представяне на метод за определяне изменението на ъгловата скорост (силата пораждаща въртеливо движение) на куршума (проектила) при проявящи се трибологични характеристики и определяне и изчисляване на зависимостите изменящи тази скорост.

3 Определяне на зависимостта между силите на триене в резултат на трибологичните характеристики и силата пораждаща ъгловата скорост на проектила

Изчисляването на изменението на ъгловата скорост на проектила, в резултат от силите на триене породени от трибологичните характеристики, се извършва посредством формулата за определяне изменението на скоростта, на всяко движещо се тяло, съгласно зависимостта за закъснително движение [2, 3, 7, 9]:

(1) $$\omega_0 = \omega_d - [(a_\tau + a_n).t_1] \quad [s^{-1}],$$

където: ω_0 – начална ъглова скорост на проектила след преминаването му през гумения обтюратор [s^{-1}];

ω_d – дулна ъглова скорост [s^{-1}];

a_τ – тангенциално ускорение на проектила [s^{-2}];

a_n – нормално ускорение на проектила [s^{-2}];

t_1 – време необходимо за преминаване на проектила през обтюратора [s].

Съгласно динамиката на ротационно движение, тангенциалното ускорение на проектила се изчислява по формулата [2]:

(2) $$a_\tau = \frac{l_o}{t_1} \quad [m/s],$$

където: l_o – дебелина на обтюратора [m];

t_1 – време необходимо за преминаване на проектила през обтюратора [s].

Нормалното ускорение на проектила се изчислява по формулата [2]:

(3) $$a_n = \frac{M}{I} \quad [s^{-2}],$$

където: M – момент на сила спрямо ос [N.m];

I – инерционен момент на материална точка [$kg.m^2$].

Момента на сила спрямо ос се изчислява по формула [2]:

(4) $$M = F_w . R_k \quad [\text{N.m}],$$

където: F_w – сила на триене при въртеливо движение [N];

R_k – радиус на проектила [m].

Съгласно динамиката на твърди тела инерционния момент се изчислява по формулата [3]:

(5) $$I = m . R_k{}^2 \quad [\text{N.m}^2],$$

където: m – маса на проектила [kg];

R_k – радиус на проектила [m].

Силата F е силата получавана в резултат на триенето между проектила и обтюратора при въртеливото му движение. За изчисляването на пълната сила на триене, след извършване на анализ на контактната схема и използвайки формулите за изчисляване силата на триене съгласно изчочници [1, 8, 10], се събират компонентите на силите на триене, които се проявяват при контакта на проектила с гумения обтюратор. В рзултат на това за изчисляването ѝ се използва формулата:

(6) $$F_w = \mu_\omega . (W + F_r) + F_v + F_a \quad [\text{N}],$$

където: F_w – сила на триене при въртеливо движение [N];

μ_ω – коефициент на триене при въртеливо движение;

W – нормално натоварване [N];

F_r – сила на триене за ротационни детайли [N];

F_v – сила на триене при флуидни течения [N];

F_a – адхезионна сила на триене [N].

За изчисляване на коефициента на триене при въртеливо движение се използва формулата [5, 7]:

(7) $$\mu_\omega = \frac{V_d}{\omega_d} . \mu,$$

където: V_d – дулна постъпателна скорост [m/s];

ω_d – дулна ъглова скорост [s^{-1}];

μ – коефициент на триене при плъзгане.

Изчисляване на нормалното натоварване се извършва посредством формула от модела на Херц [8]:

(8) $$W = \frac{4.N.E^*.S_r^{\frac{3}{2}}}{3.\pi^{\frac{3}{2}}.\mathcal{R}} \quad [\text{N}],$$

където: N – брой на издатините на грапавините;

E^* – ефективен модул на еластичност [N/m^2];

S_r – реална контактна площ [m^2];

$\mathcal{R}$ – комбинирана кривина [m].

За изчисляване на силата на триене при флуидни течения се използва формулата [5]:

(9) $$F_v = \frac{h^2.\eta}{t_1} \quad [\text{N}],$$

където: h – хлабина между куршума и обтюратора [m^2];

η – динамичен вискозитет на газа [Pa.s];

t_1 – време за преминаване на куршума през обтюратора [s].

За изчисляване на адхезионната сила на триене се използва формулата [1, 8, 10]:

(10) $$F_a = \tau_a . S_r \quad [\text{N}],$$

където: τ_a – напрежение на срязване [N/m^2];

S_r – реалната контактна площ [m^2].

За изчисляване силата на триене за ротационни детайли се използва формулата по модела на Петров [10]:

(11) $$F_r = \frac{2.\pi.\eta.{R_k}^2.l_o.\omega_d}{h} \quad [\text{N}],$$

където: η – динамичен вискозитет на газа [Pa.s];

R_k – радиус на проектила [m];

l_o – дебелина на обтюратора [m];

ω_d – дулна ъглова скорост [s^{-1}];

h – хлабина между проектила и обтюратора [m].

За изчисляване на реалната контактна площ се използва формулата на Братнева Г. М.-Лаврентьева В. В. [1]:

(12) $$S_r = S_a \,.\left[1 - k_1.e^{-\delta.\left(\frac{W}{S_a}.E\right)^{\frac{2}{3}}}\right] \quad [\text{m}^2],$$

където: S_r – реалната контактна площ на полимерни материали [m^2];

S_a – номинална площ на допиране [m^2];

$k_1 = 0.8 \div 1$ – табличен коефициент;

$e = 2{,}71$ – неперово число;

δ – нормално приближение;

W – нормално натоварване [N];

E – еластичен модул на гумения обтюратор [N/m^2].

Съгласно модела на Бартенева Г. М. - Лаврентьева В. В. нормалното приближение се изчислява по формулата [1]:

(13) $$\delta \cong 1{,}2.\left(\frac{\alpha\,.\mathcal{R}}{R_z}\right)^{\frac{1}{3}},$$

където: δ – нормално приближение [бездименсионен];

∂ – параметър отчитащ съотношението на грапавините;

$\mathcal{R}$ – комбинирана кривина[m];

R_z – височина на грапавините на профила [m].

Параметърът отчитащ съотношението на грапавините се определя по формулата [1]:

(14) $$\partial = \frac{n_o}{n_m},$$

където: n_o – среден брой на грапавините;

n_m – брой грапавини на единица номинална площ.

Куршумът (проектила) има сложна форма, поради което номиналната контактна площ, трябва да се раздели на две части – конусна и цилиндрична част. Тогава:

(15) $$S_a = \left(2.\pi.r_{cy}.l_{cy}\right) + \left(\pi.r_{co}.c\right) \quad [\text{m}^2],$$

(16) $$c = \sqrt{{r_{co}}^2 + l_{co}^2} \quad [\text{m}],$$

където: S_a – номинална контактна площ (площта на куршума) [m^2];

r_{cy} – радиус на цилиндричната част на куршума [m];

l_{cy} – височина на цилиндричната част на куршума [m];

r_{co} – радиус на основата на конуса на куршума [m];

c – образувателна на дължината на конуса [m];

l_{co} – дължина на конуса [m].

Времето необходимо за преминаване на проектила през обтюратора се изчислява по формулата [2, 3, 7, 9]:

(17) $$t_1 = \frac{l_o}{V_d} \quad [\text{s}],$$

където: l_o – дебелина на обтюратора [m];
V_d – дулна постъпателна скорост [m/s].

4 Изводи

1. Предложен е метод за изчисляване изменението на въртеливата скорост на проектила (твърдо метално тяло), в резултат от силите на триене за проявяващи се трибологични характеристики, при преминаването му през гумен обтюратор (полимер).

2. Предложената формула за изчисляване пълната сила на триене обединява силите на триене при наличие на течение на газове, адхезионна сила на триене и сила на триене от динамичното движение на тялото (въртеливо движение на проектила).

3. За вземане на научнообосновани решения относно възможността за използване на предложения метод е необходимо да се извърши оценка адекватността му посредством обработка на резултати от теоретични и емпирични изследвания.

ЛИТЕРАТУРА:

[1] Беркович И. И., Громаковский Д. Г., Трибология. Физические основы, механика и технические приложения. Самара, (2000).

[2] Григорьев А.Ю., Малявко Д.П., Федорова Л.А. Теоретическая механика. Кинематика: Учеб. пособие. СПб.: НИУ ИТМО; ИХиБТ, (2013).

[3] Екснер Г. Обща физика 1. Механика и молекулна физика за химици. Университетско издателство „Паисий Хилендарски“, (2016).

[4] Христов, Х. Алгоритмичен подход при изследване динамиката на системи твърди тела. Механика на машините / Национален комитет по теория на механизмите и машините. – Варна, ISSN 0861-9727 (2000).

[5] Христов, Х. Експериментално изчислителни методики за определяне скоростта на движение на снаряда в тялото на оръдие. Научна сесия на Фак. "Артилерия, ПВО и КИС”- Шумен: сборник научни трудове. - Шумен: Нац. военен унив. "Васил Левски", ISSN1314-1953, (2010).

[6] Христов, Х. Определяне полиномиална зависимост между количеството барут - начална скорост на мината при 60 мм миноxвъргачка. Научна конференция "40 години Шуменски Университет" т.4, Шуменски Университет, Шумен, ISBN 978-954-577-620-5 (2012).

[7] Amirov SH., Elementary physics. Baku, (2012).

[8] Bhushan B., Introduction to Tribology. 2nd Edition. USA, (2013).

[9] Lahiri A., Basic physics. Principles and concepts. Fourth revision. I., (2017).

[10] Rebai H., Tribology and machine elements. Subject of Bachelor’s thesis. Riihimäki: HAMK, (15.08.2014).

Име на автор(ите): Яна Димитрова Димитрова
Месторабота: Катедра „Въоръжение и технологии за проектиране“ на Факултет „Артилерия, ПВО и КИС“ към НВУ „Васил Левски“
E-mail: dimitrovax2yana@gmail.com
доц. д-р инж. Андрей Илиев Богданов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Инженерна логистика“
E-mail: a.bogdanov@shu.bg

METHOD FOR THE SELECTION OF A LOGISTICS PROVIDER BY USING EXPERT ASSESSMENT

ANDREY I. BOGDANOV YANA D. DIMITROVA

ABSTRACT: *Solution selection tasks are very common in logistics practice. It is so because of various factors that influence the whole process of the decision-making. The report deals with an example algorithm for selecting a logistics provider by using expert assessments.*

KEYWORDS: *logistics, algorithm for selecting, expert evaluations*

МЕТОД ЗА ИЗБОР НА ЛОГИСТИЧЕН ПОСРЕДНИК ЧРЕЗ ИЗПОЛЗВАНЕТО НА ЕКСПЕРТНИ ОЦЕНКИ

АНДРЕЙ И. БОГДАНОВ ЯНА Д. ДИМИТРОВА

АБСТРАКТ *Задачите за избор на решение са много често срещани в логистичната практика. Тяхното разнообразие, се поражда от множеството фактори които влияят върху изработването на решението. В доклада е разгледан примерен алгоритъм за избор на логистичен посредник чрез използването на експертни оценки.*

1 Въведение

Сред моделите и методите, използвани в логистиката, може да се открояят редица модели, които позволяват да се вземе решение за избора на най-добра алтернатива от няколко налични. Това са моделите по избор на технически посредници, вземане на решения „направи или купи“, избор начин на транспорт, избор на превозно средство, избор на стратегия за управление на запасите, възможност за инвестиции в логистичната инфраструктура и много други практически задачи, решавани в различни области на логистиката на предприятието.

2 Избор на логистичен посредник

Изборът на логистични посредници като: доставчици, спедитори, превозвачи и др., е най-често срещаната задача за повечето функционални области на логистиката. Очевидно е, че при наличие на конкуренция във всички звена на логистичната система се наблюдава много вариантност, която се изразява както в голям брой посредници, които могат да извършват съответните операции, така и в присъствието на алтернативни решения, формирани от различни връзки на логистичната система [9].

В логистичната литературата широко са разгледани въпросите за избора на посредници, които, се различават главно по дълбочината на проучването и разгледаните примери. В повечето източници изборът на логистични посредници се извършва в условия на определеност и се разглежда като еднокритериален или многокритериален проблем.

От анализа на литературните източници [1, 2, 3, 5 и др.], могат да се разграничат два подхода, за избор на логистичен посредник:

- аналитичен, на избор се извършва чрез формули, които включват редица параметри, характеризиращи логистичните посредници;

- експертен, който се основава на оценките на експерти за параметрите, характеризиращи логистичните посредници, и са описани процедурите за получаване на интегрални експертни оценки (рейтинги).

Аналитичният подход е универсален, но включените в него параметри на логистичните посредници могат да изискват експертна оценка [5].

При експертния подход рейтингите често се използват като критерий за избор на логистичен посредник. В литературата разгледаните алгоритмите и примерите за изчисляване на интегрални (рейтингови) оценки за логистични посредници са много и разнообразни. В [4] е представен един от възможните начини за сравнителна оценка на превозвачите. Изчислението включва два етапа:

- първата стъпка на всеки критерий се присвоява определено „тегло“, отразяващо относителното му значение за изпращача.

- втория етап ефективността на превозвача се оценява за всеки критерий, като същевременно се използва и тристепенна скала: 1 - висока ефективност, 2 - средна, 3 - ниска.

Рейтингът за всеки критерий се определя чрез умножаване на рейтингите "относителна важност" и "ефективност", а крайният рейтинг на превозвача - чрез сложна оценка. В таблица е 1 показана примерна оценката на превозвач въз основа на описания метод за избор.

Таблица 1 Примерна рейтингова оценка на превозвач

Критерий за оценка	**Относителна значимост**	**Ефективност на превозвача**	**Рейтинг на превозвача**
Разходи	1	1	1
Транспортно време	3	2	6
Надеждност (стабилност на транспортното време)	1	2	2
Технически и сервизни възможности	2	2	4
Достъпност	2	2	4
Безопасност	2	3	6
Общ рейтинг на превозвача	**-**	**-**	**23**

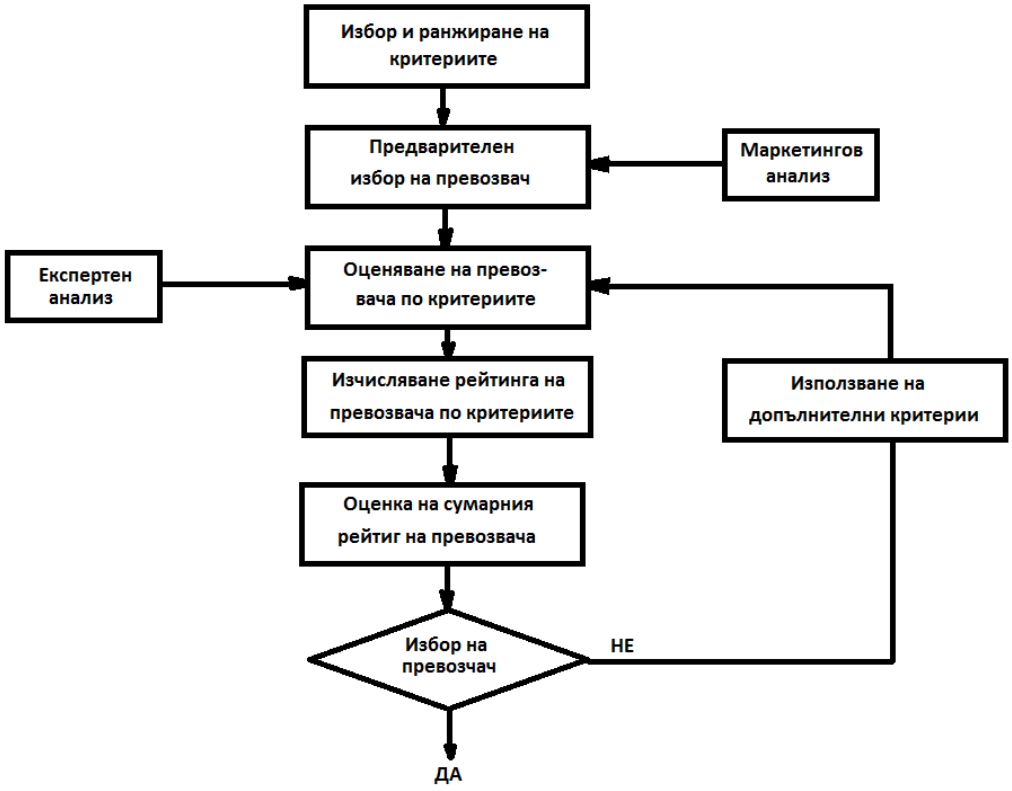
По-сложен е алгоритмичния подход за избор на превозвач [4] (фиг. 1). Практическото използване на алгоритми за изчисляване на рейтинги е ограничено в практиката. Една от причините за това е, че участието на експерти в процедурите за оценка не е формализирано и варира в широки граници.

Един примерен вариант включва:

1. Общо описание на N показатели (критерии), характеризиращи определен тип логистичен посредник;

2. Ранжиране на показателите;

3. Определяне на точки (рангове) на оценките;



Фиг. 1. Алгоритъм за избор на превозвач

4. Избор на *M* показателя (критерия) за оценка на логистичните посредници от общия брой избрани показатели *N*;

5. Определяне на тегловни коефициенти ω_i, за *M* показателя по формулата:

$$\omega_i = \frac{M}{i}, \qquad (1)$$

където *i = 1, 2, ..., N* е ранг (бал), преписан на *i-тия* показател.

6. Избор на скала за оценка на показатели за конкретни логистични посредници, например „добро“ (*1*), „удовлетворителен“ (*2*), „лошо“ (*3*) и др.;

7. Определят се точки на всеки *j-ти* логистичен посредник, т.е. действителната процедура за оценка под формула (1) за оценката a_{ij} за *i-ти* индикатор и *j-ти* логистичен посредник;

8 Изчислява се интегрална оценка A_j за всеки *j-ти* логистичен посредник:

$$A_j = \sum_{i=1}^{n} \omega_i a_{ij}, \qquad (2)$$

В таблица 2 са показани резултатите от изчисляването на рейтингите, получени съгласно описаната последователност. Най-добрият резултат съответства на по-ниския ранг, следователно вторият логистичен посредник ще бъде най-предпочитан.

Таблица 2. Рейтинги на логистични посредници

Критерии	Ранг	Тег-ло	I превозвач		II превозвач		III превозвач	
			оцен-ка	рей-тинг	оцен-ка	рей-тинг	оцен-ка	рей-тинг
1. Надеждност на дос-тавките	1	5,0	3	15,0	1	5,0	2	10,0
2. Тарифи за превоз	2	2,5	1	2,5	2	5,0	3	7,5
3. Финансова стабил-ност	5	1,0	1	1,0	3	3,0	2	2,0
4. Безопасност на товара	9	0,55	3	1,65	2	1,10	2	0,42
5. Проследяване на пратките	12	0,42	2	0,84	2	0,84	1	0,42
Сумарен рейтинг				**20,99**		**14,94**		**21,02**

Този метод предвижда участие на експерти в седем операции, което, от една страна, затруднява и оскъпява получаването на крайните резултати, от друга страна, води до различни варианти за избор на логистичен посредник дори за една и съща логистична система поради произволните оценки и субективността при извършване редица операции

Натрупаният опит от оценяването дават възможност за разработването на обща методика за избор на логистичен посредник при следната последователност:

1. Всички показатели (критерии) са разделят в три групи: количествени, качествени, логически („да“/„не“). Това позволява да се използват различни подходи при тяхното определяне и изчисляване на интегрални оценки за логистичния посредник.

Логическите показатели са тези които включват, имат само два отговора: „да“ или „не“. Например посредникът има ли подходящ сертификат за качество или лиценз, застрахователни полици, допускане до определени процедури (международни превозвачи), предоставяне на допълнителни услуги и др. Логическите показатели увеличава обективността на процеса на подбор, а също така намалява обема на работата на експертите.

Подреждане на критериите, подходящо за последващ подбор на зависимостта, според което се изчисляват коефициентите на тежест.

Един от методите за ранжиране на критериите е методът за двойно сравнение, по време на който се попълва матрицата I_{kj}. Елементите на матрицата могат да бъдат определени по формулата:

$$\begin{bmatrix} I_{jk} = 1 \rightarrow X_k = X_j \\ I_{jk} = 0 \rightarrow X_k < X_j \\ I_{jk} = 2 \rightarrow X_k > X_j \end{bmatrix}, \qquad (3)$$

Знаците за равенство, „по-малко“ и „по-голямо“ съответстват на еквивалентността на критериите, съответно по-малката и по-голяма значимост на един критерий в сравнение с друг.

Въз основа на резултатите от ранжирането, се избират тегловите коефициенти, като се отчита степента на влияние на показателите върху общата оценка. При линейна или близка до линейна зависимост тегловите коефициентите се изчисляват по формулата:

$$\omega_i = \frac{2(N-i+1)}{N(N+1)}, \qquad (4)$$

където N е броят на взетите под внимание показатели $i=1,2,....,N$.

При нелинейна зависимост тегловите коефициентите се определят по формулата:

$$\omega_i = \Delta_\tau e^{(-x_i)}, \qquad (5)$$

където x_i - средата на *i-тия* интервал, $i=1,2,....,N;$

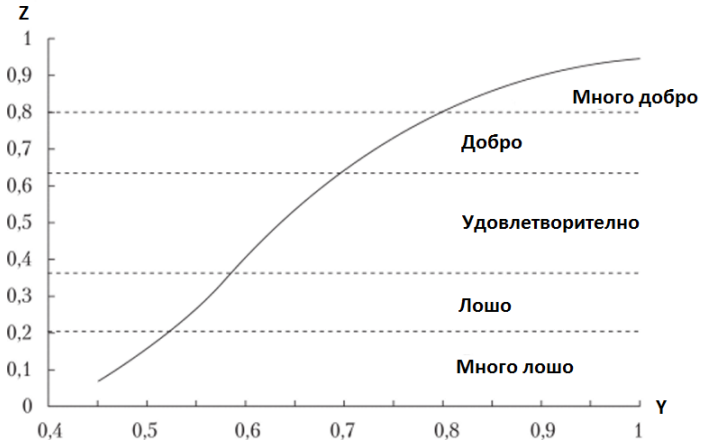
Δ_τ - интервал, изчислен като се вземат предвид броят на показателите и обхватът на стойностите *x*.

За определяне на тегловите коефициентите могат да се използват и други зависимости, по – специално плътността на разпределението на вероятностите (закон на Поасон, нормален закон и др.).

За определяне на стойностите на количествените показатели освен експертни оценки се използват различни източници на информация (доклади, справочници, ценови листи, резултати от проучвания и анкети и др.).

Обработката на количествените показатели се извършва в съответствие с методите за измерване на качеството.

За да се получат оценки на качествените показатели, се използва функцията на Харингтън [7] (Фигура 2).



Фиг. 2 Стойности на функцията на Харингтън

Използването на функцията Харингтън позволява да се намалят качествените оценки на показателите до количествени, като и двете са в диапазона *0 - 1*.

Изчислява се обща оценка и рейтинг на доставчика. Тази оценка е сумата от оценки на количествени и качествени показатели за работата на логистичния посредник, като се вземат предвид тегловите критерии.

При многократен избор на логистичен посредник, е важно да се контролира неговата дейности. Съществуват много методи за оценка на качеството, включително интуитивен, статистически, експериментален и др.

Използването на функцията Харингтън позволява да се намалят качествените оценки на показателите до количествени, като и двете са в диапазона *0 - 1*.

Изчисляване на обща оценка и рейтинг на доставчика. Тази оценка е сумата от оценки на количествени и качествени показатели за работата на логистичния посредник, като се вземат предвид тегловите критерии.

3 Заключение

Разгледания метод за избор на логистичен посредник, намалява субективизма при вземане на решение и осигурява стройна система за класиране на кандидатите при нужда от избор. Използването на различни източници на информация (доклади, справочници, ценови листи, резултати от проучвания и анкети и др.) води до конкуренция между експертите и стремеж за осъществяване на обективна класация на кандидатите [6, 8].

При многократен избор на логистичен посредник, е важно да се контролира неговата дейности. Съществуват много методи за оценка на качеството, включително интуитивен, статистически, експериментален и др.

ЛИТЕРАТУРА:

[1] Вауэрсокс Дональд Дж., Дейеид Дж. Логистика: интегрированная цепь поставок. - Москва: Олимп-Бизнес, 2001. - 640 с.

[2] Гаджинский А. М. 11рактикум по логистике. - 2-е изд., перераб. и доп. Москва: ИВЦ „Маркетинг“, 2001. 180 с.

[3] Сергеев В. И. Менеджмент в бизнес-логистике. - Москва: Филинъ, 2007.

[4] Ballou Ronald H. Business Logistics Management. - Prentice-Hall International, Inc., 2009.

[5] Coylejohn J., Bardi EdwardJ., Langlay John Jr. The Management of Business Logistics. A. Supply Chain Perspective, 1-e - South-Western devise of Thomson Harming, 2003.

[6] Kodzheykova, V., Y. Yankova-Yordanova. Methodology for logistics system management in medium serial production. Journal scientific and applied research, USA, EBSCO, ISSN 1314-6289 (2019).

[7] Tolles, Juliana; Meurer, William J (2016). "Logistic Regression Relating Patient Characteristics to Outcomes". JAMA. 316 (5): 533-4. doi:10.1001/jama. 2016.7653. ISSN 0098-7484. OCLC 6823603312. PMID 27483067.

[8] Yankova-Yordanova, Y., Ts. Tsankov. New approaches in the management of reverse logistics. SocioBrains, www.sociobrains.com, Publ.: Veselina Nikolaeva Ilieva, Bulgaria, Issue 62, October, ISSN 2367-5721 (2019).

[9] Yankova-Yordanova, Y., V. Kodzheykova. Expert approach for analysing a logistics control system and quality management in the conditions of small and medium serial production. Journal scientific and applied research, USA, лицензиран в EBSCO, Volume 15, ISSN 1314-6289 (2019).

Име на автор(ите): доц. д-р инж. Андрей Илиев Богданов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Инженерна логистика“
E-mail: a.bogdanov@shu.bg
Яна Димитрова Димитрова
Месторабота: Катедра „Въоръжение и технологии за проектиране“ на Факултет „Артилерия, ПВО и КИС“ към НВУ „Васил Левски“
E-mail: dimitrovax2yana@gmail.com

INTEGRATED MATERIAL MANAGEMENT IN THE SUPPLY CHAIN THROUGH ERP SYSTEMS

ALEKSANDAR I. BORISOV

ABSTRACT: *Materials management (MM) is a core functionality of every Enterprise Resource Planning system. The functionality within MM is the engine that drives logistics and supply chain management. The report describes the importance of the MM functionality in the context of the overall functionality of ERP software and as part of supply chain*

KEYWORDS: *Materials management, Enterprise Resource Planning system Production Planning, Quality Management Warehouse Management.*

ИНТЕГРИРАНО УПРАВЛЕНИЕ НА МАТЕРИАЛИ ПО ВЕРИГАТА ЗА ДОСТАВКИ ЧРЕЗ ERP СИСТЕМИ

АЛЕКСАНДЪР И. БОРИСОВ

АБСТРАКТ: *Управлението на материалите (Materials management (MM) е основна функция на всяка система за планиране на ресурсите на предприятието ERP. Функциите в MM са двигателят, който движи логистиката и управлението на веригата за доставки. Докладът описва значението на функционалността MM в контекста на цялостната функционалност на ERP софтуера и като част от веригата за доставки chain*

1 Въведение

Управлението на материалите е основна част от функционалността на всяка ERP система в контекста на цялостната и работа, и в частност като елемент от веригата за доставки. Реализацията му посредством ERP софтуер включва много аспекти, като снабдяване, получаване на материалите, съхранението им, консумация на база планиране и ревизия. Това предполага висока степен на интегриране на модула за управление на материали (MM) с финансово-счетоводен (FI), планиране на производството (PP), продажби и дистрибуция (SD), контрол на качеството (QM) и модула управление на склад (WM). Управлението на материалите заема централно място при всяко имплементиране на ERP система и модулът отговарящ за реализацията му се явява основен двигател, фактор и компонент на веригата за доставки.

За да се оцени напълно значимостта на управлението на материалите трябва да бъде разгледан начина по който се интегрира с останалите модули и мястото което заема в ERP структурата. Започвайки с основната му роля в множество бизнес процеси постепенно ще се разкрие как се използва като основна част от логистичната система и веригата за доставки.

2 Изложение

Всяка логистична система контролирана от ERP софтуер е съвкупност от няколко компонента следващи движението на материалите от производител до клиент. При това основна цел на логистиката е управление на бизнес процеси и операции включващи снабдяване, съхранение, транспортиране и разпространение по веригата за доставки. Тя е мрежа от разпространители, дистрибуционни канали, транспортни компании, складови

площи и доставчици участващи в продажби, доставка и производството на определен продукт.

От логистична гледна точка и съобразно веригата за доставки модулът за управление на материалите е неразделна част от логистичните функционалности на всяка една ERP система. При работа с (MM) по веригата за доставки е необходимо да се отчетат слените три основни потока:

- Материалният поток описва движението на материали от доставчика до компанията и следващото от компанията до клиента (трябва да се предвидят и обратните движения от компанията към доставчик и от клиент към компанията, поради рекламации, грешни количества, материали, и т.н.). В днешно време много компании не просто работят, а се кооперират с някои доставчици и клиенти. Следователно всяко подобрение върху мониторинга на материалните потоци което може да бъде осигурено ще позволи на компаниите да бъдат по-гъвкави и способни да отговорят на изискванията на клиентите. Целта на всеки клиент е да работи с компании отзоваващи се на нуждите му. Такива компании постигат растеж на пазара благодарение на гъвкавост, бързина и надеждност.

- Информационния поток включва придвижваните заявки и поръчки в електронен вид (посредством EDI), и поддържане на актуална информация за статуса на всички доставки. Компании, които могат да предоставят детайлна информация в реално време на клиенти и доставчици рязко се открояват и са предпочитан партньор на фона на останалите.

- Финансовият поток включва финансовите документи създадени при всяко едно материално движение. Ако даден материал има стойност, движението независимо кредитно или дебитно се осъществява между съответните акаунти за да отрази придвижването и.

След като дефинирахме на логистичните функции и потоците по веригата за доставки нека идва въпросът как ERP софтуера обезпечава нейния контрол и въз основа на това предимство на компанията в силно конкурентна среда. Организацията и управлението на логистичната система трябва да е реалистично, всеобхватно, координирано, прозрачно, лесно контролируемо, икономично, гъвкаво и адаптивно [1].

ERP софтуера осигурява нужните материали, на нужното място в нужното време и нужното количество на нужната конкурентна цена. Истински напредък и големи ползи ще бъдат постигнати, когато фирмата контролира този процес включително отношенията си с доставчици и клиенти. Също така (MM) позволява контрол на наличността, прогноза на клиентските заявки и получаване на навременна информация съобразена с всички аспекти на транзакциите по веригата за доставки.

Основен принцип при проектирането на логистична система е първичното идентифициране на протичащите процеси и техните характеристики. Само тогава е възможно да се установят връзките между тях за да се постигне истинско оптимизиране и максимални печалби [3].

Разглеждайки по-подробно цялата структура, функционалностите и компонентите включени в управлението на веригата за доставки се убеждаваме, че въпреки основното значение на (MM) като интегрална част от логистиката, модулът е само една от частите в такава сложна система. За да функционират добре всички компоненти, или модули на ERP системата трябва да обвързани с реалните бизнес процеси протичащи в компанията. Някои основни от логистична гледна точка и на веригата за доставки бизнес процеси в които модулът за управление на материали играе централна роля са:

- При този бизнес процес заявката за снабдяване с материал може да бъде създадена ръчно създадена от бизнес потребител или автоматично генерирана от модула за планиране

на производството и снабдяването. Изискването на даден материал в (MM) започва със заявка за купуване, която се конвертира в искане за оферти които се разпращат до свързаните доставчици. При получаването офертите от доставчици се записват (поддържат автоматично) в искането за оферти. Следва сравняване на цените от всички получени оферти и избор на доставчик за искания материал. Останалите оферти се маркират като отхвърлени, за да не продължи определен потребител да ги обработва поради грешка. До отхвърлените доставчици се изпращат уведомителни писма. Избраната оферта се конвертира в количества, стойност и доставни срокове под формата на поръчка. В зависимост от приоритетите поръчката може да подлежи на процес на одобрение, изразен в освобождаването (разрешаването) и от определен в йерархично потребител. След освобождаване на поръчката материалът бива доставен, приет в склада. Фактурата на доставчика бива системно записана, проверена (наличие на заявка, приета стока и фактура) и на доставчика му се плаща.

- Обикновено продуктите се произвеждат в самата компания, като планирането включва не само производството, но и необходимите материали, и опаковки (които много често се поръчват на външен доставчик). Планирането се осъществява посредством приложение за планиране на материалите (MRP). Бизнес процесът на закупуване на материали инициира снабдяването с нужните материали и опаковки. След приемането има в склада на компанията производствения процес може да започне. Изписването на суровини, материали и опаковки необходими за производството на даден продукт включва използването на (IM) функционалността (управление на наличности) като неразделна част от модула за управление на материали. След приключване производството на даден продукт той бива доставен в склада, отново използвайки (MM) модула.

-Търговските и дистрибуционните процеси започват след получаване на запитване от клиент на компанията за определен продукт от каталога и. Това запитване се записва, поддържа и обработва от модула за управление на търговията и дистрибуция (SD). На база запитването търговските агенти генерират оферта до клиента (системните номера на запитването и офертата са обвързани). Ако клиента приеме офертата тя се трансформира в поръчка за продажба (SO). При готовност продукта да бъде доставен на клиента компанията го изписва от склада, като системно материалното движение е обвързано с конкретната поръчка за продажба. Технически това материално движение (като инвентаризационен процес) отново се осъществява посредством модула за управление на материали. Стоката се фактурира на клиента и след получаване на плащането то бива записано системно във вземанията по сметки.

-Управлението на поддръжката, като резервните части и консумативи необходими за работата на машинния парк, сграден фонд, и други активи се поръчват посредством разгледаните по-горе бизнес процеси на закупуване на суровини и материали, или се изписват от склада ако има наличност. Това изписване на резервни части и консумативи от склада е процес на управление на наличността (IM), и се реализира като част от управление на материалите (MM), системно обвързано с конкретна поръчка за поддръжка във управление на поддръжката (PM).

Ако разгледаме детайлно веригата за доставки ще се убедим, че (MM) работи в тясна връзка с останалите функционалности и инструменти на ERP софтуера. По този начин се създава ефективна среда за управление на веригите за доставки.

За да се генерира материален поток във веригата за доставки е нужно от ERP системно искане за материали създадено чрез модула за планиране на производството (PP), или от поръчка за продажба генерирана от модула за продажби и дистрибуция (SD). След

създаване на нужния системен документ заявката за доставка се изпраща към снабдителя следвайки инструкциите за количества, доставна дата и цена. Доставчика изпраща дадения материал, който след получаването си може да подлежи на качествен контрол реализиран системно чрез модула за управление на качеството (QM). След одобрение материалът може да се складира използвайки системно модула за управление на склада (WM). В бъдеще материалът може да бъде изискан за дадена производствена поръчка чрез модула за планиране на производството (PP), или да стане част от по-голям проект чрез модула за управление на проекти (PS). В резултат материалът е наличен за клиента, може да бъде изписан от склада чрез сканиране и натоварен за клиента използвайки модула за търговия и дистрибуция (SD). Преминавайки схематично през този опростен поток ние се убеждаваме колко силно е интегриран модула за управление на материалите сред останалите (ERP) функционалности.

Ефективното управление на логистичните процеси е възможно само при наличието на нужната информация за всеки един процес във всичките му стадии [2]. Най-ясен пример за информационен поток е когато той започва с поръчка от клиент. Клиентската поръчка бива предадена на (ERP) софтуера посредством система за електронен обмен на данни (EDI). Информация се обработва в (ERP) системата по различен начин в зависимост от това има ли наличност от поръчаното. Ако няма информацията се изпраща до инструментите на модула за планиране на материалите (MRP). До клиента се връща информация с потвърдени количества и дати за доставка. (MRP) събира цялата информация относно производствени графици, капацитет на машинен парк и сгради, налични материали нужни за производството, и създава производствени поръчки, и искания за материали в системата за снабдяване.

Тази информация в системата за снабдяване създава поръчки с нужните доставни дати, които биват изпратени на доставчиците. Обратната информация от доставчика потвърждава датите за доставка. Доставчика може да изпраща и периодични (EDI) протоколи за потвърждение статуса на определена доставка.

При получаване на материала информацията се предава системно от получените документи към модула за управление на склада (WM), за да се съхрани материалът коректно. Следва предаване на информацията към производствената система (PP), която изчислява дали е налично всичко необходимо за да започне производствената поръчка. Когато материалът е готов за товарене информацията се изпраща до (SD) и от там до клиента.

Цялата информация се записва във всяка една от тези пресечни точки и е достъпна за преглед и анализ. Колкото повече информация се споделя по веригата за доставки, толкова по-добър ефект се постига чрез подобрения на база анализ.

Типичния поток от финансова информация по веригата за доставки включва фактури получени в компанията от доставчик, плащания към доставчици, фактури изпратени към клиент и входящи плащания. Доставчикът снабдява компанията с материали и изпраща фактура за да бъде платена.

ERP системата може да се настрои по два начина за извършване на плащане:

- Плащане при получаване на материала.
- Плащане при получаване на фактурата.

Отделът за плащане на задължения обезпечава тези функции. Процесът на проверка на фактурата е отличен пример за взаимодействието между модулът за управление на материали и този за управление на финансите (FI). Добре работещият ERP софтуер позволява да се анализират ключовите финансови показатели за ефективност (KPI), които

са част от цялостната верига на доставките. Някои от най-често анализираните са оборот на наличността, период за реализация на оборотния капитал, престой на наличността в склада, срок за събиране на вземанията и срок за реализация на плащанията. Интегрирането на (MM) с другите основни в логистично отношение функционалности обезпечава прецизно и навременно тази важна информация.

3. Заключение

Функционалността на модулът за управление на материали е основата или гръбнак на всяка ERP имплементация. Той може да бъде описан като основен двигател на веригата за управление на доставки при ERP софтуера. Освен с голяма част от останалите модули, (MM) може да се интегрира с множество допълнителни приложения и инструменти.

ЛИТЕРАТУРА:

[1] *A. Bogdanov*, "*Metods for analysis of logistics systems*," *in Association Scientific and Applied Research International Journal*, 2015, *ISSN* 1314–9784, *vol.*4, *p* 19–50.

[2] *A. Bogdanov*, "*Analysis of* the *management systems of logistics warehouse operations*," *in Association Scientific and Applied Research International Journal*, 2013, *ISSN* 1314–6289, *vol.* 4, *p* 135.

[3] *A. Bogdanov*, "*Analysis of modern logistics systems*," *in Association Scientific and Applied Research International Journal*, 2014, *vol.* 3, *p* 54.

[4] *J. Akhtar and M. Murray*, *Materials management with SAP S/4HANA. SAP PRESS*, 2018.

[5] *N. Sachan and A. Jain*, *Warehouse management in SAP S/4HANA. SAP PRESS*, 2018.

[6] *A. Y. Khan*, 10 *Steps to a successful ERP implementation. Linkedin*, 2015. [*Online*] *Available*: *https://lincedin.com/pulse/10-steps-successful-erp-implementation-ahmed-yasir-khan*

Име на автора: Александър Борисов Иванов
Месторабота: Фирма „Ново стъкло" ЕАД Нови пазар
E-mail: aib6791@abv.bg

METHODOLOGY FOR DETERMINING THE ECOLOGICAL EFFICIENCY OF A COMBINED TRANSPORT LOGISTICS SYSTEM

MARIYAN I. RAHNEV

ABSTRACT: *Combined transport is the modern technology through which the European Union seeks to reduce the harmful impact (up to 85-90%) on the living environment of the main pollutant in transport - trucks. The use of combined transport can save 30 to 80% of liquid fuels, depending on the distance traveled, significantly reduce road accidents, unload motorways and reduce maintenance costs. Road transport is the most polluting - according to the latest data, it produces 71% of CO2 emissions from transport as a whole (passenger cars produce about two thirds of this amount). Other modes of transport pollute much less. The share of sea and air transport is 14% and 13%, respectively, and of inland waterway transport - only 2%. Rail transport pollutes the least - less than 1% of emissions.*

KEYWORDS: *Combined transport, Ecological efficiency.*

МЕТОДИКА ЗА ОПРЕДЕЛЯНЕ ЕКОЛОГИЧНАТА ЕФЕКТИВНОСТ НА КОМБИНИРАНА ТРАНСПОРТНА ЛОГИСТИЧНА СИСТЕМА

МАРИЯН И. РАХНЕВ

АБСТРАКТ: *Комбинираните превози са съвременните технологии, чрез които Европейския съюз търси да намали вредното въздействие (до 85-90%) върху жизнената среда от основния замърсител в транспорта – товарните автомобили[9]. Използването на комбинирани превози може да спести от 30 до 80% от течните горива, в зависимост от изминатото разстояние, да намали значително пътнотранспортните произшествия по шосе, да разтовари автомагистралите и да съкрати разходите по поддържането им. Шосейният транспорт е най замърсяващият — по последни данни той произвежда 71 % от емисиите на CO2 на транспорта като цяло (личните автомобили произвеждат около две трети от това количество). Другите видове транспорт замърсяват много по малко. Делът на морския и въздушния транспорт е съответно 14 % и 13 %, а на транспорта по вътрешни водни пътища — едва 2 %. Железопътният транспорт замърсява най малко — под 1 % от емисиите.*

1 Въведение

Комбинираните превози обединяват предимствата на конвенционалните видове транспорт и намаляват неговите недостатъци. Развитието на комбинираните превози съдейства за свободното движение на стоки и за разширяване на търговията и точно поради това се издига като един от основните приоритети на транспортната политика на Европейския Съюз.

По своята същност комбинираният транспорт представлява ефективна интеграция на различни видове транспорт, т.е. на отделни транспортни оператори и инфраструктурни предприятия в контекста на транспортната логистична верига. Той е познат още и под наименованието интермодален или мултимодален транспорт [1], [3], [5].

2 Определяне на екологичната ефективност

Транспортът е процес на пространствено преместване на хора и стоки във времето. В този процес не се създава нова продукция в натурално-веществена форма, а само се увеличава стойността на транспортирания обект. Транспортната логистична система

представлява рационално организирана съвкупност от два или повече видове транспорт[3], осъществяващи превозната дейност на основата на конкуренцията и взаимодействието между тях. Тя по своята същност представлява подходи, принципи и методики за планиране, контрол и управление на транспорта.

Методиката за определяне на екологичната ефективност включва:

— избор на технология за комбиниран транспорт;

— Системата "Подвижно шосе (Ro-La)", която е с няколко технологии:

-Ro-La придружавани превози – целият камион се качва на платформен вагон и има отделен вагон за шофьорите на камионите;

-Ro-La не придружавани превози – на „джоб" вагон се качват само ремаркетата без влекачите;

-Ro-La превози при които се комбинират контейнери и не придружавани превози.

Избира се Ro-La придружавани превози.

Една от основните причини за развитието на „Ro-La" превозите е търсенето на нови възможности за решаване на транспортните проблеми свързани със замърсяването на околната среда [2], [4]. Товарния автомобилен транспорт оказва съществено въздействие за замърсяването на околната среда, поради което в Европейските директиви са заложени норми за допустимите количества на отделяните в атмосферата вредни емисии (CO_2- въглероден диоксид, SO_2- серен диоксид, NH_3 - амоняк, Pb - олово и др.).

— отчитане на екологичната ефективност – за отчитане на екологичната ефективност

— от автомобилния транспорт, съществуват три подхода, отразяващи степента на влияние на вредните емисии:

-опростен подход – базира се на използването на емисионни параметри, определени на база на изразходваното гориво и условие на пътуване – извън населено място и режим на работа на двигателя – топъл.

(1) $$E_{AT,i}^{cx} = L_{AT} \cdot EF_i \text{ , } [g]$$

където:

E_i - масата на съответната емисия;

L_{AT} - изминат път [км];

EF_i - емисионен параметър за съответната емисия i [g/km].

-детайлен подход - базира се на използването на емисионни параметри, определени на база на изразходваното гориво и условие на пътуване – населено място, извън населено място и автомагистрала. Емисията за всяко едно от тях се получава от сумиране на емисиите при два режима на работа на двигателя – топъл и студен (в населено място). Може да се въведе и показател „възраст на превозното средство".

(2) $$E_i^{\text{общо},j} = E_i^{\text{студен},j} + E_i^{\text{топъл},j} \text{, } [g]$$

където:

E_i - маса на съответната емисия;

j- отчита съответния режим на движение.

-комплексен подход – прилага се чрез програми, симулиращи превозният процес, като се базира на: техническите характеристики на превозните средства, възраст, технически въведения за намаляване на замърсяването и други.

3 Определяне броя на автомобилите във влаковата композиция

За разглеждания вид комбиниран превоз в състава на влака влизат локомотиви, спален вагон за автомобилните водачи и специализирани вагони за превоз на товарни автомобили [7], [8], [9]. По формула 3 се определя броят на автомобилите в една влакова композиция, който е равен и на броят на специализираните платформени вагони:

(3) $$N_a^{ВЛ} = \frac{Q_{с.max} - Q_{сп}}{q_{авт} + q_{ваг}}, \text{ бр.}$$

където:
$Q_{с.max}$ - максимална тежина на влака, *t*;
$Q_{сп}$ - масата на спалния вагон, *t*;
$q_{авт}$ - тегло на автомобила, *t*;
$q_{ваг}$ - тегло на един платформен вагон (тара), *t*.

изчисляване на вредните емисии от товарен автомобил на собствен ход - $E_{AT,i}^{сх}$ по формула:

(4) $$E_{AT,i}^{сх} = K_a L_{AT} \cdot EF_i, [g]$$

където:
E_i - масата на съответната емисия;
L_{AT} - изминат път [km];
EF_i - емисионен параметър за съответната емисия i [g/km];
K_a - коефициент, отчитащ допълнителни фактори на влияние.
изчисляване на вредните емисии от превоз на товарен автомобил с жп. транспорт – E_{ro-la} по формула:

(5) $$E_{ВЛ,i} = k_в \cdot Q_{бр} \cdot L_{вл} \cdot Рел.EF_{елi}, [g]$$

където:
$Q_{бр}$ – бруто тегло на влака [t]
$L_{вл}$ - изминат път [km];
$EF_{елi}$ - емисионен параметър за съответната емисия i [g/km];
$Рел$ – консумирана ел. енергия [kWh/бр.тон.км];
$k_в$ - коефициент, отчитащ допълнителни фактори на влияние.
сравнение на получените резултати от двата вида превози и определяне на ефективността по условието, отнесено за един автомобил

(6) $$E_{AT}^{жт} < E_{AT}^{сх}$$

изчисляване на екологичната ефективност $П_{ек}$ в стойностно изражение:

(7) $$П_{ек} = (E_{AT}^{сх} - E_{AT}^{жт}) \cdot C_{EF}, \text{ лв. или /EUR/}$$

Използвани са данни за Емисионни параметри, отнесени за километър пробег, показани на табл. 1 [6], [10].

Таблица 1. Емисионни параметри съгласно методика CORINAIR-94

Вид МПС	замърсители, *g*/*km*					
	NO_X	VOC	CH_4	CO	CO_2	N_2O
товарен автомобил (ср. разход 30,8 *l*/100 *km*)	10,9	2,08	0,06	8,71	800	0,03

При изчисляването на екологичната ефективност в стойностно изражение – $П_{ек}$, е ползвана емисионна ставка от 30 EUR на тон. Получените от изчисленията резултати за вредните емисии от движението на автомобил на собствен ход са дадени в таблица 2.

Таблица 2. Резултати за вредни емисии от движението на автомобил на собствен ход

МПС, брой	замърсители, *g*/*km*					
	NO_X	VOC	CH_4	CO	CO_2	N_2O
1	4591,08	876,096	25,272	3668,652	336960	12,636

Понеже имаме 24 тежкотоварни автомобила, т.е. колкото са и броя на вагоните в състава на влака, получените резултати за вредните емисии от движението на автомобилите на собствен ход са дадени в таблица 3.

Таблица 3. Резултати за вредни емисии от движението на автомобилите (24 бр.) на собствен ход

МПС, брой	замърсители, *g*/*km*					
	NO_X	VOC	CH_4	CO	CO_2	N_2O
1	110185,9	21026,3	606,528	88047,64	8087040	303,264

Вредни емисии /CO_2/от железопътния превоз:
- $E_{ВЛ,i}$ = 6720924 g;
- $E_{AT}^{жт}$ = 280038,5 g.

Екологичната ефективност за CO_2 от Ro-La превоза е:
- за влак - 673920 g;
- за автомобил - 56921,5 g.

Екологична ефективност в стойностно изражение:
- за влак -80,27 лв.;
- за автомобил - 3,34 лв.

4 Заключение

Комбинираният превоз „автомобил–железница“ представлява екологична алтернатива на товарния автомобилен превоз [6], [8]. От тази гледна точка напълно оправдани са мерките за преориентиране на част от превозите от автомобилен на комбиниран транспорт. Приоритетните оперативни цели и задачи са:

- развитие на комплекс от железопътни товарни възли отговарящи на стандартите на ЕС и способни да допълват и да се конкурират ефективно с други видове транспорт;

- модернизиране на железопътната мрежа в съответствие с нуждите на участниците в товарния транспорт и ефективно конкуриране с пътната мрежа;

- подобряване на услугите и насърчаване употребата на товарен жп транспорт между заинтересованите страни за привличане на повече потребители и оператори и установяване на общо разбиране и сътрудничество с други заинтересовани лица и стопански субекти;

- иницииране и насърчаване разработването на необходимите законови и институционални разпоредби;

- предприемане на необходимите действия за изграждане на модерни подпомагащи системи;

- изграждане и експлоатация на „товарни селища“ и продължаващо развитие на мрежите и системите на интермодалния транспорт.

Постигането на целите на ЕС за климата изисква силно намаляване на емисиите на въглероден диоксид на транспорта, които представляват поне 20 % от парниковите емисии на ЕС [5], [7]. За да се намалят световните емисии с 80 % количеството, необходимо за поддържане на изменението на климата в безопасни граници (увеличение на температурата с не повече от 2 °C), транспортният сектор трябва да намали емисиите си с 60 % до 2050 г.

ЛИТЕРАТУРА:

[1] Беров, Т., Стайков, Д., Стаменов, В., Стоянов, И. Подход за определяне ефективността на Ро-Ла превози през България. ВТУ „Т. Каблешков“, София.

[2] Димитров, П., Толев, М., Тодоров, Ф. Логистични системи. УИ „Стопанство“ (2010), ISBN 978-954-644-130-0.

[3] Пламен Дянков, Антон Антонов. Мултимодални превози и насоки за развитието им в България. "INTERNATIONAL SCIENTIFIC CONFERENCE 2015", Факултет по „А, ПВО и КИС” – гр. Шумен, 2015 ISSN 2367-7902, стр. 160 – 164

[4] Тодоров, Ф. Логистични комплекси. Тракия М (2011), София.

[5] Цанков, Ц., Янкова-Йорданова, Й. Намаляване на последствията от транзитно преминаващите товарни автомобили по пътищата на Република България. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново (2019), ISSN 2535-0315.

[6] Цанков, Ц., Константинова, Е. Подход за използването на електромобили при далечни пътувания. Сборник статии от V международна научно-практическа интернет конференция „Рекултивация выработанного пространства: проблемы и перспективы“, Кузбасский государственный технический университет имени Т. Ф. Горбачева (2020), ISBN 978-5-00137-142-7.

[7] Янкова-Йорданова, Й., Цанков, Ц. Необходимостта от намаляване на неблагоприятните последствия за околната среда при транзитен превоз на товари. Седма международна научна конференция „Техника. Технологии. Образование. Сигурност“, Велико Търново (2019), ISSN 2535-0315.

[8] Lilov, V., Borisov, A., Tsankov, Ts. Reducing exhaust emissions by increasing the power-to-volume ratio of the internal combustion engine. Proceedings of the Eighth student scientific conference “Ecology and environment” (2020), ISSN 2367-5209.

[9] Plamen Dyankov, Anton Antonov. Metod za otsenka na efektivnostta na „ro-la „ prevozi. MATTEX 2012, Volume 2, ISSN: 1314-3921, str. 332 – 334

[10] https://ec.europa.eu/info/topics/transport_bg

Име на автора: инж. Мариян Илиев Рахнев
Месторабота: Българска Железопътна Компания „ЕАД“, гр. София
E-mail: marian.rahnev@brc-bg.com

GENERAL MATHEMATICAL CONCEPTS USED IN LOGISTICS OPERATIONS MANAGEMENT

STEFAN M. KAZAKOV

ABSTRACT: *The modern definition of the term model is based on the presented idea, defining the model as a reflection of certain characteristics of the object in order to study it. According to another broader definition, a model should be understood as such a mentally represented or materially realized system, which by reflecting or reproducing the object of research, is able to replace it and give new information about it*

KEYWORDS: *logistic, operation, concepts, managment.*

ОБЩИ МАТЕМАТИЧЕСКИ ПОНЯТИЯ ИЗПОЛЗВАНИ В УПРАВЛЕНИЕТО НА ОПЕРАЦИИТЕ В ЛОГИСТИКАТА

СТЕФАН М. КАЗАКОВ

АБСТРАКТ: *Съвременното определение на понятието модел се основава на изложената идея, дефинирайки модела като отражение на дадени характеристики на обекта с цел неговото изследване. Според друго по-широко определение под модел трябва да се разбира такава мислено представяна или материално реализирана система, която като отразява или възпроизвежда обекта на изследването, е способна да го замества и да дава нова информация за него.*

1. Приложение на понятието модел.

Понятието модел се прилага широко в семантиката, логиката, математиката, физиката, химията, кибернетиката и други науки в различно, макар и близко смислово съдържание. Едни от най-съществените признаци на модела са следните:

а. обективно съответствие с моделирания обект;

б. способност да замества моделирания обект в определени отношения;

в. способност на модела в хода на изследването да дава някаква допускаща опитна проверка информация;

г. наличие на достатъчно ясни правила за преход от моделната информация към информацията за самия обект.

Все още обаче няма единно и общоприето определение на понятието модел. Той може да се определи като: система от представи за едни или други интересуващи ни свойства на даден конкретен обект, процес или явление, за техните взаимни връзки и взаимни зависимости, изразени чрез словесно или писмено описание, чрез създаването на аналогични вещи или процеси, чрез графично представяне с помощта на рисунки или чертежи, чрез описание с помощта на математически символи и системи от формули, уравнения и неравенства, с цел да се получи нова, допълнителна информация за изучавания обект, процес или явление, необходима за неговото изследване.

2. Моделирането като всеобщ метод на познанието

Като метод на познанието и като елемент на абстрактното мислене то съществува от най-дълбока древност.

Методът на моделирането въплъщава в себе си творческата природа на човешкото познание, плодотворно се прилага в научното обяснение на фактите, в теоретичното осветляване на бъдещето, в решаването на все по-сложни и по-сложни задачи, които стоят пред научната мисъл [4], [5].

Колкото по-широка и опосредствана е сферата на взаимодействие на човека с природата чрез производството и науката, в толкова по-големи мащаби се прилага методът на моделирането като инструмент на познанието. Проникването в реалния процес на логистичното развитие, познаването на дълбоките закономерности на това развитие, задълбоченото изучаване на обществените потребности се извършват с помощта на икономико-математическото моделиране.

Моделирането на икономическите процеси е приложение на математическите методи в икономическите изследвания, в анализа и прогнозирането на икономическите системи. В областта на моделирането човечеството е вървяло от по-простото към по-сложното.

Постепенно човекът се е научил при изучаването на сложните явления да ги анализира, да изследва техни аналози, отражения и копия и да насочва усилията си към онези техни свойства и качества, които са представлявали особен интерес от гледна точка както на познанието, така и на практиката.

Моделирането е изследване на обектите на познанието въз основа на техните модели, построяване, анализ и изучаване на моделите на обектите. Понятието моделиране има изключително съдържателен характер, тъй като е познавателна категория. Предмет на моделиране могат да бъдат както конкретни, така и абстрактни обекти (стойност, норма на печалбата, разходи и пр.), както реално съществуващи, така и подлежащи на конструиране системи. Икономико-математическото моделиране е описание на икономическите процеси във вид на математически модели.

През последните десетилетия ролята на моделирането значително нараства във връзка с развитието на персоналните компютри и друга специализирана техника на тяхна основа. Компютризирането много силно разширява областта на явленията, които се поддават на моделиране (явления в живата природа, логистиката, икономиката, езикознанието и т.н.). Основа на моделирането е теорията на подобието, която формулира условията за разпространението на резултатите от експеримента, извършен с някакъв обект (модел) с обекти от друга размерност (във физически или геометричен смисъл) и с друга физическа природа.

В моделирането могат да се проследят три стадия на анализ на: структурата, на динамиката и на връзките между явленията. Изучаването на структурата дава възможност да се разкрият количествените и качествените признаци, да се отсеят съществените от несъществените, да се определят йерархичността или хоризонталната поставеност на структурата и факторите, които влияят върху нейното изменение.

Изучаването на динамиката позволява да се разкрият някои устойчиви признаци на развитието и условията за тяхното изменение.

1. Анализът на връзките между отделни обекти довежда до разкриване на съществените връзки и с това - и на даден вид функции, които ги описват.

2. Най-подходящият модел за изследване на операциите в логистиката са:

- математическите;
- икономико-математическите.

Математически модел на операциите

Операция се нарича всяка съвкупност от действия с оглед постигане на определена цел. От дефиницията на понятието операция се вижда, че то е достатъчно общо и всяка

съзнателна дейност може да се разглежда като операция. Съществуването на цел в една операция предполага съществуването на активни участници, които се стремят да постигнат целта. Опериращa страна се нарича всяка съвкупност от лица, които се стремят към постигане на поставената с дадената операция цел. Наред с лицата, формиращи опериращата страна, съществуват и други лица, които може да имат цели, различни от целта на разглежданата операция. При изучаването на дадена операция изследването се води от позицията на опериращата страна и основната задача се състои в намиране на един или друг начин за постигане на поставената цел. От средата на опериращата страна може да се обособи един неин представител, който се нарича изследовател на операциите.

Изследователят на операциите преследва същата цел, както и останалите членове на опериращата страна. Сам той не взема решения по избора на средствата за действия, но подпомага с научни методи, средства и резултати при формиране на решението. Изследователят обикновено изучава операцията значително по-рано във времето от нейното протичане и по една или друга причина не разполага с достатъчно информация, с която разполагат останалите членове на опериращата страна непосредствено или по време на протичане на самата операция. Всичко това предполага, че изследователят трябва предварително да предвиди тези особени ситуации, трябва да ги изучи и да подготви варианти на решенията [1], [7], [10].

Ще се отбележи една съществена страна на операцията, а именно това, че тя винаги е управляемо мероприятие, т.е. от опериращата страна зависи как да се изберат параметрите, които характеризират дадената операция. "Организацията" се разбира в широк смисъл и включва техническите, финансовите и други средства за провеждане на операцията. Изследователят на операциите използва математическите модели като основно средство за изучаване на операциите. В математическите модели се разглеждат т. нар. активни средства (означават се с a), които по същество са ресурси за провеждане на операцията. Всяко действие за постигане на целта е начин на използване на тези ресурси. Всеки начин на използване на активните средства се нарича стратегия. Прието е стратегиите да се означават с x. Величината x може да бъде вектор, число или функция. Стратегиите по същество са фактори, които се използват от опериращата страна при постигане на дадената цел. Тези фактори са контролируеми от опериращата страна. Обаче наред с контролируемите фактори съществуват и неконтролируеми фактори, влияещи на хода на операциите. Опериращата страна не разполага с неконтролируемите фактори. Неконтролируемите фактори ще означим с променливата y. Те формират т. нар. обстановка на провеждане на операцията.

Описанието на всяка операция в най-общия случай завършва с описание на информираността на опериращата страна и изследователя на операциите за обстановката, при която протича операцията. Наред с това от особена важност е взаимната информираност на отделните части на опериращата страна и изследователя на операциите за решенията, действията и резултатите от действията на тези части.

Математическият модел на операцията трябва да даде количествено описание на последната. Неконтролируемите фактори от гледна точка на това, дали изследователят на операциите има информация за тях, се делят на три групи - фиксирани, случайни и неопределени.

Фиксираните неконтролируеми фактори са известни на изследователя на операциите. Случайните неконтролируеми фактори са известни напълно на изследователя на операциите със законите им на разпределение. Неопределените неконтролируеми фактори са детерминирани или случайни величини, за които е известно само множеството от

стойности или класа на възможните закони на разпределение. Ползата от понятието фиксирани неконтролируеми фактори е в това, че то дава възможност да се обособят някои величини, на които опериращата страна не може да въздейства по никакъв начин [2], [8].

Наред с тях случайните и неопределените неконтролируеми фактори също не подлежат на никакво въздействие от страна на опериращата страна - нещо повече, те приемат стойности, които не са известни на изследователя на операциите, а това усложнява още повече задачата му. Случайните фактори са известни на изследователя с тяхната функция на разпределение. Изследователят знае значително по-малко за неопределените неконтролируеми фактори. Направеното описание на неконтролируемите фактори се прави от гледна точка на изследователя на операциите. Възможно е по време или непосредствено преди операцията опериращата страна да разполага с допълнителна информация - тогава е възможно да отпадне дори цялата неопределеност. Развитието на операцията може да се опише с множество от фазови променливи ξ_1 (t), ξ_2(t), … $\xi_к$ (t), които зависят от времето. Съответствието на развитието на операцията на поставената цел в математическите модели се характеризира с критерий за ефективност *W*. Критерият за ефективност е функция на фазовите променливи, стратегиите и неконтролируемите фактори, които от своя страна също могат да бъдат функции от времето. В математическите модели целта на операцията се изявява с изискването за екстремум (максимум или минимум) на критерия за ефективност. Изследователят на операциите се занимава с критерия за ефективност при изучаване на математическия модел. Изборът на целта и съответно на критерия за ефективност е в прерогативите на опериращата страна.

Не съществуват универсални методи за съставяне на математически модели. Във всеки конкретен случай моделът се избира съобразно вида на операцията и целта, която е присъща на разглежданата операция. Математическият модел трябва да отразява най-съществените страни на операцията, да съдържа всички съществени фактори, от които зависи протичането на операцията. Изследователят винаги е изправен пред две опасности: или да състави модел, който е подробен и отразява повече показатели на операцията, но е трудно решим или въобще не е решим, или да построи много по-общ и груб модел, който също не удовлетворява изследователя.

Счита се и то с пълно основание, че съставянето на математически модел е изкуство, което се усвоява постепенно в процеса на многогодишни изследвания. В специализираната литература по математическо моделиране се срещат различни класификации. Общоприето е в повечето от съществуващите класификации моделите да се делят на динамични и статични. Динамичните модели изучават явленията в развитие като функция на времето и по-точно описват реалността. В много случаи е достатъчно да се разгледа статичният модел. В този случай стратегията и действието са неконтролируеми фактори и се разглеждат като единичен акт, фазовите координати не се вземат под внимание и критерият за ефективност се разглежда като функция само на стратегиите и неконтролируемите фактори, т.е.:

$$W = F(x,y)$$

Много често изучаването на една операция започва с построяването и изучаването на статичния й модел. Понякога дори в този случай не е възможно да се представи в явен вид критерият за ефективност като функция на стратегиите и неконтролируемите фактори [3], [6], [9].

В общия случай стратегията *x* при статичните модели е функция на случайните неопределени неконтролируеми фактори y, понеже други неизвестни параметри при тези

модели не се разглеждат. Прието е тази зависимост x (y) да се означава с x^*. Множеството

от стойности, които приема $\tilde{x}$, се означава с *X* и зависи от вектора на активните средства. В най-общия случай стратегията е изображение на множеството на възможните стойности на неконтролируемите фактори *Y* в множеството *X*. Множеството на стратегиите $\tilde{x}$, определени от активните средства и информираността на оперираща срана, се нарича пространство от стратегии и се означава с $\bar{X}$ /математическо очакване/. Логически е възможно да се допусне, че всички стратегии, които не зависят от допълнителна информация за неконтролируемите фактори, също принадлежат на $\bar{X}$. Множеството на такива стратегии-константи съвпада с множеството на възможните стойности X и затова те се означават с x. Лесно се вижда, че когато оперираща страна изключва възможността за допълнителна информация, пространството от стратегии съвпада с множеството X. Това множество X е възможно най-бедното на стратегии множество. И така, при статичния модел критерият за ефективност W е функция на $\tilde{x}$ и y, т.е.

Статичната форма на модела *W* на операцията се използва за получаване на най-общи резултати и изводи.

Примери:

Пример 1. Оператор на определена машина следи за нейната неизправност. На базата на своя опит и наблюдения операторът има основание да смята, че машината се повреждa с вероятност 0,1 и е изправна с вероятност 0,9. Операторът трябва да реши дали да замени машината с друга, чиято стойност е 10 парични единици, а загубата от неотстранената неизправност е 100 парични единици, с оглед минимизация на загубите. В случая са налице две възможни стратегии: x_1 - да се замени машината с нова, и x_2 - да не се заменя машината с нова. Състоянието на машината е случаен неконтролируем фактор с две стойности: y_1, - изправен, и y_2 - неизправен. Критерият за ефективност може се представя по следния начин:

$$W = \begin{matrix} & y_1 & y_2 \\ x_1 & 10 & 10 \\ x_2 & 0 & 110 \end{matrix}$$

Пример 2. Избор на асортимента от стоки.

Да предположим, че е налице *a* количество на суровина (активни средства), от която може да се произведат *n* различни вида взаимно незаменяеми стоки. От една единица суровина се произвеждат q_i единици стока от i-тия вид. Предполагаме, че е известно общото количество стока *b*, която се търси на пазара, и минималните оценки $c_i, i = \overline{1,n}$ на търсената стока по видове i, при което:

$$\sum_{i=1}^{n} c_i < b$$

Стратегия на оперираща страна (производител или търговец) е векторът x = (x_1, x_2 ,..., x_n), x_i - количеството суровина, което се използва за производството на i-тия вид стока. Пространството от стратегии *X* може да се представи по следния начин:

$$X = \left\{ x \mid x_i \geq 0, i = \overline{1,n}, \sum_{i=1}^{n} x_i = a \right\}$$

Неконтролируем фактор е векторът y = (y_1, y_2, ..., y_n), от всички видове стока, която се търси. Лесно се вижда, че y е неопределен неконтролируем фактор с област на възможните стойности:

$$Y = \left\{ y \mid y_i \geq c_i, i = \overline{1,n}, \sum_{i=1}^{n} y_i = b \right\}$$

За цел на операцията избираме максимално възможно удовлетворяване на търсенето или минимално възможно неудовлетворяване на търсенето на всички видове стока. Така стигаме до критерия за ефективност:

$$W = \sum_{i=1}^{n} \min[q_i x_i - y_i, 0]$$

В случая критерият W е равен на сбора от неудовлетвореното търсене и е по-малък или равен на нула. Когато предложението $q_i x_i$ превишава търсенето y_i приемаме, че е налице удовлетворение на търсенето.

ЛИТЕРАТУРА:

[1] Ангелов Д., Желязкова Д. Стопанска логистика Варна, Наука и икономика, 2007

[2] Антон Антонов, "Методы симуляции в логистике". 10th International Conference on Bionics and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, Liepaya, 2014, ISBN 978-9934-10-573-9, стр. 138 - 142

[3] Кирова, Антоанета – Управление на транспорта в логистиката, Университетско издателство “Стопанство”, 2003

[4] Atanasov V., Ivanova, A., Student modelling in a web-based platform for learning games composing , Proceedings of the 13th International Scientific Conference "eLearning and Software for Education, Buchares, Romania April 27 - 28, 2017.

[5] Anton Antonov,Simulation software for modeling the flow of material flows. Journal Scientific And Applied Research, лицензиран в EBSCO , USA, Vol. 14, 2018г., ISSN 1314-6289

[6] Dybskaya, V.V. i dr., 2008. Logistika (Polnyy kurs MBA), Moskva

[7] Philip Oling, Dzheyn Tindal, Корпоративна рентабилност и логистика, Delfinpres Burgas, 2007

[8] Spath, D. and Weisbecker, A., Potenziale der Mensch-Technik Interaktion fur die effiziente und vemetzte Produktion von Morgen, Stuttgar, 2013

[9] Tzvetkova, G., Petrova, D., Hristov, H., Cheremensky, A. Identification of Linear Parameters in Dynamical Systems. Journal of Theoretical and Applied Mechanics, vol. 32 (2002).

[10] Vassileva, P., Petrova, D., Hristov, H., Cheremensky, A. Control Design in One Non-Orthogonal Attitude Problem. Journal of Theoretical and Applied Mechanics, vol. 32 (2002).

Име на автор(ите): Стефан Маринов Казаков
Месторабота: ШУ „Епископ Константин Преславски“
E-mail: kazakov@shu.bg

APPROACHES AND PRINCIPLES FOR CREATING INFORMATION SYSTEMS FOR LOGISTICS MANAGEMENT

STEFAN M. KAZAKOV

ABSTRACT: *The formation of an information system is a complex and multifaceted process in which the achievements of modern information technology, the latest computer systems are used, which makes possible the successful management of production processes based on the application of adequate information technology, methods and forms of information provision. the logistics system as a whole.*

KEYWORDS: *logistic, information, communication, management, process.*

ПОДХОДИ И ПРИНЦИПИ ЗА ПОСТРОЯВАНЕ НА ИНФОРМАЦИОННИ СИСТЕМИ ЗА ЛОГИСТИЧНО УПРАВЛЕНИЕ

СТЕФАН М. КАЗАКОВ

АБСТРАКТ: *Формирането на информационна система е сложен и многопланов процес, в който се използват достиженията на съвременната информационна технология, най-новите компютърни системи, което прави възможно успешното ръководство на производствените процеси на основата на прилагането на адекватна информационна техника, методи и форми на информационно осигуряване на логистичната система като цяло.*

1. Подходи.

Един от подходите за създаване модел на информационните потоци в производството е извършването на анализ на съществуващата система за управление. В съответствие с принципите на системния подход всяка система отначало трябва да се изследва във взаимоотношенията й с външната среда, а вече след това вътре в структурата си. Този принцип за последователното придвижване по етапите на създаване на системата трябва да се съблюдава и при проектирането на логистичните информационни системи [3], [7]. От позициите на системния подход към процесите на логистиката се различават три нива (фиг.4).

Първо ниво – работното място, на което се осъществява логистичната операция с материалния поток, т.е. придвижва се, разтоварва се, опакова се и т.н. товарната единица, детайлът или някакъв друг елемент на материалния поток.

Второ ниво – участъкът, цехът, складът, където протичат процесите на транспортиране на товарите, разполагат се работните места.

Трето ниво – системата за транспортиране и преместване като цяло, обхващаща веригата от събития, за начало на която може да се приеме моментът на разтоварване на суровините от доставчика, а за край – постъпването на готовите изделия при крайните потребители.

Фиг. 4. Нива на логистичните процеси от позициите на системния подход

Структурният модел трябва да съдържа два основни елемента, а именно производствените мощности и средствата за организация на материалния поток. Комбинирайки тези елементи, изследователите и системните организатори разделят цялата структура на предприятието на буферна и технологична части. При това се обхващат всички видове дейност – от получаването на суровините до предаването на готовата продукция на купувача. Основният критерий, отличаващ буферната от технологичната зона, е съсредоточен във въпроса: предметът на труда в стационарно състояние ли се намира или е приведен в движение? Получавайки отговор на този въпрос, по-нататък се определят данните, които трябва да бъдат събрани, обработени и предадени за осигуряване оптимално управление на материалния поток. Определените по този начин групи от предавани данни трябва да включват в себе си следните девет информационни елемента, които, както се счита, създават база за информационен контрол на цялата структура на материално-техническото снабдяване:

- тип на предмета на снабдяване;
- количество или обем на предмета на снабдяване;
- произход на този предмет;
- неговото местоположение (разполагане);
- време за пристигане в пункта за разполагане;
- време за отправяне от пункта за разполагане;
- система за транспортиране;
- време за транспортиране;
- резервиране.

Изброените групи от данни се съставят за всички места за разполагане и за всеки превозван обект. За тази цел се установяват пунктове за отчитане и предаване на информация във всички места за разполагане. Като правило, такива пунктове се препоръча да се организират на границата между буферните и технологичните секции на производството [1], [2], [10].

Заключителният етап от построяването на информационен модел на системата за материално-техническо снабдяване е свързан с разпределението на получените данни по две компютърни системи с различни области на функциониране. Едната система е свързана с поръчките за транспортиране и контролира потока от материали и осъществява управлението му, а другата непосредствено управлява производството и следи за заделените количества материали, нивото на които се определя от изискванията на производствения процес. В редица случаи двете системи се обединяват в една. В който и да е вариант информацията започва да се обработва веднага след постъпването на

производствена поръчка, също както се извършва и регистрация на материалите, които вече са превозени с помощта на транспортната система.

С други думи, в съответствие с концепцията на логистиката информационните системи, отнасящи се към различните групи, се интегрират в единна информационна система. Различават се вертикална и хоризонтална интеграция [5], [8].

За вертикална интеграция се смята връзката между плановата, диспозитивната и изпълнителната системи, осъществявана посредством вертикалните информационни потоци.

За хоризонтална интеграция се смята връзката между отделните комплекси от задачи в диспозитивните и изпълнителните системи, осъществявана посредством хоризонталните информационни потоци.

Като цяло преимуществата на интегрираните информационни системи се заключават в следното:

• нараства скоростта на обмена на информация;

• намалява количеството на грешките в отчетността;

• намалява обема на непроизводителната, "книжната" работа;

• съвместяват се разпръснатите информационни блокове.

В литературата се посочва и един друг аспект на подхода за създаване на логистични информационни системи – като процес, включващ стратегическо планиране на системите, съчетан с така нареченото "ситуационно действие".

В стратегическото планиране на информационната система се включват следните стъпки:

• определяне на подразделенията на предприятието, които ще бъдат включени в интегрираната информационна система (с отчитане на перспективите);

• грубо проектиране на функционалните области на информационната система и съотношенията между тях;

• определяне на важните за работата на предприятието обекти (заявители, доставчици на материалите, детайлите и др.) и изобразяването им в информационната система (това е най-сложната задача на стратегическото планиране, тясно свързана с предидущата стъпка);

• определяне на възможностите за използване на функционалните области на системата в различните подразделения на предприятието и оценка на очаквания ефект;

• установяване на правила за архитектурата и техническата реализация на подсистемите и съединяващите звена, създавани със собствени сили;

• установяване на общи, независими от функциите, правила и формати за предаване на данните между функционалните области на информационната система;

• установяване на параметри за изчислителната техника (апаратното оборудване, операционната система, системата за управление на данните, йерархичните нива на ЕИМ, техническите методи за предаване);

• разработване на проект за реализация (приоритети, срокове и т.н.).

Стратегическият общ план се създава в течение на няколко месеца. Необходима е ежегодната му актуализация с отчитане на новия опит при реализацията на отделните проекти, измененията в пазарната среда и по-нататъшното развитие на информационната техника.

За създаването на стратегическия общ план се препоръчва образуване на малобройна група от специалисти по информатика и сътрудници от подразделенията, които ще използват системата. Решаваща предпоставка за успешна работа на такава група се явява

поддръжката от ръководството на предприятието, тъй като то формулира целите и контролира хода на работите [4], [6], [9].

Ситуационото действие означава бързо реагиране на външни събития (например, на изменения на пазара, технически новости, организационни или персонални изменения в предприятието). Решението се взема на основата на ситуацията в настоящия момент, то не зависи от дългосрочното планиране. Обаче в благоприятния случай проектът може така да се формулира, че той да покрива предвидената в стратегическия план функционална област, или в лошия случай – новият проект да се включи в общия план.

Ситуационото действие подразбира също и проверка за съвместимост на появилото се на пазара ново стандартно програмно осигуряване със стратегическия общ план и на приложимостта му без отчитане на предвидените в плана приоритети.

Стратегическото общо планиране на информационната система трябва да се комбинира със ситуационното действие, което ще позволи да се вземат решения за отделните проекти гъвкаво и с отчитане потребностите на отделните подразделения, но без възникване на изолирани, несъгласувани частни решения.

2. Принципи.

При построяването на логистични информационни системи е необходимо да се съблюдават определени принципи, а именно:

- изграждане на модулна структура на системите, както в апаратното оборудване, така и в програмното осигуряване;
- осигуряване на възможност за поетапно създаване на системата;
- точно определяне на местата за свързване (много важен принцип);
- осигуряване на гъвкавост на системата от гледна точка на специфичните условия и изисквания на конкретното й приложение;
- изграждане на системата с отчитане изискванията на ползвателя за осъществяване на диалога “човек-машина”.

Принцип за използване на апаратни и програмни модули. Под апаратен модул се разбира унифициран функционален възел радиоелектронна апаратура, изпълнен във вид на самостоятелно изделие. Като модул на програмното осигуряване може да се счита унифицирания, в определена степен самостоятелен програмен елемент, изпълняващ определена функция в общото програмно осигуряване. Съблюдаването на принципа за използване на апаратни и програмни модули позволява да се:

• осигури съвместимост на изчислителната техника и на програмното осигуряване на различните нива на управлението;
• повиши ефективността на функциониране на логистичните информационни системи;
• понижи стойността им;
• ускори тяхното построяване.

Принцип за осигуряване на възможност за поетапно създаване на системата. Логистичните информационни системи, както и другите автоматизирани системи за управление, са постоянно развиващи се системи. Това означава, че при проектирането им е необходимо да се предвидят възможности за постоянно увеличаване броя на обектите за автоматизация и за разширяване състава на реализираните от информационната система функции и на количеството на решаваните задачи. При това следва да се има предвид, че определянето на етапите на създаване на системата, т.е. изборът на първостепенните задачи,

оказва голямо влияние на по-нататъшното развитие на логистичната информационна система и на ефективността на функционирането й.

Принцип за точното установяване на местата на свързване. В местата на свързване материалният и информационният поток преминава през границите на правомощията и отговорностите на отделните подразделения на предприятието или през границите на самостоятелните организации. Осигуряването на плавно преодоляване на местата на свързване е една от важните задачи на логистиката.

Заключение:

При построяването на логистичните информационни системи е необходимо да се съблюдават определени принципи, с което се осигурява ефективното им функциониране с отчитане развитието на изчислителната техника, изискванията на ползвателите им и конкретните условия на експлоатацията им.

ЛИТЕРАТУРА:

[1] Ангелов Д., Желязкова Д. Стопанска логистика Варна, Наука и икономика, 2007
[2] Антон Антонов, "Методы симуляции в логистике". 10th International Conference on Bionics and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, Liepaya, 2014, ISBN 978-9934-10-573-9, стр. 138 - 142
[3] Кирова, Антоанета – Управление на транспорта в логистиката, Университетско издателство “Стопанство”, 2003
[4] Г. Георгиев, А. Антонов, Интелигентни системи в автомобилния транспорт. Международна научно-практическа конференция „Устойчиво Развитие -2019”, 04 - 09.06.2019г. Варна, Година IX Брой 3/2019, ISSN 1314-4138 (print), ISSN 2367-5454 (online).
[5] Atanasov V., Ivanova, A., Student modelling in a web-based platform for learning games composing , Proceedings of the 13th International Scientific Conference "eLearning and Software for Education, Buchares, Romania April 27 - 28, 2017.
[6] Transporten entsiklopedichen rechnik, katedra “Ikonomika na transporta”, 1992
[7] Материали на ОСЖД, 2000-2005
[8] Tzvetkova, G., Petrova, D., Hristov, H., Cheremensky, A. Identification of Linear Parameters in Dynamical Systems. Journal of Theoretical and Applied Mechanics, vol. 32 (2002).
[9] Vassileva, P., Petrova, D., Hristov, H., Cheremensky, A. Control Design in One Non-Orthogonal Attitude Problem. Journal of Theoretical and Applied Mechanics, vol. 32 (2002).
[10] https://дигиталнаиндустрия.bg/

Име на автора: Стефан Маринов Казаков
Месторабота: ШУ „Епископ Константин Преславски“
E-mail: kazakov@shu.bg

PURPOSE AND CLASSIFICATION OF LOGISTICS INFORMATION SYSTEMS

STEFAN M. KAZAKOV

ABSTRACT: *The new tasks that arise before the organizers and production managers in the field of practical implementation of logistics principles, lead them to the need to create information systems that would allow the collection, organization and transmission of information in accordance with the objectives.*

KEYWORDS: *logistic, information, system, classification.*

ПРЕДНАЗНАЧЕНИЕ И КЛАСИФИКАЦИЯ НА ЛОГИСТИЧНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ

СТЕФАН М. КАЗАКОВ

АБСТРАКТ: *Новите задачи, които възникват пред организаторите и ръководителите на производството в областта на практическата реализация на логистичните принципи, ги водят към необходимостта от създаване на информационни системи, които биха позволили да се събира, организира и пренася информация в съответствие с поставените цели.*

1. Въведение

При традиционната и вече отиваща на втори план в развитите страни концепция за организация на материално-техническото снабдяване функциите на снабдяването (закупуването) винаги са били отделени от функциите на производството, складирането, маркетинга и продажбите. Те са се подчинявали на различни структури за управление (съответно търговска, производствена и за реализиране на продукцията) и са били слабо свързани помежду си (такава връзка се открива, и то епизодично, само на ниво главно управление на фирмата или предприятието). Това води до дълбоко разделение на задачите на посочените служби. Като следствие на такава организация се явява положението, когато задачите за управление на транспорта, складирането и материалните потоци се решават непълно, тъй като се намират в компетенциите на конкретни подразделения, които в рамките на крупните предприятия в по-голяма степен се конкурират помежду си за фондове и място в йерархията отколкото да се подчиняват на единна система от ценности и цели. Това се вижда от анализа на дейността в производството, което се стреми да използва собственото си складово стопанство със съответните резервни запаси и да противостои на непрекъснатия натиск на пазарната система върху производството. Задачите на реализацията на продукцията водят до необходимостта от ориентация към потребителите, а следователно, степента на готовност за доставки на продукцията на пазара се превръща в критерий за оценка ефективността на управлението. Счита се, че такава система за организация може да възникне и да работи в условията на пазарна икономика само в случаите, когато сложността на задачите за снабдяване и транспортиране не е висока или когато разходите, свързани с решаването на тези задачи, са относително ниски, а влиянието на услугите, предоставяни от системата за снабдяване, складиране и транспортиране, е сравнително малко. Слабата взаимна връзка на отделните сфери на дейност при

неизбежните грешки при съгласуването им води до завишаване на складовите запаси и оборотните фондове, диспропорция на производствените мощности, непълнота на изходната информация при вземането на алтернативни решения от типа "да произвеждам или да купувам", а също към неадекватно натоварване на отделните производствени линии, т.е. необходимо е обединение на всички елементи от производствено-разпределителната верига. Инструмент за подобно обединение се явяват информационните логистични системи, които осигуряват в информационно отношение всички логистични процеси, започвайки със закупуването на суровините и материалите и завършвайки с реализацията на готовата продукция. Това е така защото потоците от информация се явяват онези свързващи нишки, на които се "нанизват" всички елементи на логистичната система.

Преди да бъдат разгледани въпросите, отнасящи се до класификацията и структурирането на автоматизираните информационни системи в логистиката, е целесъобразно да бъдат изяснени някои основни понятия от областта на информационното осигуряване, и в частност, в сферата на информационната логистика.

Под понятието **"логистична информация'** е прието да се разбират "съществуващите и циркулиращите в различните обекти на икономическата (производствено-разпределителната) дейност данни (сведения) за производството, разпределението и потреблението на стоки и услуги, които имат съществено значение за управлението на тази дейност". Тя се дели на официална (генерира се чрез стандартни процедури, т.е. данните, от които тя се получава, са числови и съществуват върху формални документи) и неофициална (субективна, предавана чрез разговори и включваща мнения, предложения, слухове; най-вероятно е тя да има качествен характер; използва се при вземане на решения, но е малко вероятно да служи за обосновката им).

Понятието "информационната логистика" се дефинира като "функционална област на логистиката, която се занимава с изследването на информационните потоци в логистиката и използването им за логистично управление".

2. Същност и предназначение на логистичните информационни системи.

Под понятието "логистична информационна система" се разбира "структура, включваща персонал, оборудване и технологии, които са обединени от информационния поток, използван от логистичния мениджмънт за планиране, регулиране, контрол и анализ на функционирането на логистичната система". С други думи, съвкупността от организирани, преобразувани и взаимно свързани по определен начин потоци от информация образуват вътре в самата логистична система много характерна подсистема, която поради спецификата и завършеността си често се нарича информационна подсистема (система) на логистичната система.

Известно е, че всяка логистична система се състои от редица структури, които могат да се представят във вид на хоризонтални функционални подсистеми в областта на закупуването, производството и реализацията на готовата продукция. На свой ред, в рамките на всяка подсистема има структури от функционален характер – складово стопанство, транспортиране, производство, услуги, осигуряване и обработка на информацията. Всеки от тези елементи неизбежно присъства във всяко производство (производствено-разпределителна верига), а логистиката ги обединява в система с единни цели и задачи, които се намират в областта на минимизацията на разходите на цялото производство (производствено-разпределителна верига), а не на отделно взетия негов елемент.

Информационната система се явява онзи съществен компонент на логистичната структура, който я свързва в едно цяло и служи за координиране на доставките, производството и продажбите на готова продукция.

Информационната логистика се вписва в рамките на компютърните технологии. Компютърната система за предаване и съхранение на информация носи двойна полза. Първо, такава система подобрява управлението на все по-усложняващото се материално-техническо снабдяване. За компактните и високо организираните системи за производство, такива, като синхронно производство и доставки "точно навреме", управлението на движението на постъпващите материали става все по-важно. Второ, благодарение използването на информационната логистика при обмена на данни за снабдяването, се повишава ефективността на управлението на запасите. Моменталното получаване на данни за движението на стоките дава увереност за своевременното им доставяне и като че ли позволява да се заменят реалните запаси с информационни потоци.

Обменът на снабдителни данни, разпростиращ се върху мрежата от фирми-доставчици и транспортни компании, позволява на производителя да намали разходите, свързани с осигуряване дейността на пълната логистична верига. Повишавайки ефективността й, фирмата-производител получава осезателна икономия. Тя фактически се дели в определени пропорции между трите страни: производител, доставчик и транспортна компания, компенсирайки разходите за създаване и поддържане на съвременни информационни системи и създавайки допълнителна печалба от използването им. Получаването на ефект от информационната логистика стимулира всички участници в логистичния процес да поддържат достигнатото ниво на този процес, а също да влагат нови средства за оптимизацията му. Страничен продукт на системата за координация на доставките се явява постоянно попълваната база от данни, помагаща да се оцени ефективността на работата на логистичните служби.

По оценки на специалистите, на логистичните информационни системи се падат 10-20% от всички логистични разходи. Цените на апаратното оборудване в света бързо се понижават, расте съотношението между производителността на ЕИМ и цената им. Преди няколко години съотношението между стойностите на апаратното оборудване и на програмното осигуряване беше около 1:3. Но относителната тежест на програмното осигуряване в това съотношение непрестанно расте, както поради увеличаването на мащаба и сложността на информационните системи, така и вследствие на поевтиняването на апаратното оборудване.

Информационната система, необходима за адекватно изпълнение функциите на логистиката, притежава всички характеристики, които превръщат обикновената съвкупност от информационни компоненти в завършена система, а именно:

1. Информационните потоци в логистиката имат свойството да взаимодействат един с друг, образувайки единно цяло, което по очевиден начин се разчленява на части. Те могат да са с различна физическа природа и форма (например, потоци от съставени и попълнени по определен начин документи и потоци от масиви от данни, преместващи се между компютрите по локални мрежи), бъдейки при това съвместими в информационно отношение.

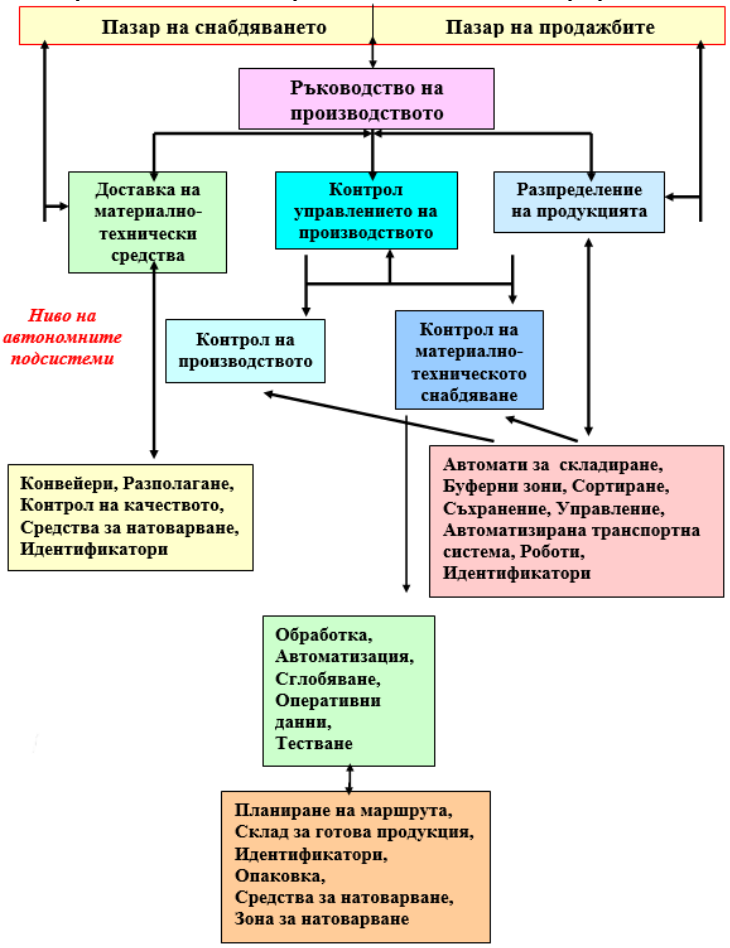
2. Между информационните компоненти (потоци) съществуват взаимни връзки от различно естество, в т.ч. и причинно-следствени. Взаимните връзки и взаимната зависимост между информационните компоненти (потоци) в информационната система са по-силни и по естествени, отколкото връзките на тези компоненти с външната среда.

Именно това разделя информационната система от близо разположените компоненти на външната среда.

3. Фактическото обединяване на информационните компоненти (потоци), притежаващи посочените по-горе системообразуващи предпоставки, се извършва в резултат на работата по обединяването и организацията им. В резултат се създава една или друга конкретна информационна структура. Това предполага, че се подреждат взаимните връзки и йерархията на подчиненост на компонентите на тази структура.

4. Информационните системи в логистиката трябва да притежават свойството интегративност. В дадения случай това означава, че информационната система може да осигури такива възможности за логистично управление, каквито този или онзи отделно формиран поток (без отчитане на другите потоци и без взаимодействието с тях) не може да осигури.

На фиг.1 е представена най-типичната информационна логистична система, функционираща в едно отделно взето производство. Тя има редица особености. **Първо,** тя е всепроникваща – за нея няма закрити зони; от нейните канали и датчици са пронизани всички нива по хоризонталата и вертикалата. **Второ,** тя е строго йерархична, управляващите нива са точно очертани и носят отговорност за поверените им функции. **Трето,** функциите за външни връзки са делегирани само на определено ниво от йерархията.



Фиг.1. Пример за организация на информационна логистична мрежа в производството

На върха на пирамидата на информационната мрежа на предприятието се намира генералното му ръководство с функциите за мениджмънт (планиране и контрол).

Функционалният контрол се осъществява на следващото ниво и включва доставката на предметите за снабдяване, управлението на предприятието, управлението на разпределението. Основните контролируеми параметри са времето за обработка, обслужването на доставките, запасите, производителността. На ниската степен са разположени системите, непосредствено влизащи в контакт с работните места и функционално управляващи производството и материално-техническото снабдяване. Тук контролируеми параметри са производствените мощности, количеството и маршрутите за преминаване на продукцията, сроковете за производство. Отделно се откроява нивото на автономните подсистеми, състоящи се от локални информационни мрежи. Локалната информационна мрежа, свързана с конвейера, събира и предава данни за: разположението на предметите за снабдяване; контрола на качеството им; състоянието на средствата за товарене; маркировката и идентификацията на продукцията и за постъпването й в склада. Тази мрежа предава данните непосредствено на второто ниво, отговарящо за доставянето на материално-техническите средства. Локалните информационни мрежи, разположени непосредствено на работните места, захранват с информация структурата за контрол на производството за темповете на сглобяването, резултатите от тестването и пр. А информацията за положението в буферните зони и в складовете се получава от структурата за контрол на материално-техническото снабдяване. Двете контролиращи системи активно си обменят информация на своето ниво. Накрая, локалната мрежа, събираща данни за обработката на готовата продукция и за превозването й до клиентите, ги предава в подразделенията, водещи разпределението на продукцията.

По такъв начин, сама по себе си, тя представлява един от най-важните елементи на производството, а в системите за материално-техническо снабдяване играе решаваща роля в повишаването на ефективността им. Този процес на интензификация на производството е обусловен както от кратките срокове за обработка на материалите при по-ниско ниво на запасите и нарастваща гъвкавост на производството, така и от високата “прозрачност” на всеки участък от предприятието.

Информационните системи в логистиката, както и всички системи с обратна връзка, освен със структурата си, се характеризират и с такива количествени показатели като величина на закъснение и степен на усилване.

Закъсненията при вземането на логистични решения в сравнение с постъпването на информацията, водеща до тези решения, могат да са различни по величина и да възникват на различни места на регулирания материален поток (фиг.2).

Обикновено закъсненията в производствено-разпределителната дейност съставляват величини от порядъка на седмица. Затова за измервателна единица при тях се приема седмицата. Така средно времето за транспортиране съставлява една седмица, закъснението при счетоводните операции – три седмици, пощенското закъснение – половин седмица, закъснението при търговците на едро и в различните видове разпределителни пунктове, също както и закъснението между отделните операции по време на производството, съставлява средно по една седмица. Накрая, времето между вземането на решение за изменения в производството и достигането на съответното значение на материалния поток на изхода на производственото подразделение съставлява средно шест седмици.

На понятието **степен** или **коефициент на усилване** на звеното от системата за автоматично регулиране в логистиката съответства набора от правила, модели и алгоритми, поставящи едни или други управляващи директиви в съответствие с измененията в информацията за хода на производствено-разпределителната дейност. Поведението на лицето или органа, вземащ решение, определяно от получената от него информация, може

да се представи като най-обикновена реакция на колебанията на материалния поток относно едно или между две нива. То може да се определя също и с дълга подробно разработена и формализована верига от изчисления. Във всички случаи една или друга роля играят интуицията, личните качества и талантът на лицето или лицата, вземащи решение. Тази роля може да се изменя от спомагателна до определяща.

Опирайки се на получаваната информация, лицето или органа, вземащи решение, трябва да осигурят качествено логистично управление, т.е. под въздействието на логистичното управление производствено-разпределителната система трябва да преминава от едно установено състояние определяно от условията на обкръжаващата икономическа среда в ново състояние, съответстващо на станалите в тази среда изменения. Този преход трябва да става със съблюдаването на изискваните показатели за качество.

Фиг.2. Видове закъснения в логистичните системи

В класическата теория за регулиране и управление такива показатели за качеството на развиващ се във времето преходен процес от старо установено значение към ново установило се такова са следните:

- време за протичане на преходния процес, определяно като време, необходимо за приближаване фактическото значение на регулируемия параметър към новото ниво на зададена малка величина;
- степен на колебание на преходния процес, който може да бъде монотонен или колебателен; в последния случай степента на колебание се определя с броя на колебанията на регулируемия параметър, извършвани до достигане на зададеното му приближение към новото значение;
- величина на пререгулирането, измервана с максималното превишаване от регулируемия параметър на новото му значение, което може да стане по време на преходния процес;
- интегрален показател за качеството, представляващ подинтегралната площ на кривата на преходния процес.

Преходните процеси могат да бъдат устойчиви и неустойчиви. Устойчивите преходни процеси рано или късно завършват и в системата възниква ново установилото се състояние. Неустойчивите преходни процеси са налице, когато изменението на външната икономическа среда извежда производствено-разпределителната система от равновесие и инициира в нея преходни процеси, които няма да завършат никога. Или с други думи, системата никога няма да се успокои и няма да заеме ново установило се състояние.

Такава загуба на устойчивост може да има, когато управляващите въздействия закъсняват по отношение на предизвикващите ги причини или ще са неадекватни на тях по величина – по-силни или по-слаби. Тогава такива въздействия вместо да компенсират произтичащите отклонения, могат още повече да ги засилват, което и ще доведе до нарастване размаха на колебанията в системата.

Очевидно е, че изискванията за устойчивост и качество на логистичното управление водят до определени изисквания към величините на закъснението и усилването, с които се характеризират информационните системи в логистиката.

Задачата за осигуряване на оперативно и адекватно реагиране на изменящите се условия за функциониране се решава понастоящем по два пътя.

Първият от тях е функционалният подход, който традиционно преобладаваше до неотдавна. При него всяко функционално подразделение създава своя собствена система за събиране, обработване и използване на информацията. При това то използва свои форми на документите и организация на документооборота, собствени архиви, канали за връзка, методи, средства и пунктове за събиране на данни. Такива информационни системи е прието да се наричат организационно-функционални. При такъв подход има дублиране на информацията, попълване на излишни документи, недостатъчна гъвкавост на управлението и, най-важното, отсъстват хоризонталните връзки между производителите и между функционалните подразделения. Вторият подход се отнася към структурните методи за осигуряване на актуална и адекватна информация. Той се заключава в *прехода от функционалния към системния подход.* Системният подход предвижда създаване на информационни системи, ориентирани към производствено-разпределителния процес като цяло. В резултат на такъв подход информационната система се обособява от системите за производство, снабдяване и пласмент, в такъв смисъл, че събирането, съхранението, преработката, търсенето и подаването на информация се извършва със свои, присъщи само на информационните процеси, методи и средства. При такава структура в информационните системи се организират хоризонтални връзки, унифицират се формите за представяне и технологията за обработка на информацията. Организираните по този принцип информационни системи е прието да се наричат **интегрирани.**

Използването на интегрирани информационни системи позволява да се осъществи централизация на всички работи по информационната технология в рамките на производствено-разпределителната система като единно цяло.

Освен това наличието на интегрирана информационна система позволява на участниците в производствено-разпределителната дейност да създават т.н. “синергичен портфейл”, който служи за отслабване на отрицателния синергичен ефект. Под **синергичен ефект** се разбира взаимното усилване на връзките между компонентите при техните съвместни (корпоративни) действия.

Положителен синергичен ефект има, когато своевременното изпълнение на задълженията от всички доставчици води не само до своевременно изпълнение на задълженията по доставяне на продукцията (която е резултат на общата работа на всички участници) на потребителя, но и до повишаване технологичната дисциплина и качеството на крайната продукция, а също и до снижаване нивото на необходимите запаси и намаляване на производствено-разпределителните разходи.

Отрицателният синергичен ефект се изразява, например, в това, че при неизпълнение на задълженията от два или повече доставчика, общите загуби, възникващи вследствие на срива на продажбите и загубата на клиенти, се оказват значително по-големи

от общата сума на не извършените доставки. За това способства лавинообразното нарастване на последващите загуби по цялата производствено-разпределителна верига.

3. Класификация на логистичните информационни системи.

Информационните системи в логистиката, независимо от конкретното им предназначение, по структурата си се изграждат по йерархичния принцип, обикновено на три нива (три ранга). В съответствие с това логистичните информационни системи се подразделят на три групи:

- **планови (планиращи);**
- **диспозитивни (диспечерски);**
- **изпълнителни (оперативни).**

Логистичните информационни системи, влизащи в различните групи, се отличават както по своите функционални, така и по осигуряващите си подсистеми.

Функционалните подсистеми се отличават по състава на решаваните задачи.

Осигуряващите подсистеми могат да се отличават по всичките си елементи, т.е. по техническото, информационното и математическото си осигуряване.

Ще се спрем по-подробно на спецификата на отделните видове информационни системи.

Плановите информационни системи се създават на административното ниво на управление и служат за вземане на дългосрочни решения със стратегически характер. Сред решаваните от тях задачи могат да бъдат следните:

- създаване и оптимизация на звената на логистичната верига;
- управление на условно-постоянните, т.е. на слабоизменящите се данни;
- планиране на производството;
- общо управление на запасите и др.

Диспозитивните информационни системи се създават на ниво управление на склада или цеха и служат за осигуряване на отрегулирана работа на логистичните системи. Тук могат да се решават следните задачи:

- детайлно управление на запасите (местата за складиране);
- разпореждане с вътрешноскладовия (или вътрешнозаводския) транспорт;
- подбор на товарите по пръчки и комплектоването им, отчет на отправяните товари и други задачи.

Изпълнителните информационни системи се създават на административното или оперативното ниво на управление. Обработката на информацията в тях се извършва с темп, определян от скоростта на постъпването ѝ в ЕИМ. Това е така наречения режим на работа в реален мащаб на времето, който позволява получаване на необходимата информация за движението на товарите в текущия момент от време и своевременно да се подават съответните административни и управляващи въздействия на обекта за управление. С тези системи могат да се решават разнообразни задачи, свързани с контрола на материалните потоци, оперативното управление на обслужването на производството, управлението на преместванията и други подобни.

Разгледаните по-горе особености на различните видове информационни системи са в разреза на функционалните им подсистеми. Но, както вече беше отбелязано, различия има и в осигуряващите подсистеми. Ще се спрем по-подробно на характерните особености на програмното осигуряване на плановите, диспозитивните и изпълнителните информационни системи.

Създаването на автоматизирани системи за управление на материалните потоци с много нива е свързано със значителни разходи, основно в областта на разработката на програмното осигуряване, което, от една страна, трябва да осигури многофункционалност на системата, и от друга – висока степен на интеграцията й. Във връзка с това при създаването на автоматизирани системи за управление в сферата на логистиката трябва да се изследва възможността за използване на сравнително евтино стандартно програмно осигуряване, с адаптирането му към местните условия.

Понастоящем се създават достатъчно съвършени пакети от програми. Но те са приложими не във всички видове информационни системи. Това зависи от нивото на стандартизация на решаваните при управлението на материалните потоци задачи.

Най-високо е нивото на стандартизация при решаването на задачи в плановите информационни системи, което позволява при тях с най-малки трудности да се адаптира стандартното програмно осигуряване. Възможностите за приспособяване на стандартния пакет програми при диспозитивните информационни системи са по-ниски. Това се дължи на следните причини:

- производственият процес в предприятията се формира исторически и трудно се поддава на съществени изменения в името на стандартизацията;
- структурата на обработваните данни съществено се различава при различните ползватели.

В изпълнителните информационни системи на оперативно ниво се използва, като правило, индивидуално програмно осигуряване.

Заключение:

Широкото навлизане на логистиката в сферата на икономиката в значителна степен се дължи на компютъризацията на управлението на материалните потоци. Способността на микропроцесорната техника да решава сложните въпроси на обработката на информацията позволява да се извършва анализ и взаимен обмен на големи обеми информация между различните участници в логистичния процес..

ЛИТЕРАТУРА:

[1] Ангелов Д., Желязкова Д. Стопанска логистика Варна, Наука и икономика, 2007
[2] Кирова, Антоанета – Управление на транспорта в логистиката, Университетско издателство “Стопанство”, 2003
[3] Антон Антонов, "Методы симуляции в логистике". 10th International Conference on Bionics and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, Liepaya, 2014, ISBN 978-9934-10-573-9, стр. 138 - 142
[4] Dzhon Gatorna, Основи на логистиката и дистрибуцията, Delfinpres, 1996
[5] Philip Oling, Dzheyn Tindal, Корпоративна рентабилност и логистика, Delfinpres Burgas, 2007
[6] https://www.sisecamkariyerim.com

Име на автор(ите): Стефан Маринов Казаков
Месторабота: ШУ „Епископ Константин Преславски“
E-mail: kazakov@shu.bg

NOTES ON THE DESIGN OF THE INFORMATION SYSTEM IN THE MANAGEMENT OF AN ORGANIZATION

PLAMEN B. DYANKOV, SVETLOZAR P. STOYANOV

ABSTRACT: *A proposal (concept) has been developed for the construction of a new information system for the management of the organization or for the improvement of the existing one. It is the result of the findings and conclusions of a survey and analysis of the existing information system for the management of the organization. The concept itself is the basis for its design. It is essential to clarify the structure of factual decisions at different levels of governance, as well as the scale, period of action and level of governance at which they are taken*

KEYWORDS: *Proposal, Design, Factual solutions.*

БЕЛЕЖКИ ЗА ПРОЕКТИРАНЕТО НА ИНФОРМАЦИОННАТА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ОРГАНИЗАЦИЯТА

ПЛАМЕН Б. ДЯНКОВ, СВЕТЛОЗАР П. СТОЯНОВ

ABSTRACT: *Базис за изграждането на нова информационна система за управление на организацията или за усъвършенстването на съществуващата е разработено предложение (концепция). То е резултат от констатациите и изводите от проведено проучване и анализ на съществуващата информационна система за управление на организацията. Самата концепция е основата за нейното проектиране. При него същественото е да бъде изяснена структурата на фактическите решения на различните нива на управленска дейност, а също мащабът, периодът на действие и нивото на управление, на което се взимат.*

Концепцията (разработеното предложение) е базис за изграждането или за усъвършенстването на информационната система за управление на организацията (ИСУО). Резултат е от констатациите и изводите от проведено проучване и анализ на съществуващата ИСУО, а самата концепция е основата за нейното проектиране [2, с. 20; 3, с. 70 – 71].

Същественото при проектирането на ИСУО е да бъде изяснена структурата на фактическите решения на различните нива на управленска дейност, а мащабът, периодът на действие и нивото на управление, на което се взимат, предполагат, че могат да бъдат разделени на:

- стратегически – определят конфигурацията на системата на организацията. Те са дългосрочни, т.е. за период от три до не повече от 5 години. Съдържат висок риск и неопределеност. Установяват отношенията на системата на организацията с външната среда. Взимат се от висшето ръководство. Задължителни са. Определят развитието на системата на организацията (инвестирането, разширяването на дейността, навлизането на нови пазари, внедрителската дейност и др.) [16], [17]. Всички останали решения следва да са съобразени с тях;

- тактически – свързани са с планирането и контрола. Те са средносрочни, т.е. за период от една до 3 години. Взимат се от средния управленски персонал, който е и координатор, за своевременно подобряване на резултатите от дейността. Установяват

структурата на системата на организацията. Конкретизират стратегическите решения и осигуряват връзката им с решенията на низовия управленски персонал;

- оперативни – свързани са с текущото изпълнение. Те са краткосрочни, т.е. обхващат дни, седмици, месеци до по-малко от година. Взимат се бързо от низовия управленски персонал, прилагат се веднага, най-динамични са, като са в определени рамки. Оперативни решения се взимат и от висшето ръководство, и от ръководителите на средно ниво [1, с. 98 (бел. 9), с. 99, с. 131, с. 145; 4, с. 49; 5, с. 112 – 113; 6, с. 293; 7, с. 186 – 187; 9, с. 24 – 25; 10, с. 67 – 68; 11, с. 112; 12, с. 47; 13, с. 73 – 74, с. 99; 14, с. 69 – 72, с. 99; 15, с. 18].

По отношение на структурата на фактическите решения на различните нива на управленска дейност, същите могат да бъдат разделени на:

- структурирани – подчиняват се на точно определени правила. Процедурата за взимане на такова решение би могла да се представи като логическа последователност от определени стъпки на изпълнение (блок схема). От своя страна използваната информация е точна и еднозначна;

- неструктурирани – не се подчиняват на ясни правила. Тук не могат да се ползват разработени процедури. Решенията от този тип се основават на интуицията и опита, а използваната информация е неопределена и недостатъчно точна [2, с. 20; 10, с. 68].

Проектирането на ИСУО включва цялостна характеристика на процеса на обработка на информацията, т.е. от възникването на данните до използването на регулиращата информация за взимането на фактически решения на съответното ниво на управленска дейност:

- цел и предназначение – описва се целта, която трябва да се постигне с автоматизирането на съответната дейност (нови показатели, по-голяма аналитичност на съществуващите, своевременност и точност на данните, вариантност и рационалност на решенията и др.);

- обхват и функционална структура – какви информационни задачи и подзадачи включва, връзките между тях, взаимодействие на входа и изхода с други подсистеми (съществуващи или предвидени за изграждане);

- схема – описание на информационните процеси, технологичната последователност на операциите по регистрирането, обработката по определени алгоритми и движението на информацията по структурни звена;

- проектиране на изхода – резултативните документи, които съдържат обработената информация – обхват и структура, носител – на печат, монитор, предназначение, ползватели и др.;

- проектиране на входните документи – обхват и структура, начин на създаване, начин на въвеждане, контрол и др.;

- кодове и класификатори – използвани шифро-кодови системи, структура на кодовете, номенклатура и класификатори и др.;

- проектиране на информационната база – описание на файловете [файлът е широко понятие и включва освен понятието информационен масив (информационна съвкупност, която описва елементите на определени производствено-стопански или други обекти, явления или процеси, записани върху традиционни или машинни носители) и понятието програма (съвкупност от записи)], записите (записът е информационна структура, позволяваща обединяването на фиксиран брой разнородни елементи, т.е. реквизити и характеристики, наречени полета, съдържащи инструкции за обработка на данните) и елементите (елементът, т.е. полето, е най-малката информационна единица, участваща в процеса на обработка на данните, която може да се представи във вид на текст или число)

в тях; за всеки информационен масив се дава: наименование, предназначение, метод на организация, типове записи, дължина и др.; за всеки запис се дава: идентификация, ключове, структура, елементи, дължина и др.; за всеки елемент се дава: име, дължина, тип на данните (букви, букви и цифри, цифри) и др.;

- описание на програмното осигуряване – обосновава се използването на определени операционни системи и програмни продукти;

- описание на техническото осигуряване – дава се комплексът от технически средства (компютри, печатащи устройства, средства за мрежи и комуникации), които са необходими за обезпечаване на функционирането на подсистемата при определения обхват и програмно осигуряване;

- описание на организационното осигуряване – функции и задачи на отделните звена и изпълнители при експлоатацията на подсистемата, контрол и защита на данните, срокове и графици за обработките, задължения на администратора на подсистемата за общата база данни (БД) [2, с. 21 – 22, с. 23, с. 24; 12, с. 48].

От управленска гледна точка ИСУО е средство, обхващащо всички форми на събиране, съхраняване, извличане, обработка и разпространение на информация. Множество е от взаимосвързани компоненти, доставящо информационни услуги и подпомагащо процеса на взимане на решения, координацията и контрола в организацията [8, с. 12].

По отношение на бизнеса (стопанската организация) ИСУО би било добре да се разглежда като организационно и управленско решение, което използва информационни технологии (обхващат различните средства, необходими за функционирането на дадена система). Прилагането им изисква детайлно познаване на съответната организация, заедно с нейните основни характеристики: човешки ресурси, структура, оперативни процедури, политики и култура. В тази връзка съществено изискване към всяка ИСУО е да осигурява и поддържа интегриран информационен поток в рамките на дадената организация, за да може във всеки един времеви момент, всеки, който има необходимост, да получи необходимите му сведения [8, с. 13].

ЛИТЕРАТУРА:

[1] Асенов, А., Дилков, Ц., Емилова, И. Основи на управлението. Свищов, 2017, Академично издателство „Ценов”.

[2] „Глава 7. Информационната система и информационната база на фирмата”. – <http://fbm.uni-ruse.bg/d/ist/U-7-2002.pdf>, 1 – 32, 04.07.2020.

[3] Гочева-Илиева, С. Приложни информационни системи. Пловдив, 2015, Университетско издателство „Паисий Хилендарски”.

[4] Димитров, П. (ред.) и др. Логистични системи. Първо издание. София, 2010, Университетско издателство „Стопанство”.

[5] Кирильчук, С. (ред.) и др. Экономика предприятия. Практикум. Учебное пособие для СПО. Москва, 2019, Издательство „Юрайт”.

[6] Лукинский, В., Лукинский, В., Плетнева, Н. Логистика и управление цепями поставок. Учебник и практикум для СПО. Москва, 2018, Издательство „Юрайт”.

[7] Милчев, Г. Съвременни информационни системи и повишаване конкурентноспособността на малките и средните предприятия. – Списание „Управление и устойчиво развитие”, София, 2002, Том 6, Бр. 1 – 2, 186 – 191, Лесотехнически университет.

[8] Пенева, Ю. Информационни системи. София, 2014, Нов български университет – Департамент по информатика.

[9] Пенчева, И. Управленски умения. Съвети за мениджъри. Велико Търново, 2013, Издателство „Абагар”.

[10] Петков, А. Бизнес информационни технологии. Русе, 2015, Русенски университет „Ангел Кънчев”.

[11] Раковска, М., Драгомиров, Н., Луканов, К. Бизнес логистика. София, 2018, Издателски комплекс – УНСС.

[12] Славова, П. Информационните системи в управлението на бизнес организацията. – Списание „Управление и устойчиво развитие”, София, 2015, Том 52, Бр. 3, 45 – 50, Лесотехнически университет

[13] Станчева, А. Основи на управлението. Учебно помагало. Трето преработено и допълнено издание. Варна, 2006, Издателска къща СТЕНО.

[14] Тодоров, Ф. Проектиране на логистични системи. София, 2017, Издателски комплекс – УНСС.

[15] Markov, K. Problems of the strategic management and the strategic analysis. – International scientific refereed indexed online journal with impact factor “SocioBrains”, Bulgaria, Sofia, 2016, Issue 21, <http://sociobrains.com/bg/top/issues/issue-21%2C-may-2016/>, 16 – 29, Smart Ideas – Wise Decisions Ltd.

[16] Kodzheykova, V., Y. Yankova-Yordanova. Methodology for logistics system management in medium serial production. Journal scientific and applied research, USA, EBSCO, ISSN 1314-6289 (2019).

[17] Yankova-Yordanova, Y., V. Kodzheykova. Expert approach for analysing a logistics control system and quality management in the conditions of small and medium serial production. Journal scientific and applied research, USA, лицензиран в EBSCO, Volume 15, ISSN 1314-6289 (2019).

Имена на автора: доц. д.н. инж. Пламен Борисов Дянков
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Инженерна логистика“
E-mail: p.dqnkov@shu.bg
Имена на съавтора: ас. инж. Светлозар Панайотов Стоянов
Месторабота: Шуменски университет „Епископ Константин Преславски“, Факултет по технически науки, катедра „Инженерна логистика“
E-mail: s.p.stoyanov@shu.bg

A NEW LOOK AT THE CAPABILITIES OF THE HWK 109-509 SERIES ROCKET ENGINES

HRISTO A. HRISTOV, TSVETOSLAV S. TSANKOV

ABSTRACT: *The modern development of missile technology is based on the real technical development of missile technology in Germany before and during World War II. The main ideas and specific technical solutions were made in this period. In the present work, we will consider an interesting series of engines developed by Prof. Hlemut Walter and manufactured in his factory Walterwerke in Kiel, in which highly concentrated hydrogen dioxide is used as an oxidizer.*

KEYWORDS: *Hydrogen peroxide, Rocket engine.*

НОВ ПОГЛЕД КЪМ ВЪЗМОЖНОСТИТЕ НА РАКЕТНИТЕ ДВИГАТЕЛИ ОТ СЕРИЯТА HWK 109-509

ХРИСТО А. ХРИСТОВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Съвременното развитие на ракетната техника има като своя основа реалното техническо развитие на ракетната техника в Германия преди и по време на Втората световна война. Основните идеи и конкретни технически решения са направени в този период. В настоящата работа ще бъде разгледана една интересна серия двигатели, разработени от проф. Хлемут Валтер и произвеждани в неговата фабрика Walterwerke в град Kiel, в които като окислител е използван висококонцентриран водороден диоксид.*

Основни обозначения:

B-stoff	вещество B (състои се от 92% хидразин хидрат и 8% вода)
C-stoff	вещество C (състои се от 57% метилов спирт, 30% B-stoff и 13% вода)
Me.163	абревиатура на Месершмид, модел 163, вид немски самолети, популярни през 30 и 40 години на 20 век и през Втората световна война (ВСВ)
T-stoff	воден разтвор на 80% водороден диоксид

Въведение

В края на Втората световна война за Съюзниците е ясно, че германските учени са провели много подробни научни изследвания в областта на ракетите с течно гориво. В Германия през 1945 г. имало големи количества химически и машиностроителни заводи, както и много квалифицирани учени, инженери и техници. Било е решено, че след залавянето на този персонал и техните лаборатории, могат да бъдат създадени полезни технически решения на място, в самата Германия, използвайки вече готови съоръжения, спестявайки разходи и време за изграждане на подобни заводи във Великобритания и САЩ. Идеята е била да се разширят или завършат съществуващите проекти с техническия персонал преди съществуващите лаборатории и техния персонал да бъдат разформировани.

„Sanger Raketentechnisches Forschunginstitut“ Trauen е изпитателно съоръжение, построено от немците на ръба на Luneburg Heide. Това съоръжение е било отдалечено и със

значителна площ, позволяваща да бъдат изградени големи изпитателни стендове за течни горивни ракети, а отделните изпитвателни сгради били разпръснати за безопасност. То било добре оборудвано със стендове за изпитване на ракети, лаборатории и завод за течен кислород на място. Били доведени 82 заловени учени – ракетчици и химици, от Walterwerke, Пенемюнде и други места. Първоначално те са били събрани в Куксхафен, където съюзниците са управлявали Операция „Обратен огън“, сглобявайки и изстрелвайки ракети V2. Тези учени пристигат в Трауен в началото на 1946 г. и продължават експерименталната програма, докато (поне официално) цялата активна работа не спира на 16 юни 1946 г.

Специално във Великобритания се интересуват от разширяването на своите познания за:

- ракетите с течен кислород;
- развитието на горивните системите с азотна киселина;
- стабилността при работа на пероксидните горива;
- химията на катализаторите;
- възпламеняването на водородния диоксид и възможността за използването му за охлаждане.

Всичко това идва да покаже значението, което има развитието на ракетните двигатели с течно гориво в Германия и в частност серията 109-509. Интересът към тях не е намалял до наши дни.

Основни технически параметри

Двигателите от серия HWK 109-509 са бипропелантни, като използват за окислител 80% водороден диоксид (T-stoff) и като гориво известното C-stoff.

На основата на архивни исторически данни [4], [6], беше съставена таблица, в която може да се проследи развитието на техническите параметри на серията 109-509 течно горивните ракетни двигатели. Основните показатели са следните – модел, тяга, тегло, самолет (на който е монтиран и използван), бележки (табл. 1).

Таблица 1. Технически параметри

№	Модел	Тяга [кг сили]	Тегло [кг]	Самолет	Бележки
1.	RII.203	150 – 750	–	Me.163A	Агрегат, работещ по „Студен“ цикъл. Използващ T-stoff като монопропелант
2.	RII.211 (109-509.A-0)	150 – 1500	170	Me.163B	Прототип на агрегата A-1 „Hot“ – работещ по „горещ“ цикъл – бипропелантен, използващ T-stoff като окислител и C-stoff като гориво. За първи път лети през май 1943 г.
3.	109-509.A-1	150 – 1700	170	Me.163B	Най-ранното масово производство на агрегата A-1 работещ по „горещ“ цикъл. Използва електрически стартер за запалване на горивото и окислителя

4.	109-509.A-2	150 – 1700 160 – 1400	160	Me.163B	Развитие на агрегат A-1. Премахнати са електрическия пусков двигател и кутията със зъбна предавка. Има намалено тегло, запуск при стартиране с T-Stoff, добавени са ежектори, работещи с пара
5.	109-509.B	150 – 1700 300 – 100	201	Me.163B	По същество това е агрегат A-1. Добавена е допълнителна „крейсерска“ горивна камера, осигуряваща работа на двигателя в установен „крейсерски“ режим, за икономия на гориво и повишаване времето за работа. Изработени са само десет броя
6.	109-509.C	150 – 2000 + 100 – 400	180	Me.263	Същите части като мотора A-2, но има втора „крейсерска камера“ и друг вид цялостен дизайн. Налягането в основната горивна камера е повишено до 24 атмосфери
7.	109-509.D	150 – 1700	170	DFS Sagefisch	Същите части като двигател A-2, но разделени на три блока, като основният блок е изведен напред в корпуса, с удължени тръби за подаване на гориво
8.	109-509.A-2E ("109-509.E")	150 – 1700	160	Ba. Natter	A-2 е разработван за ракетата „Natter“. Някои части са пренаредени – включително пусковия стартер на T-Stoff и парогенератора, за да позволят правилното функциониране за вертикален пуск. Завършени са 15 експериментални единици през 1944 г., които са били предназначени за тестване. Проектът отпада през февруари 1945 г. Производствената единица би била с индекс „109-509.E“, но ракетата „Natter“ никога не е била завършена като проект
9.	109-509.S-1 Heimat-schützer I	150 – 1700	160	Me.262	A-2 е разработван за Me.262. Монтиран в опашната част на Me.262, този двигател му осигурява изключителен темп на изкачване във височина. Но инсталирането и поддръжката му са били трудни
10.	109-509.S-2 Heimat-schützer IV	Max 2000	140	Me.262	Ракета, „висяща“ под корема на Me.262. Използвани са части от 109-509.A2 и C. Все още е бил в процес на изпитания в Jenbach, когато фабриката е била превзета

Конструктивна характеристика

Конструктивната характеристика е отношението на масата на двигателя към неговата максимална тяга (табл. 2). Тази обобщена характеристика е показател за конструктивното съвършенство на ракетния двигател. Тя отговаря на един много важен въпрос – колко процента от общата маса (тегло) на ракетата (която може да бъде изстреляна) е нейния двигател?

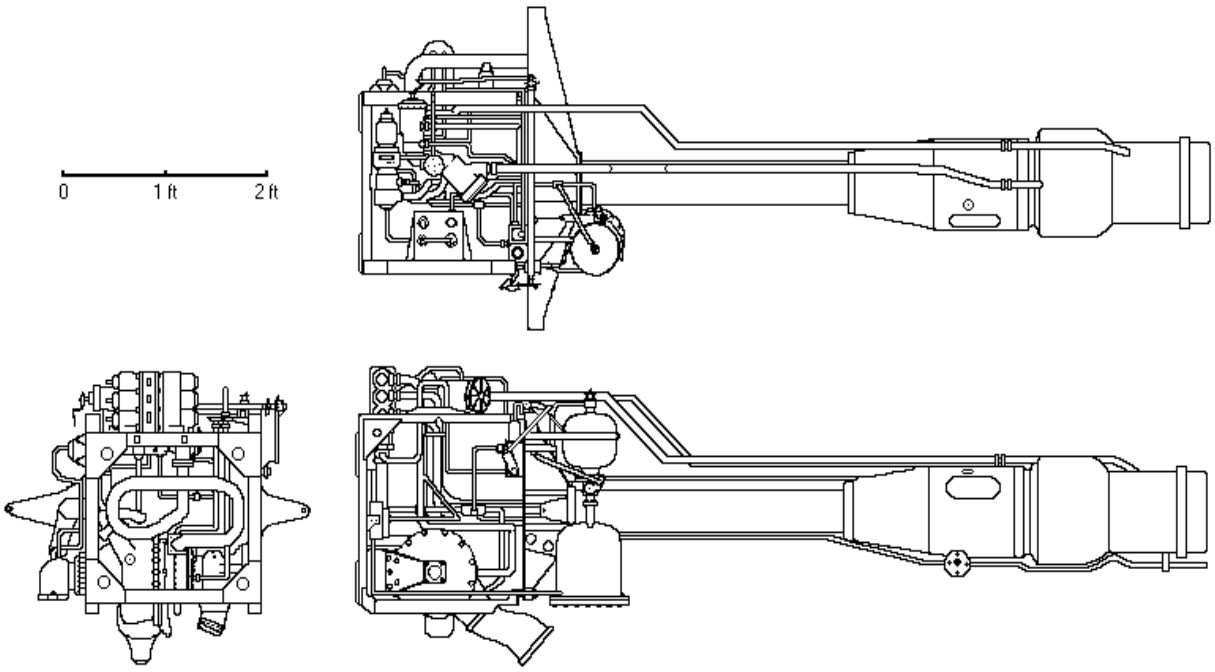
Таблица 2. Масата на двигателя към неговата максимална тяга

RII.211 109-509.A-0	109-509.A-1	109-509.A-2	109-509.B	109-509.C	109-509.D	109-509.A-2E 109-509.E	109-509.S-1	109-509.S-2
170	170	160	201	180	170	160	160	140
1500	1500	1700	1700	2000	1700	1700	1700	2000
0,1133	0,1133	0,0941	0,1182	0,0900	0,01	0,09411	0,09411	0,07
11,33%	11,33%	9,41%	11,82%	9,00%	10,00%	9,411%	9,411%	7,00%

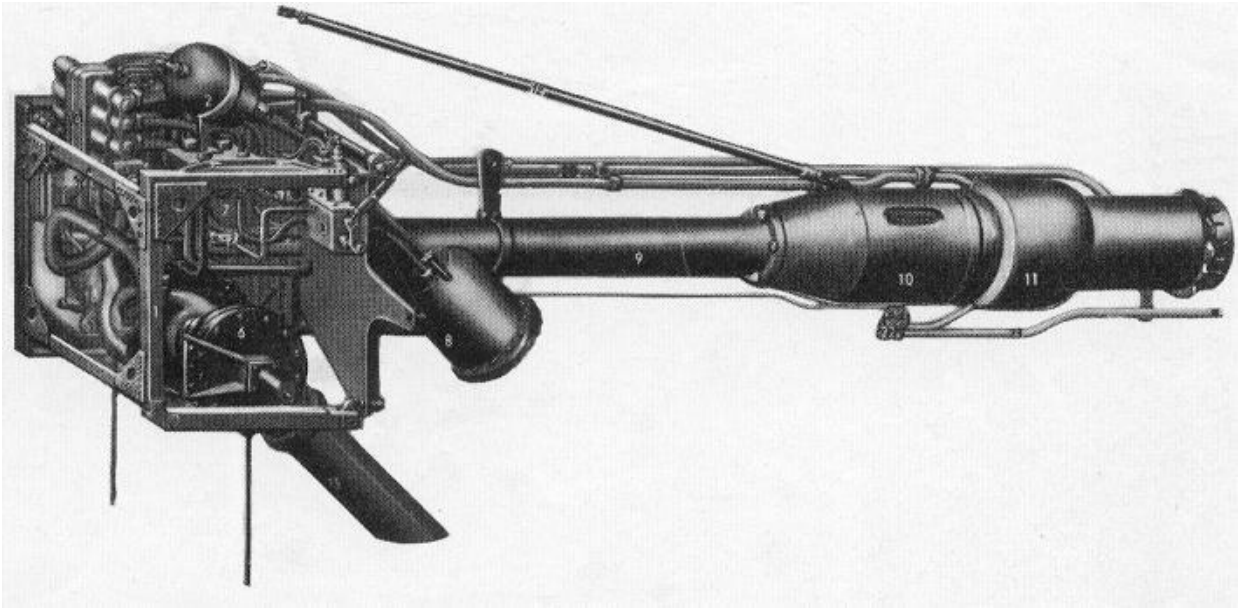
Налице е намаляване на процентите – от 11,33% до 7,00%, което е характерно и за съвременните ракети. Може да се направи извода, че от периода на ВСВ до сега не е направен съществен прогрес по този показател. Двигателите HWK 109-509 заслужават задълбочено изучаване – като конструкция и като горива, и свързаните с тях химически процеси [2], [5].

Общ вид на двигателя

Общият вид на двигателите HWK 109-509 е представен на фиг. 1 и фиг. 2.



Фиг. 1. Схема на двигателя



Фиг. 2. Снимка на реален двигател

Устройство на горивната камера и дюзите за впръскване на гориво

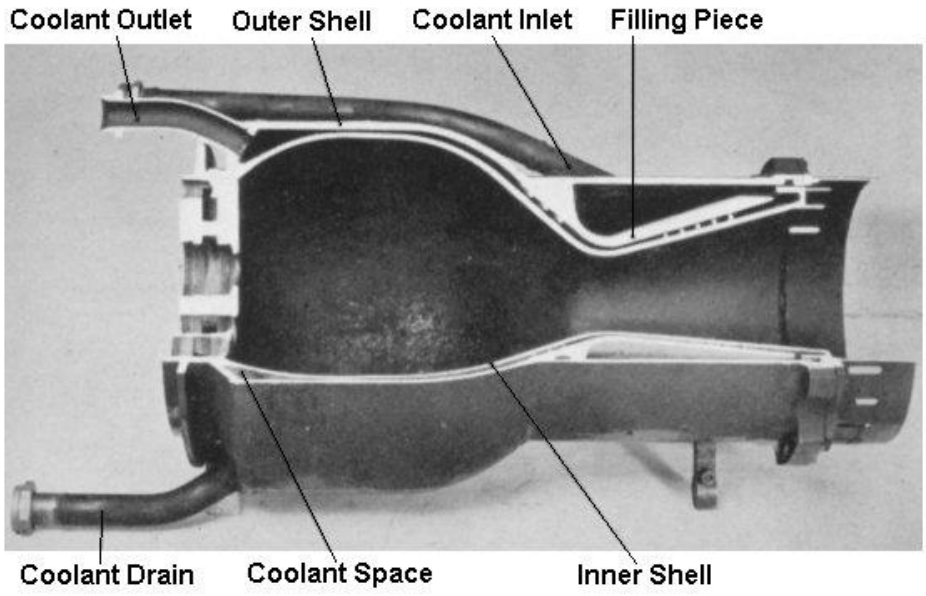
Горивна камера

Интересното при този вид горивна камера е фактът, че има охлаждане с гориво. То навлиза през Входа за охлаждащата течност, изпълва Пространството за охлаждаща течност и накрая излиза през Изхода за охлаждане и Дренажа. Този факт, както и използването на ниско температурно изгарящи горива (метанол) са довели до възможността за направата на Вътрешната черупка – същинската горивна камера от обикновена „мека“ стомана (фиг. 5).

Вътрешната черупка (горивната камера) е произведена от кована мека стомана, която е била термично обработена, за да се премахнат всички вътрешни напрежения преди окончателната обработка до точния размер. В противен случай дебелината трябва се увеличи в конвергентния участък, за да издържи на термичните напреженията, които се получават в процеса на горене. Фланците са обърнати отпред и отзад, за да се направят свързващи съединения с Външната обвивка.

Фиг. 3. Общ вид на горивната камера

Фиг. 4. Разрез на горивната камера



Фиг. 5. Разрез с означения

Coolant Inlet	Вход за охлаждаща течност
Coolant Outlet	Изход за охлаждаща течност
Coolant Drain	Дренаж за изтичане на охлаждащата течност
Coolant Space	Пространство за охлаждаща течност
Inner Shell	Вътрешна черупка – горивна камера
Filling Piece	Пространство, част за пълнене (от входа на охлаждащата течност)
Outer Shell	Външна обвивка на горивната камера

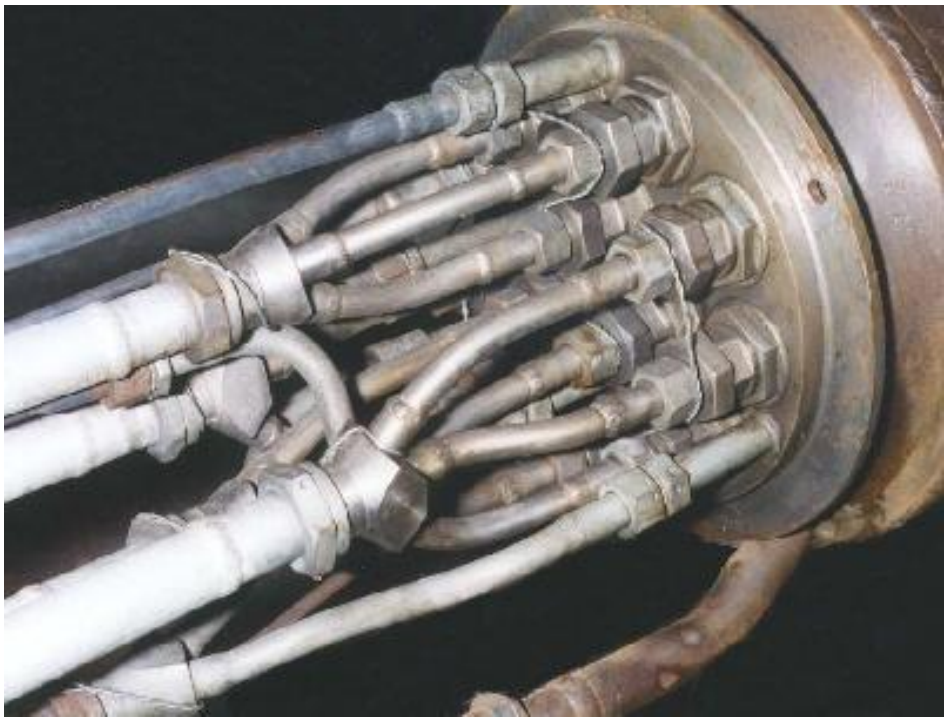
Външната обвивка е оформена от мека стомана, заварена по шева и студено пресована до диаметъра на задната цилиндрична част. Задната част е от мека стомана, заварена в цилиндър, след това заварена челно към предния участък – обърнатия стоманен фланец, заварен към цилиндъра, образува задната връзка. Съединението между вътрешната и външната обвивка е направено чрез заваряване на фланците в предния край, но отзад фланците са свободни да се плъзгат един спрямо друг за диференциално разширение по време на работа [7]. Уплътнението се прави чрез притискане на азбестова струна, покрита

с графит между фланците, за да се гарантира, че няма загуба на течност от охладителната риза.

Изискванията за лекота на производство диктуват формата на Външната обвивка така, че да се гарантира напълване и охлаждащата течност да се движи около външните повърхности на вътрешната обвивка с нормална скорост.

Глава на горивната камера

При главата (горната част) на горивната камера, входящите тръби на горивото пристигат по вътрешната страна на двигателя и завършват в комплекти разклоняващи се съединители (фиг. 6). Показана тук, всяка от големите бледо оцветени тръби се разклонява на три. Това е входът на T-Stoff и всяка тръба се разклонява, за да обслужва набор от три горелки. Знаейки, че има дванадесет горелки, може да си представим, че трябва да има „четири“ линии на T-Stoff.



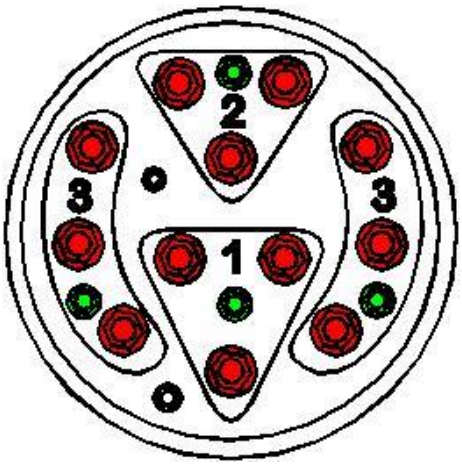
Фиг. 6. Глава на горивната камера – входящи горивоподаващи тръби

Когато двигателят работи, първият етап на тягата и вторият етап на тягата съответстват на набор от три горелки всяка, но когато е избран последният, трети етап, тягата идва от добавянето на последните шест горелки към общо дванадесет горелки, работещи с пълна мощност, максимални условия на тяга. Това става ясно от фиг. 7.

Комплектите от три горелки са подредени така, че всеки етап да създава равномерен модел на впръскване в горивната камера, а когато следващият етап на горелките влезе в действие, се създава модел на тяга, който е балансиран спрямо размерите на горивната камера.

Тръбите T-Stoff са показани в червено, а входящите тръби C-Stoff в зелено. Настройката на тягата на първия етап (1) е комплектът от горелки, който е в основата на плочата на горелката. Вторият етап (2) добавя към първия етап, като използва комплекта горелки към горната част на плочата на горелката.

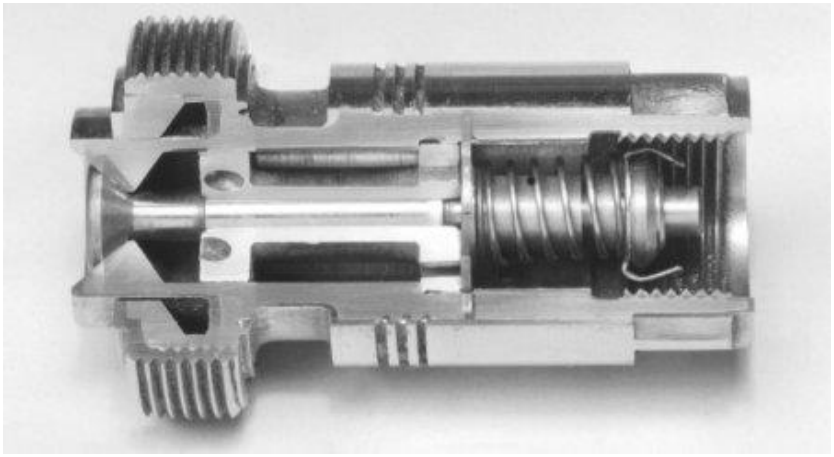
Накрая, тягата на третия етап (3) е от двата комплекта горелки от двете страни на плочата на горелката, поддържайки равномерността на тягата и изхода на тягата в баланс.



Фиг. 7. Разположение на горелките

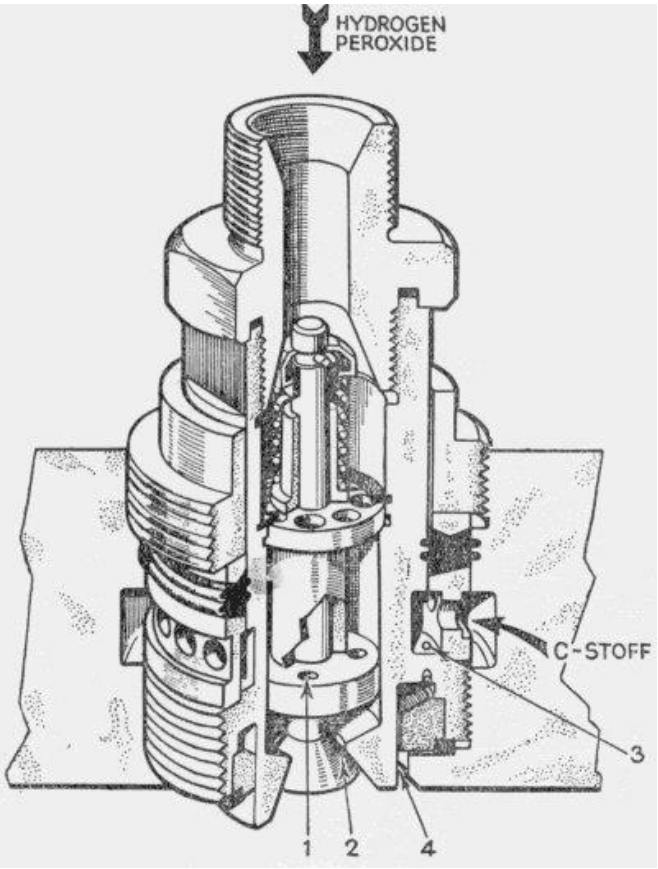
Горивни дюзи

Горивните дюзи (или „инжекторите“ – и двата термина са използвани в литературата) (фиг. 8) осигуряват средства за привеждане на ракетните горива в контакт по контролиран и точно измерен начин, за да реагират и за да произведат тягата на двигателя. Те са внимателно проектирани да произвеждат висока скорост на потока на горивото и освен това създадат фино пулверизиран спрей.



Фиг. 8. Инжектор в разрез

Горивните дюзи са показана по-горе. Както беше посочено, дванадесетте дюзи са монтирани в главата на горивната камера в групи от по три, съответстващи на настройките на тягата на първия, втория и третия етап. Това е така, защото задоволителната работа на горелката не би била възможна при голям обхват на горивните потоци без прекомерно максимално налягане. Инсталирането на мотора 109-509 в Komet е изисквало пилотът да има контрол върху тягата с променливи настройки на мощността, така че въвеждането на комплекти горелки за добавяне към изходната мощност намалява обхвата, изискван от отделните горелки.



Фиг. 9. Разрез с означения

Тялото на дюзата е изработено от цилиндрична стомана. Във вътрешния край се изрязва кръгъл жлеб, в който се свива и притиска стоманен пръстен. Този пръстен е оформен така, че в дъното на жлеба остава малка пръстеновидна камера, с тясна междина между пръстена и вътрешния радиус на жлеба, до тялото на горелката (фиг. 9).

От възпроизведената тук диаграма може да се види, че когато е монтирана дюзата, C-Stoff, доставен в главата на дюзата, преминава в канал, който е завъртян в тялото на цилиндъра. Четири тангенциално пробити отвора *3*, свързват този канал с пръстеновидната камера в главата на дюзата.

C-Stoff, преминавайки през главата на дюзата, преминава в обработения канал около дюзата, през тангенциалните отвори в пръстеновидната камера. Оттук то се инжектира в горивната камера през тясната пръстеновидна междина *4* под формата на фин цилиндричен спрей.

Около канала в дюзата има пробит филтърен пръстен, показан вляво от схемата тук. Той е снабден с фина мрежеста стоманена марля. Проектиран е за отстраняване на частици в C-Stoff. Тъй като частиците са достатъчно малки, за да преминат през основния филтър, ще преминат през дюзата – без да я блокират, било предложено да се откажат от този филтър. Когато е монтирана, мрежата е склонна да улавя частици и да запушва филтъра, така че с течение на времето дюзата се блокира толкова силно, че трябва да се смени.

Нека да разгледаме преминаването на T-Stoff – окислителят навлиза в края на дюзата през аксиално пробит отвор. Пружинен клапан, натоварен с пружина в конусовидна легло на лицевата страна на дюзата *2*, уплътнява аксиалното движение на челната страна на

горивната камера и предотвратява навлизането на C-Stoff в камерата на T-Stoff, когато двигателят работи на празен ход .

Максималният ход на изпускателния клапан се задава от дистанционна част на стеблото на клапана със заключващ пръстен, монтиран в края на стеблото на клапана. Преди да се инжектира в горивната камера, T-Stoff преминава през четири тангенциално пробити отвора във втулката на клапана близо до главата на горелката *1*. Диаметърът на тези отвори е начин за осигуряване на някакъв контрол върху калибрирането на потока на T-Stoff, по същия начин, като тангенциалните отвори в C-Stoff страната на дюзата.

Заключение

В настоящата работа е разгледано и показано устройството на реактивните двигатели HWK 109-509, както и на отделни елементи и части от целия агрегат. Не трябва да се заличават разработките от Втората световна война. Много от тях са дали тласък в технологиите до сега, а със сигурност има още открития от тогава, които заслужават внимание. В хода на войната немската армия е останала без доставки на масовите течни горива, поради което учените са имали множество достижения за преодоляването на проблема [1], [3]. Търсенето на алтернативни горива и в днешни дни стои пред човечеството, т.к. от една страна намаляват петролните залежи, а от друга е спазването на екологичните норми.

ЛИТЕРАТУРА:

[1] Богданов, А., Калев, К., Ганев, В. Анализ на методите за измерване скоростта на снаряда. XXII-ти научен симпозиум с международно участие – Метрология и метрологично осигуряване, Созопол, ISSN 1313-9126 (2012).

[2] Богданов, А., Калев, К., Ганев, В. Изследване на корелационната връзка между екологичните показатели на оръжейните системи. XVI-ти научен симпозиум с международно участие – Метрология и метрологично осигуряване, Созопол, ISBN 954-334-035-8 (2006).

[3] Богданов, А., Калев, К., Ганев, В. Изследване чувствителността на тензометричен датчик за измерване налягането на форсиране на барутните газове. XXIII-ти научен симпозиум с международно участие – Метрология и метрологично осигуряване, Созопол, ISSN: 1313-9126 (2013).

[4] Жекова, Ц., Костадинова, Д. Изследване на съвременни планировъчни решения при космическите комплекси. XVI Международна научна конференция ВСУ 2016. стр.367-373, ISSN 1314-071X. София (2016).

[5] Bogdanov, A. Kalev, K. Logical and Structural Connections in the Process of Teaching Metrology and Measurement Equipment. Second Regional Conference on Engineerin Education, Sofia (2003).

[6] Walter, H. Experiences with the application of the hydrogen peroxide for production of power. Jet Propulsion. AAIA. Vol.24, Num.3; 1954. ISSN: 1936-9980; https://doi.org/10.2514/8.6484 (2012).

[7] http://www.walterwerke.co.uk/walter/index.htm

Имена на авторите: **доц. д-р инж. Христо Ангелов Христов**
Месторабота: Българско училище „Христо Ботев“ – Братислава

доц. д-р инж. Цветослав Станиславов Цанков
Месторабота: Шуменски университет „Епископ Константин Преславски“
E-mail: c.cankov@shu.bg

EQUIPMENT OF AUTOTRACTOR WORKSHOPS WITH MACHINE TOOLS

TSVETOSLAV S. TSANKOV, EKATERINA M. KONSTANTINOVA

ABSTRACT: *The report presents the possibilities for providing long-term equipment for large and medium car repair shops, as well as for tractor workshops. Machine tools are needed both in the machining and repair of automotive parts. Closing the cycle for maintenance and repair of a personal or a business car is the best solution for large service garages.*

KEYWORDS: *Automobile repair shop, Grinding machine, Machine tool, Surface grinding.*

ОБОРУДВАНЕ НА АВТОТРАКТОРНИТЕ РАБОТИЛНИЦИ С МЕТАЛООБРАБОТВАЩИ МАШИНИ

ЦВЕТОСЛАВ С. ЦАНКОВ, ЕКАТЕРИНА М. КОНСТАНТИНОВА

АБСТРАКТ: *В доклада са представени възможностите за осигуряване с дълготрайно оборудване на големите и средни автосервизи, както и за автотракторни работилници. Металообработващите машини са необходими както в производството, така и при ремонта на автомобилните детайли. Затварянето на цикъла по поддръжката и ремонта на личен или служебен автомобил е най-доброто решение за големите автосервизи.*

Въведение

Големите автосервизи и автотракторни работилници се стремят към затваряне на цикъла по поддръжката и ремонта на автомобилите. Така например големите сервизи трябва да имат работилница за боядисване, работилница за смяна и ремонт на автомобилни колела и гуми, стенд за проверка и регулиране геометрията на окачването, работилници за двигатели, трансмисия и т.н. Собствените складове с авточасти за масовите автомобили също са голямо предимство, което освен печалба, осигурява и кратки срокове за връщане на автомобила при собственика.

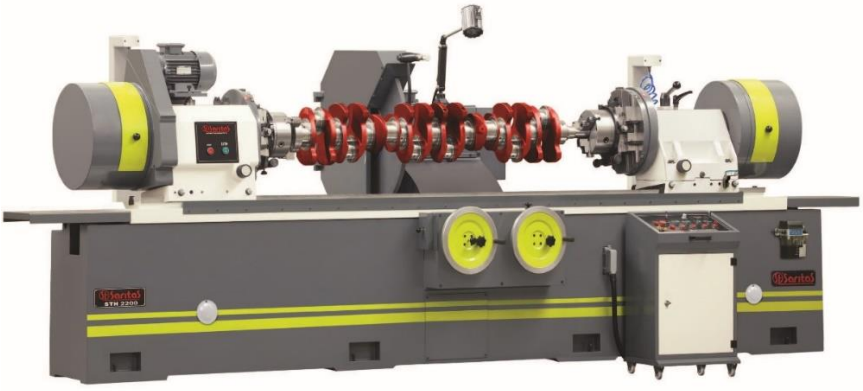
Освен за авточасти, сервизите прибягват до услугите на външни фирми и за обработка на автомобилните детайли с металообработващи машини. Няколко специализирани или универсални машини безспорно са добра дълготрайна инвестиция в големите и средни авторемонтни предприятия, а ролята им ще бъде пояснена по-долу.

Едно важно условие е работниците да имат добра подготовка, или да са специално назначени за работа с металообработващи машини.

Машина за шлайфане на колянови валове

Коляновия вал на двигателя с вътрешно горене (ДВГ) е един от най-скъпите детайли в автомобилите. В болшинството от случаите неговите основни и мотовилкови лагери са плъзгащи, като триенето им е с шийките на самия вал. Триенето е течно, като се подава масло под налягане между триещите се повърхнини. Въпреки това обаче, налице е износване след даден пробег.

За коляновите валове се предлагат ремонтен размер лагери, с които да се възстанови номиналната хлабина между вал и отвор. Това е възможно в случаите, когато не е настъпило твърде голямо износване или аварийна ситуация на непоправимо износване, дори огъване на коляновия вал. Обработката на шийките на коляновия вал до ремонтен размер става на кръглошлифовъчна машина за колянови валове (фиг. 1).



Фиг. 1. Машина за шлайф на колянови валове

Обработвания колянов вал се поставя между двете опори, които позволяват неговото завъртане. Едната опора е здвижваща, а другата е задвижвана от коляновия вал. Закрепването на вала е за двата центросместителя, които позволяват освен въртенето му по основната осева линия за шлайфане на основите шийки, отместването на коляновия вал за въртене около осева линия на мотовилкови шийки. Зад всяка от дете опори са на разположение противотежести, които служат за баланс при шлайфане на мотовилкови шийки. Шлифовъчния кръг се върти на собствен шпиндел и има възможност за радиално и осово отместване спрямо шлайфаната шийка на коляновия вал.

Работилниците за шлайфане трябва да бъдат с поддържана температура, а автомобилните детайли да са престояли достатъчно дълго при желаната температура, за да бъдат коректни всички измервания. Шлайфането протича при подаването на смазващо-охлаждаща течност, която отмива твърдите частици и не позволява прегряване.

Машини за разстъргване и хонинговане на цилиндри

Те също са тясно специализирани машини и трябва да бъдат отделени в работилница, ако не самостоятелно, то заедно с машината за шлайфане на колянови валове.

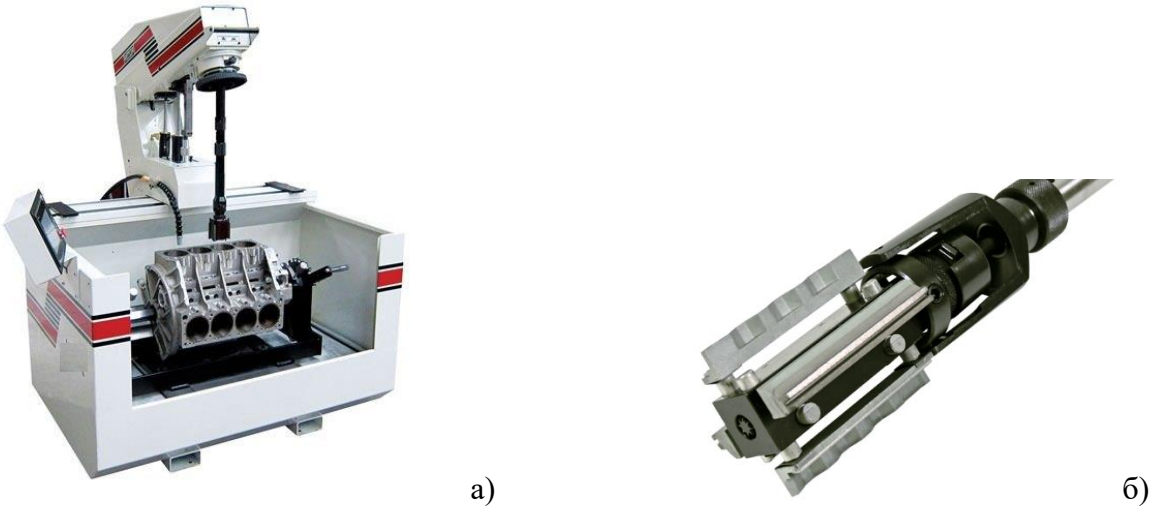
Триенето на буталото и буталните пръстени с цилиндъра води до тяхното износване. Подменят се буталото с буталните пръстени и сваляеми цилиндри за водно или въздушно охлаждане. В повечето случаи цилиндрите са изработени заедно с цилиндровия блок, а в такъв случай са предвидени ремонтни размери бутала и бутални пръстени.

За привеждането на цилиндрите в цилиндровия блок до съответната стегнатост с буталата, работата започва с машината за разстъргване и фрезоване (фиг. 2). Вертикалният шпиндел на машината трябва да бъде в съосност с обработвания цилиндър. В болшинството от случаите това е лесно, защото осевите линии на цилиндрите са перпендикулярни на повърхнината, която стъпва върху работната маса на машината. За цилиндрите, наклонени спрямо базовата повърхнина и за V-образните цилиндрови блокове се налага използването на допълнителни приставки, както при показания на фиг. 2.

Фиг. 2. Машина за разстъргване на цилиндри

Същата машина се използва и за гилзоване, което се налага тогава, когато са преминали всички предлагани ремонтни размери. Вставянето на суха втулка се извършва с необходимата стегнатост.

За достигането на точен размер на цилиндрите се използва машината за хонинговане (фиг. 3а), която обработва цилиндрите с хонинговъчна глава (фиг. 3б)



а) б)

Фиг. 3. Машина за хонинговане (а), хонинговъчна глава (б)

При специалните движения на хона се получават грапавини във вид на винтова мрежа, които могат да задържат слой масло при експлоатацията на автомобила и да спомагат за

намаляването на износването. Шлайфането на цилиндрите до огледало се прилага главно за състезателни автомобили, при които се цели повишаването на динамичните характеристики, независимо от повишеното износване и разход на масло.

Плоскошлифовъчна машина

Най-честите големи ремонти по автомобилните ДВГ са със задължително демонтиране на цилиндровата глава. Между цилиндровия блок и цилиндровата глава се използва гарнитура за уплътняване между пространствата на горивната камера, охлаждащата течност, маслена магистрала и т.н.

Гарнитурите за глава на старите модели двигатели са с армирана азбестово-графитна основа, обкована със стоманени или медни пръстени. Съвременните автомобили имат многослойни метални гарнитури, като за уплътняване се използват притискащи фигури, изработени върху някои от листовете край повечето от отворите, както и прилепнали силиконови уплътнения.

Притискащите повърхнини на цилиндровата глава и цилиндровия блок трябва да бъдат без отклонения от плоскост, а това се постига с шлайф плосък хоризонтален (ШПХ) или шлайф плосък вертикален (ШПВ), като хоризонтален и вертикален са шпинделите на шлифовъчния кръг (фиг. 4).

а) б)

Фиг. 4. Плоскошлифовъчни машини: а) ШПХ; б) ШПВ

Отклоненията от плоскост на повърхнините най-често е вследствие топлинни деформации, наслоявания, неправилни въздействия с шабър или шкурка. В болшинството от случаите отклоненията са незабележими, поради което трябва да бъдат измерени на станок, чрез обход с индикаторен часовник.

Закрепването на цилиндровия блок или цилиндровата глава към работната маса на шлайфа, обикновено става чрез електромагнит, като трябва да се осигури паралелност на базовата и шлайфаната повърхнина. Шлайфането е придружено от обилно заливане със смазващо-охлаждаща течност, отмиваща твърдите частици и непозволяваща прегряване. Характерно за шлайфа с хоризонтален шпиндел на шлифовъчния кръг е, че възвратно-постъпателното движение по оста ***X*** е много по-бързо от същото при ШПВ.

При шлайфането на чугунени цилиндрови глави и цилиндрови блокове, повърхнините стават огледални. Това не е препоръчително за двигатели с азбестово-графитни гарнитури, поради опасност от изплъзване и разкъсване на гарнитурата. В тези случаи е препоръчително повърхностите да се фрезоват фино, което е друга функция на машината за разстъргване на цилиндри.

Универсален струг

Още една машина, която ще има голяма заетост, това е универсалния струг. При избор на струг се вземат предвид големината на автомобилните детайли, които ще се обработват, за да има струга необходимия обхват. Напълно е възможно при планирането на работата да бъде предложено стругарската работилница в автосервиза да бъде оборудвана с голям струг (фиг. 5а) и с малък настолен струг (фиг. 5б).

а)

б)

Фиг. 5. Универсални стругове: а) СТ 16К20Б; б) малък настолен

Операциите, които се извършват по автомобилните детайли с универсален струг, обикновено отнемат кратко време, поради което е препоръчително да има стругарска работилница в сервиза, вместо да се използва външна фирма. Най-често стругът се използва за престъргване на спирачните дискове или барабани, като от особена важност е безупречното центроване на тези детайли.

Заключение

Изключително важна е ролята на металообработващите машини при ремонта на автомобили и трактори. Самостоятелната работа на автосервизите, без помощта на фирми, специализирани в обработване на метали, може да се постигне с оборудването на собствени работилници за обработване на автомобилни детайли.

Изброените тук машини са препоръчителни за големите автосервизи, докато за средно големите препоръчителни са плоскошлифовъчна машина и универсален струг. Задължително дори и за най-малките автосервизи е оборудването с пробивни машини, които в зависимост от необходимостта могат да бъдат от малки настолни до големи колонни.

В годините на индустриализация през миналия век, Народна република България имаше заводи за металорежещи машини. Поради крупнокорпусната конструкция на металообработващите машини, напълното им възстановяване се извършва в ремонтни заводи, които по традиция продължават да работят в Република България. Това позволява добре поддържаната машина да работи много десетилетия и да бъде една добра дългосрочна инвестиция за автотракторните ремонтни предприятия.

ЛИТЕРАТУРА:

[1] Вереина, Л.И., Усов, Б.А. Конструкции и наладка токарно-затыловочных станков. Высшая школа, М. (1985).

[2] Ловыгин, А.А., Теверовский, Л.В. Современный станок с ЧПУ и CAD & CAM система. М., ДМК Пресс (2012).

[3] Стерин, И.С. Способы и схемы обработки цилиндрических отверстий на токарном станке. Фабрика экранных учебно-наглядных пособий ВТПП ГК СМ СССР по профтехобразованию (1969).

[4] http://autoaccessoriesperformance.com/best-head-gaskets-choosing-right-gasket-car/

[5] http://uhv.cheme.cmu.edu/procedures/machining/ch7.pdf

[6] https://youtu.be/ovUxCOsMHu8

Имена на авторите: доц. д-р инж. Цветослав Станиславов Цанков,
Месторабота: Шуменски университет „Епископ Константин Преславски“
E-mail: c.cankov@shu.bg

Екатерина Минкова Константинова – студент

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ