ШУМЕНСКИ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“
KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN

том 2

2024

# МАТПЛЕХ

НАУЧНА КОНФЕРЕНЦИЯ С МЕЖДУНАРОДНО УЧАСТИЕ

# СБОРНИК НАУЧНИ ТРУДОВЕ

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ

SCIENTIFIC CONFERENCE WITH INTENATIONAL PARTICIPATION

# CONFERENCE PROCEEDINGS

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
FACULTY OF TECHNICAL SCIENCES

volume 2

**ШУМЕНСКИ УНИВЕРСИТЕТ**
**„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“**

**ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА**
**ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ**

**KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN**

**FACULTY OF MATHEMATICS AND COMPUTER SCIENCE**
**FACULTY OF TECHNICAL SCIENCES**

# МАТТЕХ 2024

## СБОРНИК НАУЧНИ ТРУДОВЕ

# МАТТЕН2024

## 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**

Университетско издателство
"Епископ Константин Преславски"

Настоящият сборник съдържа научни доклади, изнесени на проведената през месец октомври 2024 година в Шуменския университет научна конференция с международно участие MATTEX 2024 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 2024 held at Konstantin Preslavsky University of Shumen in October 2024. 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.


## EDITORIAL BOARD:

Acad. Prof. Eng. Zhivko Stoyanov Zhekov, Dr. Habil
Acad. Prof. Eng. Genadiy Maklakov, Dr. Habil
Acad. Prof. Eng. Valery Bondur, Dr. Habil
Corr. Mem. Prof. Eng. Petar Getsov, Dr. Habil
Prof. Eng. Garo Mardirosian, Dr. Habil
Prof. Eng. Evgeni Petrov Manev, PhD
Prof. Eng. Yuriy Ivanov Dachev, PhD
Prof. Eng. Sabin Ivanov Ivanov, PhD
Assoc. Prof. Eng. Janis Kaminskis, PhD
Assoc. Prof. Eng. Andrey Iliev Bogdanov, PhD
Assoc. Prof. Eng. Valentin Tonev Atanasov, PhD
Assoc. Prof. Eng. Donika Velichkova Dimanova, PhD
Assoc. Prof. Eng. Tihomir Spirdonov Trifonov, PhD
Assoc. Prof. Eng. Evgeni Grishev Stoykov, PhD
Assoc. Prof. Zdravko Yuriev Kuzmanov, PhD
Assoc. Prof. Yordanka Ivaylova Yankova-Yordanova, PhD
Acad. Prof. Eng. Tsvetoslav Stanislavov Tsankov, PhD



**ISSN: 1314-3921**

**DOI: https://doi.org/10.46687/FTN24MT**

Сборникът излиза от печат през януари 2025 година.



© Университетско издателство "Епископ Константин Преславски"

Konstantin Preslavsky University Press

# ARCHITECTURE OF AN INTEGRATED SYSTEM WITH ASYNCHRONOUS USER INPUTS IN AN OPERATIONAL ENVIRONMENT, BUILDING A MOTIVATIONAL AND STRESS-FREE ENVIRONMENT*

**VALENTIN T. ATANASOV, TIHOMIR S. TRIFONOV**

***ABSTRACT:*** *Among the main factors affecting human activity are motivation and emotions. The learning process is a part of the fundamental modern human activity, and as such, analyzing it, factors that have a positive impact and contribute to its effectiveness should be considered. In this publication, a conceptual architecture of an integrated system is considered, comprising basic autonomous subsystems, subordinated to a single goal - promoting interest and motivation among learners by introducing the learning game into the educational process by means of information and communication technologies.*

***KEYWORDS:*** *learning game, learning process, game system architecture*

***DOI: https://doi.org/10.46687/IVDL8753***

# АРХИТЕКТУРА НА ИНТЕГРИРАНА СИСТЕМА С АСИНХРОННИ ПОТРЕБИТЕЛСКИ ВХОДОВЕ В ОПЕРАЦИОННА СРЕДА, ИЗГРАЖДАЩА МОТИВИРАЩО И НЕСТРЕСОВО ОБКРЪЖЕНИЕ

**ВАЛЕНТИН Т. АТАНАСОВ, ТИХОМИР С. ТРИФОНОВ**

***АБСТРАКТ:*** *Сред основните фактори, влияещи върху човешката активност са мотивацията и емоциите. Учебният процес е част от фундаменталната съвременна човешка дейност и като такъв, анализирайки го, следва да бъдат разглеждани фактори, оказващи положително въздействие и способстващи неговата ефективност. В настоящата публикация се разглежда концептуално архитектура на интегрирана система, обхващаща основни автономни подсистеми, подчинени на единна цел – насърчаване на интереса и мотивацията сред обучаемите чрез въвеждане на обучаващата игра в образователния процес посредством информационните и комуникационни технологии.*

## 1 Въведение

В съвременното социално поле има трайно установени индивиди, поставени и опериращи в една изцяло интерактивно-технологична среда, „*в която те създават, възприемат, обработват и предоставят информация само чрез цифрови технологии*“ [2]. Може да бъде отчетено, че с такава характеристика на „*високо интерактивно поколение*“ са и доминираща част от онези, пристъпили в залите и лабораториите на съвременните висши учебни институти. В синхрон с концептуализацията на обучението в съвременната образователна теория [4] се определят елементи на структурата и основни параметри на учебните програми както и организацията на образователния процес в дигитална среда (*локална, отдалечена*).

Сред потенциалните съвременни методи в образователната сфера могат откроени обучаващите игри, базирани на информационни и комуникационни технологии. Тези

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

методи, обаче остават встрани от полезрението на основната група преподаватели като възможен дидактически инструмент, въпреки че предоставят „*мотивираща и завладяваща нестресова среда за обучаваните“* [1], че „*изживяванията в дигиталните игри са изградени около целенасочени и ефективни принципи на обучение*“ [5] и че определени преподаватели започват да прилагат обучаващи игри с цел подобряване мотивацията на обучаемите [6].

В настоящата публикация се разглежда подход за изграждане на игрова среда в учебен процес посредством архитектура на интегрирана система, обхващаща автономни подсистеми и която система се предвижда да бъде поставена в операционна среда. Следва да бъде отбелязано, че всяка една от подсистемите на предлаганата интегрирана система има изключителна автономност при своето функциониране т.е. тяхното(на подсистемите) предназначение не предполага изрично наличието на приложен програмен интерфейс (API), който да бъде ad-hoc разглеждан при междусистемната комуникация.

Инженерният подход, обаче, позволява дадена интерфейсна компонента на разглежданите подсистеми да бъде използвана по начин, обезпечаващ информационния обмен между две системи. Това обстоятелство предполага изнамирането на интерфейсни точки, които да способстват такъв информационен обмен за целите на интегрираната система.

По-долу ще бъдат представени използваните подсистеми, техните основни и за целите на интегрираната система характеристики.

# 2 Архитектура на интегрираната система

Следвайки установената инженерна практика при синтеза на дадена система, се дефинира основна цел за изграждане на разглежданата интегрирана система, която цел ще определи съществената характеристика, функционалностите и обхвата й.

## 2.1. Основна цел на интегрираната система, задачи и принципи

### *2.1.1. Основна цел*

С изграждането на интегрираната система се цели формиране на мотивираща и нестресова игрова среда, включваща основни и автономни подсистеми, обезпечаващи краен положителен ефект върху учебния процес и емоционалните възприятия на обучаемите (студенти). Следва да бъде отбелязано, че според невролози видео(компютърните) игри имат благоприятен ефект върху когнитивния процес на човека, обстоятелство отразяващо се на мозъчната структура и функция. в положителен смисъл [7].

### *2.1.2. Задачи*

В контекста на основната цел са дефинирани следните задачи:

- В процеса на изграждане на интегрираната система да бъде включен обем от знания на не по-малко от пет учебни дисциплини от учебния план от инженерните специалности („Предаване на данни и компютърни комуникации“, „Микропроцесорна техника“, „Операционни системи“, „Компютърни архитектури“, „Компютърни мрежи“, „База от данни“, „Анализ и синтез на КИС“, „Администриране на мрежи“, „Мултимедийни системи“, „WEB дизайн и програмиране“);
- Да се изнамери интерфейсен подход за съгласуван междусистемен обмен на видео и звукови данни;
- Да се формират две звена с по пет работни клиентски станции в системата;

- Всички работни клиентски станции от двете звена на системата да са с идентични апаратни и програмни характеристики;
- Да се използват системи с отворен код (Creative commons 4.0) и/или такива с валидни лицензирани права.

*2.1.3. Принципи*

- При решаването на конкретни инженерни казуси при междусистемната интеграция да се използва социално-конструктивисткият подход;
- Стилът и психофизически характеристики на използваната игрова платформа следва да предполагат ненакърняване на личността и спазване на общоприети етични норми;
- За постигането на основната цел образователната институция предоставя свои технологични ресурси.

## 2.2. Спецификации

- Основен графичен набор от ППИ/API – библиотека DirectX(DirectDraw) [8, 10];
- Изграждане на клиент-сървър модел;
- Независимост от мрежовата топология;
- Клиентските заявки към сървъра са базирани на HTTP и UDP;
- Приложимо както към системи със самостоятелна графична карта, така и към системи с интегрирана в процесора графична карта;
- Прихванатите видео и звукови данни да бъдат поточно излъчвани в подсистемата „Мултимедийна многопотребителска платформа за хостване и поточно излъчване видео и звуков тип данни“ с ниска степен на латентност;
- Изгражда се единица за мониторинг на процесите в интегрираната система;
- Изграждат се две зони, в които са разположените звената на обучаемите;
- Поради природата на компютърните игри се приема, че всеки отделен управляващ потребителския вход на системата е асинхронен;

Поради ограниченията в обема на издателя, в настоящата публикация няма да бъдат представени в детайли техническите спецификации на операционната среда, програмното, апаратното и мрежовото обезпечение, което ще бъде използвано при формулирането на изискванията към системата.

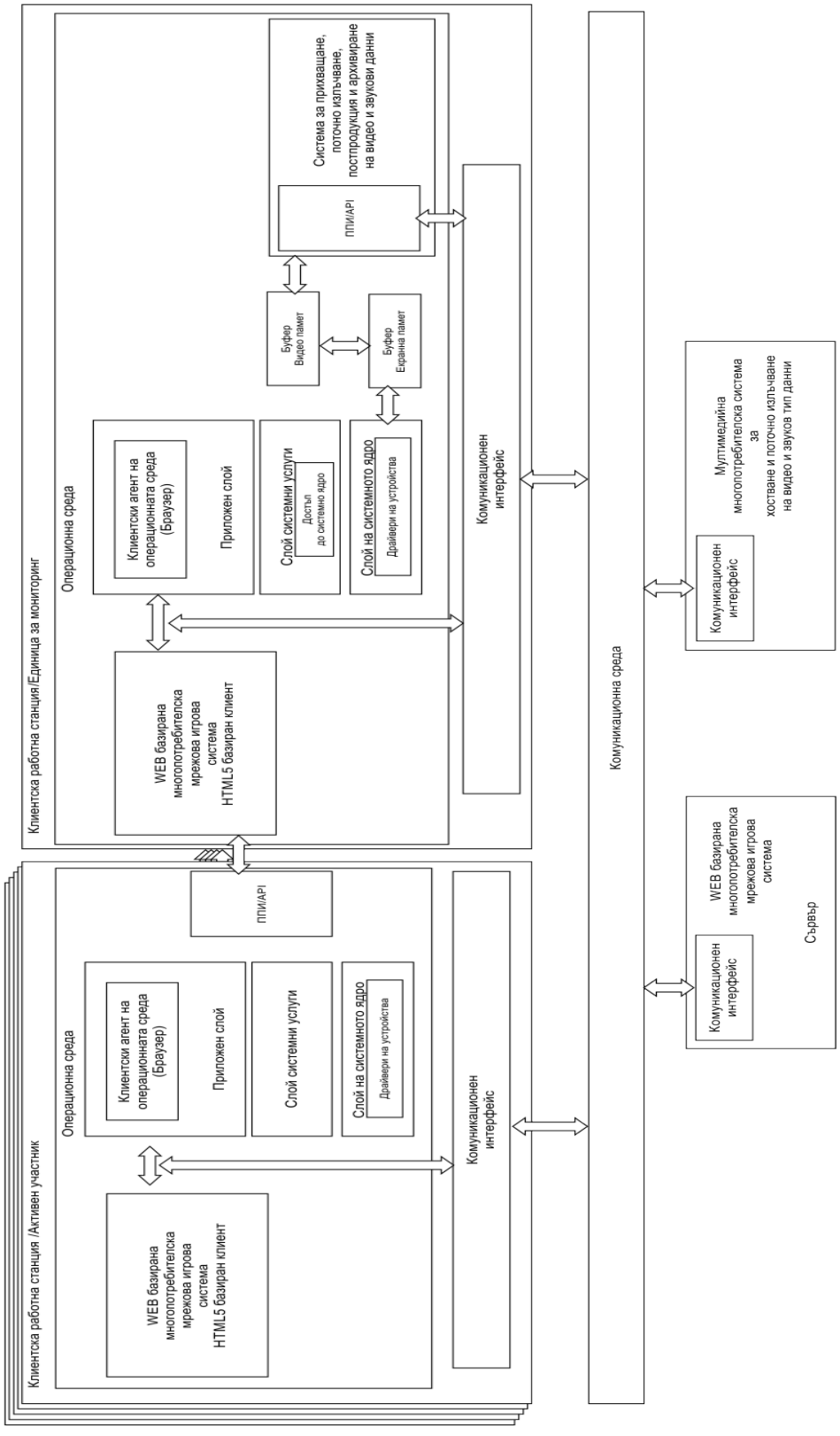
## 2.3. Избор на подсистеми и операционна среда

Като подходящи за постигане на основната цел се избират следните автономни системи, които биха осигурили висока степен на нейната ефективност:

- WEB базирана многопотребителска мрежова игрова система - League of Legends, основана на Клиент-сървър модел (Текущата версия на клиента е базирана на стандарта HTML5 и JavaScript) [11];
- Мултимедийна многопотребителска платформа(система) за хостване и поточно излъчване на видео и звуков тип данни – YouTube [3];
- Система за прихващане, поточно излъчване, постпродукция и архивиране на видео и звукови данни - Open Broadcaster Software (OBS) [10];
- За операционна среда се избира операционна система Windows 10 версия 22H2.

## 2.4. Архитектура

По-долу е представена синтезираната архитектура на интегрирана система с асинхронни потребителски входове в операционна среда (фиг. 1).




**Фиг. 1.** Архитектура на интегрирана система с асинхронни потребителски входове в операционна среда

Представената на фиг. 1 архитектура се основава на описаните в т. 2.2. спецификации.

# 3 Заключение

При синтеза на интегрираната система с асинхронни потребителски входове в операционна среда се отчитат факторите, влияещи върху оперативната съвместимост на избраните подсистеми. Това се налага поради необходимостта от обмен на видео и звукови данни. Освен изграждането на подход при информационния обмен чрез ППИ, се изисква и постигане на ниска степен на латентност на визуализираните поточно данни. Предстои провеждането на експеримент с изградената система, натрупване на емпирични данни, последващата им обработка, представяне на резултатите от експеримента и формиране на изводи.

**ЛИТЕРАТУРА:**

[1] Атанасов, В., Т., Един подход за разработка на анимиращ обект с използването на JavaScript за целите на обучаващи приложения, Сборник научни трудове, Университетско издателство „Епископ Константин Преславски", том 2, 2022, pp.35-39, ISSN: 1314-3921.

[2] Atanasov, V., Ivanova, A., A framework for evaluation of Web based learning content, International Journal on Information Technologies & Security, № 4, vol. 14, 2022, pp. 13-24, ISSN 1313-8251.

[3] Xu, A., System Design Interview: An Insider's Guide, second edition, Shroff/bytebytego, volume 1, 2020, ISBN: 979-8664653403.

[4] Miranda, J., Navarrete, Ch., Noguez, J., Molina-Espinosa, J. M., Ramírez-Montoya, M. S., Navarro-Tuch, S. A., Bustamante-Bello, M. R., Rosas-Fernández, J. B., Molina, A. The core components of education 4.0 in higher education: Three case studies in engineering education. Computers & Electrical Engineering, Volume 93, 2021, https://doi.org/10.1016/j.compeleceng.2021.107278.

[5] Gillern, S., Olsen, A., Nash, B., Stufft, C., An examination of teachers' views on video games and learning Establishing the Games and Literacy Education (GALE) scale, Computers & Education, vol.223, 105155, 2024, ISSN: 0360-1315, https://doi.org/10.1016/j.compedu.2024.105155.

[6] Chen, Ch., Huang, K., The interplay of rewards and competition in digital game-based learning Effects on intrinsic motivation, game performance and behaviors, and computational thinking, Learning and Instruction, vol. 94, 101995, 2024, ISSN: 0959-4752, https://doi.org/10.1016/j.learninstruc.2024.101995.

[7] Kühn, S., Gallinat, J., Mascherek, A., Effects of computer gaming on cognition, brain structure, and function: a critical reflection on existing literature, Dialogues in clinical neuroscience, Vol. 21, No. 3, 2019, https://doi: 10.31887/DCNS.2019.21.3/skuehn.

[8] Method for intactly obtaining GDI and DirectX data, (https://patents.google.com/patent/CN101211258A/en) (посетен на 01.10.2024).

[9] Overview of the Windows Graphics Architecture, 2022, (https://learn.microsoft.com/en-us/windows/win32/learnwin32/overview-of-the-windows-graphics-architecture) (посетен на 01.10.2024).

[10] Open Broadcast Software, Streaming, 2024, (https://obsproject.com/kb/category/4) (посетен на 01.10.2024).

[11] Riot Games, The Architecture of the League Client Update, 2016, (https://technology.riotgames.com/news/architecture-league-client-update) (посетен на 01.10.2024).

# HARDWARE PLATFORMS COMPATIBLE WITH P4 PROGRAMMING LANGUAGE*

**MUSTAFA B. UZUN, VALENTIN T. ATANASOV**

***ABSTRACT:*** *The P4 language, designed for protocol-independent packet processing, has revolutionized network programmability by enabling granular control over how packets are processed. A key factor in the success of P4 is its compatibility with diverse hardware platforms, allowing for flexible deployment in various network environments. This abstract explores several hardware platforms that support P4-programmable data planes, including programmable switch ASICs, Network Processing Units (NPUs), FPGAs, and software-based packet processors. ASICs, such as Intel's Tofino, offer high-performance, low-latency packet processing, while FPGAs provide reconfigurable logic suitable for custom data plane designs. NPUs strike a balance between flexibility and performance, ideal for specific network functions. Software-based platforms, such as BMv2, enable simulation and rapid prototyping of P4 programs. The availability of these platforms highlights the versatility of P4 and its capability to meet the varying needs of modern networks, from data centers to edge devices, ensuring efficient, scalable, and programmable network operations.*

***KEYWORDS:*** *P4 (Programming Protocol-independent Packet Processors), P4 Programming Language, SDN (Software Defined Networking), ASIC (Application-specific Integrated Circuit), FPGA (Field-programmable Gate Array), SmartNIC (Smart Network Interface Card)*

***DOI: https://doi.org/10.46687/YXBP1378***

# ХАРДУЕРНИ ПЛАТФОРМИ, СЪВМЕСТИМИ С ЕЗИКА ЗА ПРОГРАМИРАНЕ P4

**МУСТАФА Б. УЗУН, ВАЛЕНТИН Т. АТАНАСОВ**

***АБСТРАКТ:*** *Езикът P4, създаден за протоколно-независима обработка на пакети, революционизира програмируемостта на мрежите, като позволява прецизен контрол върху обработката на пакетите. Ключов фактор за успеха на P4 е неговата съвместимост с разнообразни хардуерни платформи, което дава възможност за гъвкаво внедряване в различни мрежови среди. Този абстракт разглежда няколко хардуерни платформи, които поддържат P4-програмируеми плоскости за обработка на данни, включително програмируеми ASIC комутатори, мрежови процесорни модули (NPUs), FPGA и софтуерни процесори за пакети. ASIC чипове, като Intel Tofino, предлагат високопроизводителна и нискозакъснителна обработка на пакети, докато FPGA предоставят преконфигурируема логика, подходяща за персонализирани дизайни на плоскости за данни. NPU устройствата осигуряват баланс между гъвкавост и производителност, което ги прави идеални за специфични мрежови функции. Софтуерни платформи, като BMv2, позволяват симулация и бързо прототипиране на P4 програми. Наличието на тези платформи подчертава универсалността на P4 и неговата способност да отговори на разнообразните нужди на съвременните мрежи – от центрове за данни до крайни устройства – осигурявайки ефективни, мащабируеми и програмируеми мрежови операции.*

## 1 Въведение

Развитието на мрежовите технологии и необходимостта от гъвкавост в обработката на мрежови пакети водят до нарастващ интерес към програмируемите мрежови архитектури.

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

Програмирането на „Протоколно-независимите пакетни процесори“, с езика за програмиране P4, позволяват на мрежовите устройства да обработват мрежови пакети по гъвкав и адаптивен начин, без да се обвързват със специфични протоколи. P4 дава възможност за динамично управление на потоците от данни, като дефинира как мрежовите пакети трябва да бъдат обработвани, анализирани и пренасочвани на различни мрежови слоеве.

Ключов аспект на внедряването на P4 в реални мрежови среди е съвместимостта с различни хардуерни платформи. Тези платформи обхващат широк спектър от технологии, включително ASIC (Application-specific Integrated Circuits), NPU (Network Processing Units), FPGA (Field-Programmable Gate Arrays), SmartNIC и софтуерни симулатори [5,6,7,8,9].

Всяка от тези архитектури има свои уникални характеристики, които ги правят подходяща за различни приложения. За пример може да се посочи ASIC прототип като Intel Tofino, който предлага висока производителност и ниска латентност, докато FPGA устройствата осигуряват гъвкавост и възможност за ре-конфигуриране на логиката на мрежовия процесор в реално време.

Възможността за интеграция на P4 с тези хардуерни архитектури дава предимства като оптимизирана производителност, лесна адаптация към нови мрежови изисквания и висока ефективност в управлението на мрежовия трафик.

Това прави P4 съществен компонент в модерните програмируеми мрежови архитектури, способен да се справи с нарастващите нужди на съвременните комуникационни системи.

# 2 Обща архитектура на P4.

Общата архитектура на P4 включва различни нива на обработка на пакети и ключови компоненти, които участват в този процес. Основните компоненти на процеса са разбор (parsing), входна обработка на данни (входен конвейер), изходна обработка на данни (изходен конвейер) и обратен разбор (de-parsing), като всяка стъпка може да бъде персонализирана спрямо нуждите на конкретното мрежово приложение (фиг. 1.) [10, 11].

P4 архитектурата се състои от няколко ключови компонента:

*Входен конвейер (Ingress Pipeline*):

- Разбор (parser): Първата стъпка е извличането на заглавките на пакета, наричана разбор. Разборчикът преобразува суровия поток от данни в заглавки на ниво слой 2, 3 и нагоре, например Ethernet, IPv4, TCP и др.
- Обработка на таблици: След разбор, входният конвейер изпълнява различни действия, базирани на намерени съвпадение в таблиците (match-action). Това могат да бъдат операции като предаване, филтриране или промяна на съдържание на заглавка на пакет, например модификация на IP адреса.

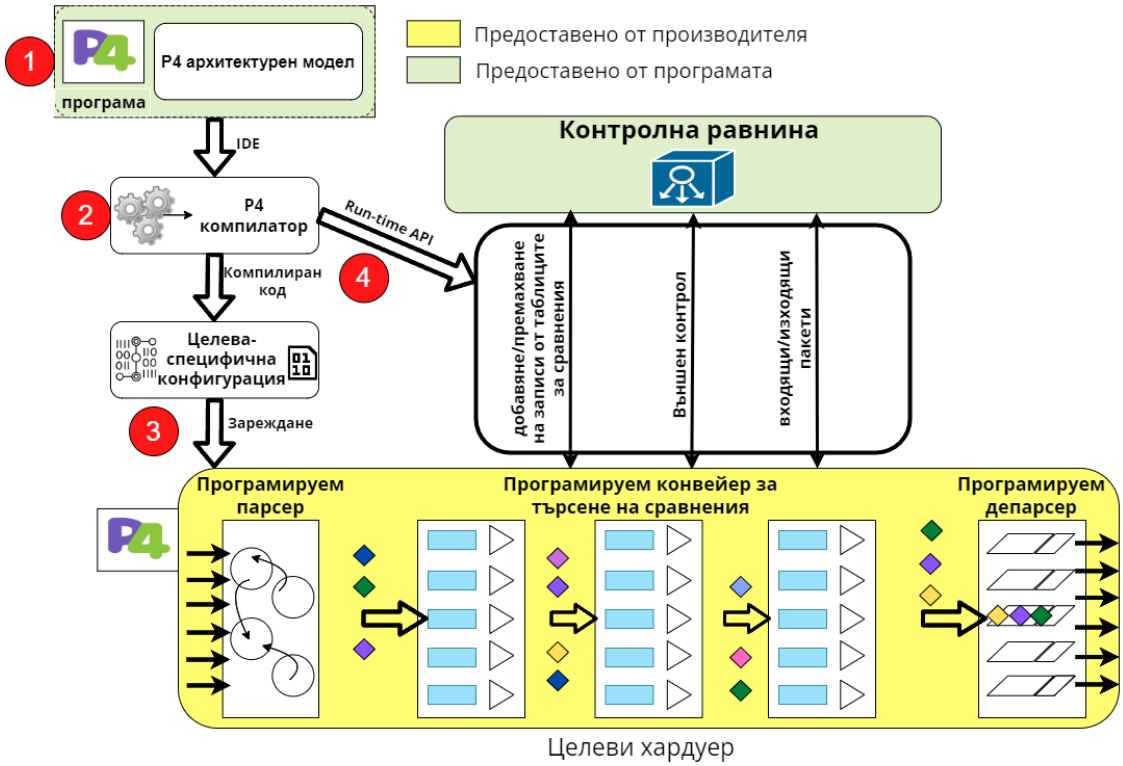
*Изходен конвейер (Egress Pipeline):*

- Обработка на таблици: Подобно на входния конвейер, тук се извършват действия на базата на намерени съвпадения в таблиците. Изходният конвейер може да определи как да се изпратят пакетите въз основа на допълнителна логика.
- Обратен разбор (deparser): След приключване на обработката, заглавките на пакетите се преобразуват отново в суров поток от битове, за да бъдат изпратени към следващата си дестинация.

*Контролна равнина (Control plane):* Контролната равнина е отговорна за управление и конфигуриране на таблици в предаващата равнина. Това обикновено се изпълнява от SDN

контролер или друга управляваща система. Тя е отговорна за вписване на правила в таблиците, като например съвпадения и действия за специфични пакети.

*Предаваща равнина (Data plane):* Това е равнината, която обработва пакетите според P4 програмата. Поточният план се състои от входни и изходни конвейери, които извършват реални действия върху пакетите според намерените съвпадения.




**Фиг. 1.** Обща архитектура на P4

## 3 Хардуерни спецификации и изисквания.

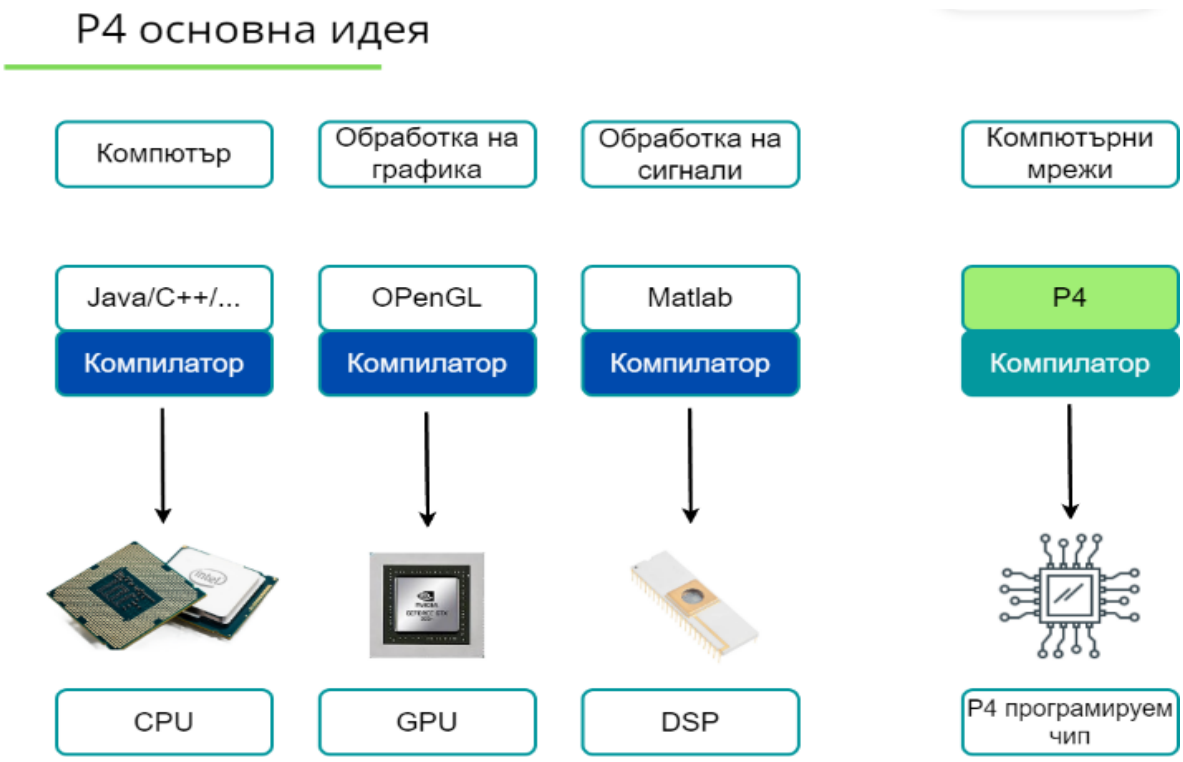
Основната идея за разработване на специфичен мрежов хардуер е възможността за изпълнение на специфични задачи като приемане, обработване и предаване на пакети. Причината за това е нуждата за постигане на все по-високи глобални и локални скорости, която довежда до създаване на специализирани мрежов хардуер, като SmartNIC, FGPA (Field Programmable Field Array) и по специално ASIC (Application-specific Integrated Circuit). Този тип хардуер е съпоставим с други хардуерни решения при различни сценарии, но с еднакво предназначение (фиг. 2.) [10].

За да се имплементират програми на P4, се изисква хардуерните устройства да поддържат програмируема обработка на мрежови пакети и да са съвместими с P4 компилатора. Основната идея на P4 е да осигури гъвкавост в обработката на мрежови пакети, което означава, че хардуерните платформи трябва да бъдат достатъчно мощни и гъвкави, за да могат да изпълняват специфични задачи по разбор и обработка на пакетите според P4 кода. Основните изисквания и хардуерни спецификации [1, 2], които устройствата трябва да покриват, за да изпълняват P4 програми са:

– Програмируеми таблици за съвпадения (Match-action Units): Устройствата трябва да имат таблици за съвпадение и действия (Match-action tables), които могат да се програмират от P4 програмата. Тези таблици служат за съпоставяне на

определени полета в пакета например IP адреси с предварително дефинирани действия, например предаване или промяна на съдържание на заглавката на пакета.

– Програмируеми (гъвкави) разбори: Устройствата трябва да могат да извършват разбор, разбиват пакетите на отделни полета според това, което е дефинирано в P4 кода. Този разбор трябва да бъде програмируем, за да може да се поддържат както стандартни протоколи (напр. Ethernet, IP), така и нови и собствени мрежови заглавки.
– Програмируеми елементи за обработка на пакети: Устройствата трябва да имат възможност да променят, добавят или премахват полета в мрежовите пакети, което се дефинира в P4 кода. Това е важно за функции като например тунелиране (encapsulation), декриптиране или транслиране (NAT - name address translation) на адреси.
– Поддръжка на P4 компилатор: Устройствата трябва да са съвместими с P4 компилатора, което превежда P4 програмите от високо ниво в машинен код-специфични инструкции за целевия хардуер. Компилаторът също така трябва да поддържа специфични цели (target platforms), като например ASIC, FPGA, или NIC.
– Висока пропускателна способност: Хардуерът трябва да поддържа висока пропускателна способност, особено за сценарии с голям обем трафик, като например центрове за данни или интернет доставчици. Платформите с висока скорост на пренос на данни, например 100Gbps или повече, са предпочитани за внедряване на P4 решения.




**Фиг. 2.** P4 хардуер основна идея

FPGA, ASIC или SmartNIC платформи с програмируема логика: Те са основните типове хардуер, които поддържат P4 програми. FPGA осигуряват гъвкавост и могат да бъдат препрограмирани за различни задачи, докато ASIC чиповете са по-бързи, но не толкова гъвкави. Важно е чипът да бъде проектиран с поддръжка на мрежова програмируемост, като например използване на P4 компилатор.

P4, първоначално е проектиран за програмируеми комутатори особено за ASIC. Понастоящем вече се разширява с възможност да изпълнява различни мрежови функции. В тези случи терминът "цел" в P4 се използва за обозначаване на целевото програмируемо мрежово устройство.

P4 съвместимите мрежови устройства обикновено включват контролна равнина и предаващата равнина а данни. P4 е проектиран да се използва за програмиране на предаващата равнина на целевото мрежово устройство.

### 3.1. **SmartNIC**

SmartNIC или Smart NIC за P4 е мрежова карта, която поддържа програмируема обработка на мрежови пакети, базирана на P4. Тези карти позволяват на разработчиците и администраторите да персонализират мрежовата логика, като дефинират как да се обработват пакетите в самата мрежова карта, подобно на програмируеми комутатори и рутери.

Чрез използването на P4 NIC, мрежовите функции като предаване, филтриране, мониторинг или други специфични задачи могат да се реализират директно на тях, без да се налага пакетите да преминават през операционната система или други компоненти. Това осигурява по-висока производителност и ниска латентност, като елиминира допълнителната софтуерна обработка [7, 8].

Основни предимства и недостатъци на SmartNIC за P4:

*Основни предимства:*

- Програмируема обработка на пакети: Мрежовата карта може да бъде конфигурирана да изпълнява специфични P4 програми за обработка на мрежови пакети, което позволява внедряване на персонализирани мрежови функции.
- Ниска латентност: Тъй като обработката на пакети се извършва директно на хардуера, латентността се намалява значително в сравнение със стандартните софтуерни решения.
- Офлайн обработка: Много от мрежовите задачи могат да се обработват без да се натоварва главния процесор, което освобождава ресурси за други задачи.

*Основни недостатъци:*

- Сложност при програмиране и поддръжка: Изисква се висока експертиза и персонал с добри познания за мрежовите протоколи, езика P4 и специфичните мрежови хардуерни платформи. Налице е висока степен на сложност при отстраняване на грешки поради липсата на инструменти за тяхното откриване и диагностика, приложими на хардуерно ниво.
- Ограничена програмируема функционалност: Въпреки че SmartNIC за P4 са програмируеми, тяхната архитектура е все пак ограничена от съответния хардуерен дизайн. Възможностите за обработка на пакети, броят на таблиците за съвпадение и действия (Match-action tables), както и поддържането на сложни функции могат да бъдат ограничени от капацитета на хардуера. Това се дължи и на ограничения капацитет на памет в която се разполагат тези таблици за съвпадения.

- Висока цена на хардуера: SmartNIC картите, които поддържат P4, обикновено са по-скъпи от традиционните NIC. Това може да бъде бариера за по-малки организации или при внедряване в по-мащабни среди, където са необходими много карти, като например центрове за данни.
- Адаптиране към специфичен хардуер: Тъй като P4 програмите са често специфични за хардуера и преминаването към друг тип мрежова хардуерна платформа, например от един производител на друг, може да изисква значителни усилия за преработка на кода.
- Зависимост от конкретни доставчици: Възможно е доставчиците, поддържащи P4, да са специфични за отделни производители и да са ограничени в тяхната логистична система. Това може да наложи използването на специфичен софтуер и драйвер, което ограничава гъвкавостта и възможността за интеграция с други технологии.

### 3.2. **FPGA.**

FPGA е вид хардуерна платформа, която може да бъде програмирана, за да изпълнява различни цифрови функции, включително обработка на мрежови пакети. FPGA се използва широко за имплементация на P4 програми, тъй като позволява гъвкавост при дефиниране на начина, по който мрежовите пакети се обработват и препращат [6, 9].

В контекста на P4, FPGA играят важна роля, като програмируеми мрежови процесори, които могат да изпълняват инструкции от P4 програмата. Те предлагат висока производителност и ниска латентност, като същевременно позволяват на потребителите да дефинират собствени мрежови протоколи и политики за обработка на трафика.

Основни предимства и недостатъци на FPGA за P4:

*Основни предимства:*

- Програмируема логика: Позволява имплементиране на специфични P4 функционалности, които могат да бъдат променяни или актуализирани чрез софтуерна програма.
- Висока производителност: FPGA може да осигури много висока пропускателна способност, което ги прави подходящи за мрежови приложения с големи изисквания към производителността.
- Гъвкавост: За разлика от ASIC с фиксиран разбор, FPGA може да бъде препрограмиран за различни задачи и обработка на различни мрежови заглавки, което го прави идеален за внедряване на P4 програми

*Основни недостатъци:*

- FPGA осигуряват много гъвкавост на дизайна, но в същото време могат да бъдат много скъпи за разработване и поддръжка. Те не са създадени за конкретна задача и трябва да се препрограмират за всяка нова задача.
- FPGA също имат малко или никаква вградена памет, което изисква други компоненти за осигуряване на достъп до паметта.

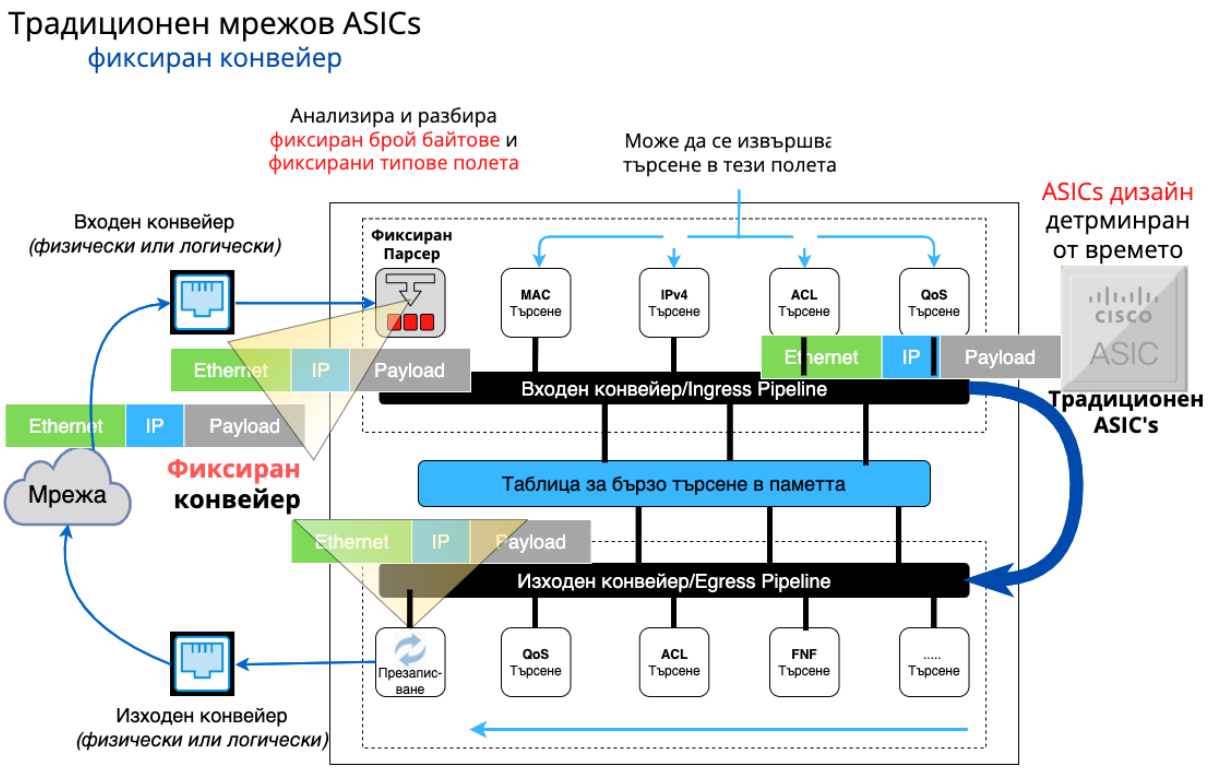
Тези ограничения обикновено пренасочват FPGA към „специална“ роля в повечето мрежови устройства. FPGA често се използват за разширяване на други ASIC, за „една допълнителна функция“, която основният процесор няма.

### 3.3. **ASIC.**

ASIC е вид интегрална схема, която е проектирана за изпълнение на специфична задача или приложение, а не за общо предназначение. В контекста на компютърните мрежи,

ASIC чиповете често се използват за оптимизиране на мрежовата производителност и за обработка на специфични мрежови функции. Те са интегрирани в различни мрежови устройства като маршрутизатори, комутатори и други, за да ускорят обработката на пакети и да осигурят висока производителност при изпълнение на задачи като маршрутизиране на пакети, управление на трафика, мрежова защита и други. Традиционните ASIC се използват от дълго време в мрежовите устройства, но с разработването на програмируеми такива те вече могат да се разделят на две категории ASIC с фиксиран разбор и ASIC с гъвкав разбор.

ASIC с фиксиран разбор са мрежови чипове, които имат предварително зададена архитектура за разбор на мрежови пакети. Разборът в тези чипове е закодиран в хардуера и може да обработва само определени пре-дефинирани мрежови протоколи и структури на пакети. Тъй като архитектурата е фиксирана, тези ASIC не могат да се адаптират към нови или „собствени“ мрежови протоколи (фиг. 3.) [4].

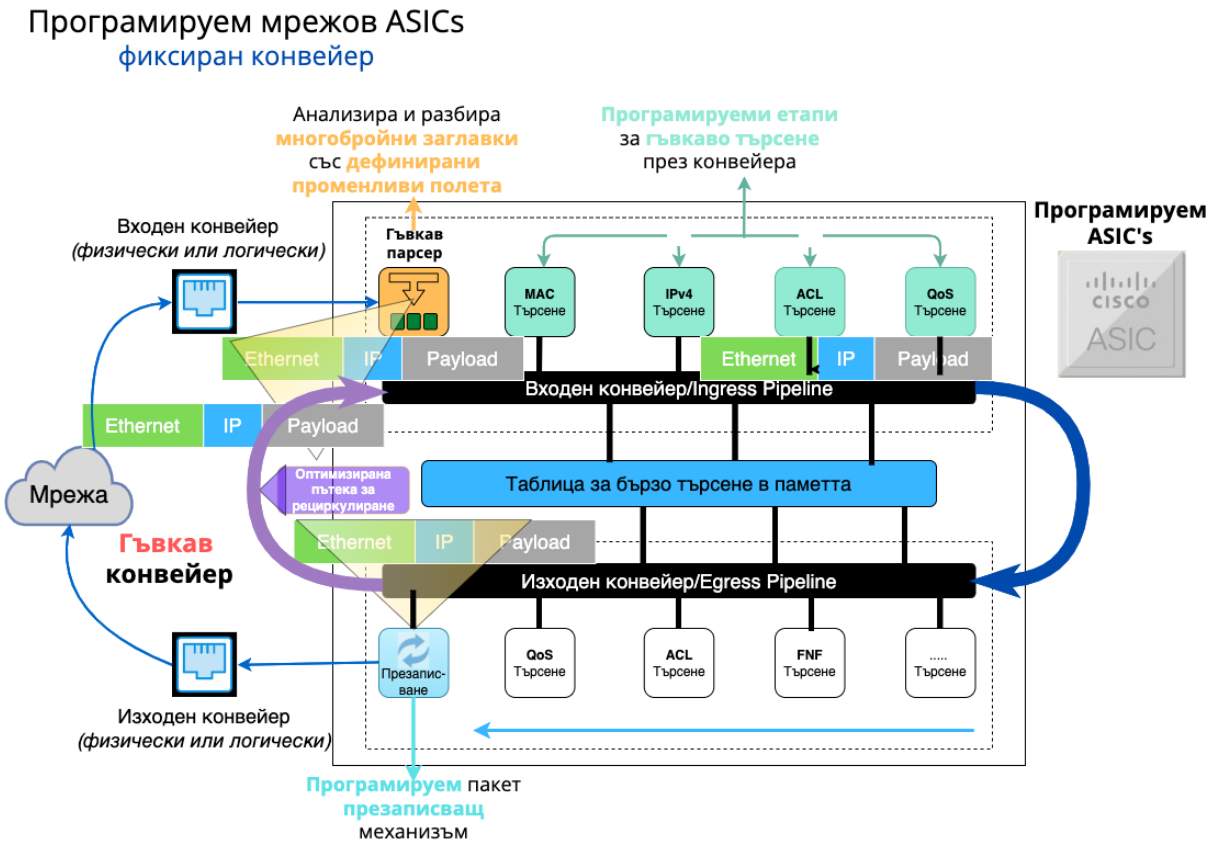



**Фиг. 3.** Традиционен мрежов ASIC с фиксиран разбор

ASIC с гъвкав разбор предлагат възможност за програмируем разбор на пакети, което позволява на мрежовите инженери да дефинират протоколи и структури на пакети, които да бъдат обработвани. Тези чипове позволяват на потребителите да задават нови правила за разбор чрез програмиране, което ги прави много по-адаптивни към нови протоколи или специфични нужди на мрежовата инфраструктура (фиг. 4.) [4, 5]. Пример за това може да се посочи протоколът VLANX, който беше създаден за нуждите на центровете за данни и първоначално беше внедрен само, в софтуерните комутатори поради невъзможността на хардуерните платформи с фиксиран парсер да обработват тези пакети.

Фиксираният разбор изисква хардуерно модифициране за разпознаване на новия формат на пакети, докато устройство с гъвкав парсер и P4 поддръжка може да бъде

препрограмиран с нов P4 код, който може да направи разбор на даден протокол със съответната логика за обработка.




**Фиг. 4.** Програмируем мрежов ASIC с гъвкав парсер

## 4 Заключение

Възходът на програмируемите мрежови архитектури, базирани на P4, бележи значителна промяна в начините, по които мрежовите устройства се проектират и управляват. Съвместимостта на P4 с различни хардуерни платформи, като ASIC, NPU, FPGA и софтуерни симулатори, предоставя нови възможности за гъвкавост и адаптивност в мрежовите среди. Всяка от тези платформи предлага уникален баланс между производителност, латентност, гъвкавост и програмируемост, което позволява на мрежовите оператори и разработчици да избират най-подходящата за своите специфични нужди.

**ЛИТЕРАТУРА:**

[1] P4. Official site. October 06, 2024 Available from: https://p4.org.

[2] P4. Official site. October 10, 2024 Available from: https://p4.org/p4-spec/docs/P4-16-v1.2.4.pdf.

[3] P4. Official site. October 10, 2024 Available from: https://p4.org/ecosystem/.

[4] Cisco. Official site. October 14, 2024 Available from: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2022/pdf/BRKARC-2091.pdf.

[5] ONF. P4_16 programming for intel Tofino using Intel P4 Studio. October 17, 2024. Available from: https://opennetworking.org/wp-content/uploads/2021/05/2021-P4-WS-Vladimir-Gurevich-Slides.pdf.

[6] AMD. Xlinx UltraScale+. October 17, 2024. Available from: https://www.amd.com/en/products/adaptive-socs-and-fpgas/fpga/virtex-ultrascale-plus.html.

[7] Netronome. Netronome Agilio. October 17, 2024. Available from: https://netronome.com/agilio-smartnics/.

[8] Nvidia. Nvidia Bluefield. October 17, 2024. Available from: https://www.nvidia.com/en-us/networking/products/data-processing-unit/.

[9] Intel. Intel FGPA (Altera). October 17, 2024. Available from: https://www.nvidia.com/en-us/networking/products/data-processing-unit/.

[10] Github. P4language. October 17, 2024 Available from: https://github.com/p4lang.

# EXPLORING ARTIFICIAL INTELLIGENCE MACHINE LEARNING IN VIDEO SURVEILLANCE*

**SILVIA H. NIKOLOVA**

***ABSTRACT:*** *Artificial intelligence (AI) and machine learning have revolutionized the field of video surveillance, making it more effective and efficient than ever before. With the ability to analyze large amounts of video data in real time, these technologies have greatly improved the capabilities of surveillance systems in identifying and responding to potential threats. This report will explore the role of AI and machine learning in real-world video surveillance, discussing their advantages, challenges and disadvantages. One of the main benefits of using AI for security with video cameras is the ability to detect and identify potential threats or suspicious activity. Through advanced algorithms, AI systems can recognize patterns and anomalies in footage, enabling immediate response and intervention when needed. This proactive approach to security is essential to preventing incidents before they escalate, ultimately ensuring the safety of people and property.*

***KEYWORDS:*** *artificial intelligence, machine learning, video surveillance, security systems*

***DOI: https://doi.org/10.46687/NBDO1689***

# ИЗСЛЕДВАНЕ НА МАШИННО ОБУЧЕНИЕ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ВЪВ ВИДЕОНАБЛЮДЕНИЕТО

**СИЛВИЯ Х. НИКОЛОВА**

***АБСТРАКТ:*** *Изкуственият интелект (AI) и машинното обучение революционизираха областта на видеонаблюдението, правейки го по-ефективно и ефикасно от всякога. Със способността да анализират огромно количество видео данни в реално време, тези технологии значително подобриха възможностите на системите за наблюдение при идентифициране и реагиране на потенциални заплахи. Този доклад изследва ролята на AI и машинното обучение във реално видеонаблюдение, обсъждайки техните предимства, предизвикателства и недостатъци. Едно от основните предимства на използването на AI за сигурност с видеокамери е способността му да открива и идентифицира потенциални заплахи или подозрителни дейности. Чрез усъвършенствани алгоритми системите с изкуствен интелект могат да разпознават модели и аномалии в кадрите, което позволява незабавна реакция и намеса, когато е необходимо. Този проактивен подход към сигурността е от съществено значение за предотвратяване на инциденти, преди те да ескалират, като в крайна сметка гарантира безопасността на хората и имуществото.*

## 1 Въведение

Изкуственият интелект (AI) се очертава като мощна технология с потенциала да революционизира много аспекти на човешкото общество. Пресечната точка на устойчивото развитие и изкуствения интелект предоставя както възможности, така и много предизвикателства за бъдещето.

От една страна, изкуственият интелект има потенциала да помогне за постигане на устойчиво развитие чрез подобряване на ефективността, намаляване на разходите и позволяване на по-информирано вземане на решения. Например AI може да оптимизира потреблението на енергия в сградите, да подобри селскостопанската производителност и да

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

подпомогне усилията за реагиране при бедствия и заплахи за сигурността на обекти и хора, например чрез видеонаблюдение [1]. Изкуственият интелект може да бъде обучен да изпълнява конкретни задачи свързани с охраната и сигурността, да анализира и взема решения за огромен обем от данни за много кратко време. Тази „настройка“ може да се осъществи чрез машинно обучение.

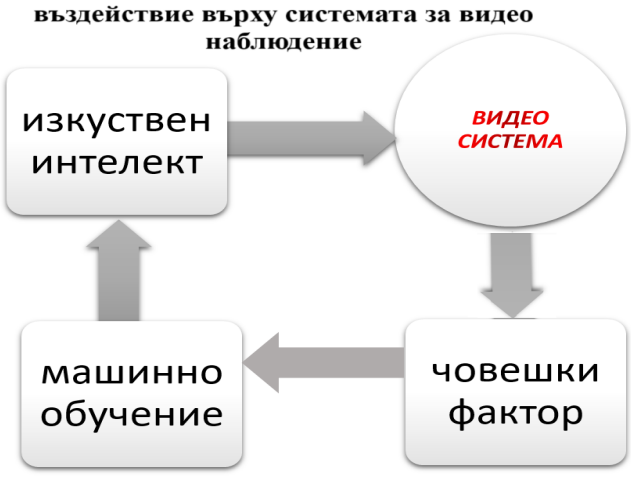
Машинното обучение е област, която привлича много внимание през последните години, особено с възхода на технологиите за изкуствен интелект. Една от областите, в които машинното обучение прави значителни крачки, е в областта на видеонаблюдението. Видеонаблюдението е ключов инструмент за поддържане на сигурността и наблюдение на дейности в обществени пространства, домове и предприятия. С помощта на алгоритми за машинно обучение системите за видеонаблюдение вече могат да обработват големи количества видео данни, да откриват и проследяват обекти и дори да предсказват потенциални заплахи или инциденти [2].

Този доклад изследва ролята на машинното обучение на AI във реално видеонаблюдение, обсъждайки предимства, предизвикателства и недостатъци.

## 2 Същност на машинното обучение

Едно от ключовите предимства на използването на машинно обучение във видеонаблюдението е възможността за автоматизиране на анализа на големи количества видео данни. Традиционно служителите по сигурността трябва ръчно да преглеждат часове видеозаписи, за да идентифицират подозрителни дейности или инциденти [3]. Този процес може да бъде значително ускорен, което позволява вниманието да се съсредоточи върху по-критични задачи. Също така се намаляват шансовете за човешка грешка и пропуск и се гарантира, че потенциалните заплахи няма да бъдат пропуснати.

Алгоритмите за машинно обучение могат също да бъдат обучени да откриват конкретни обекти или поведение във видеозаписи, като неупълномощени лица, оръжия или необичайни дейности. Тези алгоритми могат да бъдат обучени с помощта на големи набори от данни с етикетирани видео данни, което им позволява да се научат да разпознават модели и аномалии във видеозаписа. Чрез непрекъснато подобряване на тяхната производителност чрез обратна връзка от персонала по сигурността, тези алгоритми могат да станат много точни при идентифицирането на потенциални заплахи в реално време (фиг. 1). [3, 6]




**Фиг. 1.** Въздействие чрез машинно обучение




**Фиг. 2.** Генерирани аларми от различни датчици

## 3 Предимства и недостатъци на машинното обучение

Алгоритмите за машинно обучение могат да се използват и за подобряване на цялостната ефективност на системите за видеонаблюдение. Чрез автоматично филтриране на неподходящи видеозаписи и фокусиране върху области на интерес, тези алгоритми могат да помогнат за намаляване на натоварването на персонала по сигурността и да им позволят да реагират по-ефективно на потенциални заплахи. Освен това, алгоритмите за машинно обучение могат да бъдат интегрирани с други технологии, като лицево разпознаване или разпознаване на регистрационен номер, за да подобрят допълнително възможностите на системите за видеонаблюдение. В сравнение с други методи за охрана (различни по тип датчици за движение), видеокамерите с AI генерират много по-малък брой фалшиви сработвания, а след обучение те се свеждат до нула/ фиг.2/.

Въпреки многобройните предимства от използването на машинно обучение във видеонаблюдението, има и предизвикателства и ограничения, които трябва да бъдат разгледани. Едно от основните предизвикателства е необходимостта от големи и разнообразни набори от данни за ефективно обучение на алгоритми за машинно обучение. Събирането и етикетирането на такива набори от данни може да отнеме много време и ресурси, особено за редки или сложни заплахи за сигурността. Освен това осигуряването на точността и надеждността на алгоритмите за машинно обучение в сценарии от реалния свят е от решаващо значение за предотвратяване на фалшиви положителни и отрицателни резултати, които биха могли да подкопаят ефективността на системите за видеонаблюдение.

Друго предизвикателство при използването на машинно обучение във видеонаблюдението е потенциалът за поверителност и етични проблеми. Със способността да анализират и интерпретират видео данни, алгоритмите за машинно обучение могат да

нахлуят в поверителността на хората и да нахлуят в личното им пространство [5]. От съществено значение е да се установят ясни насоки и разпоредби относно използването на машинно обучение във видеонаблюдението, за да се защитят правата на хората и да се гарантира, че технологията се използва отговорно и етично.

# 4 Резултати

Емпиричното изследване е извършено чрез изследване и анализ на данни от роботизирана система за охрана с видеонаблюдение ТЕДИ [8], в продължение на една седмица, въвеждайки непрекъсната корекция на зададените първоначални параметри чрез машинно обучение.

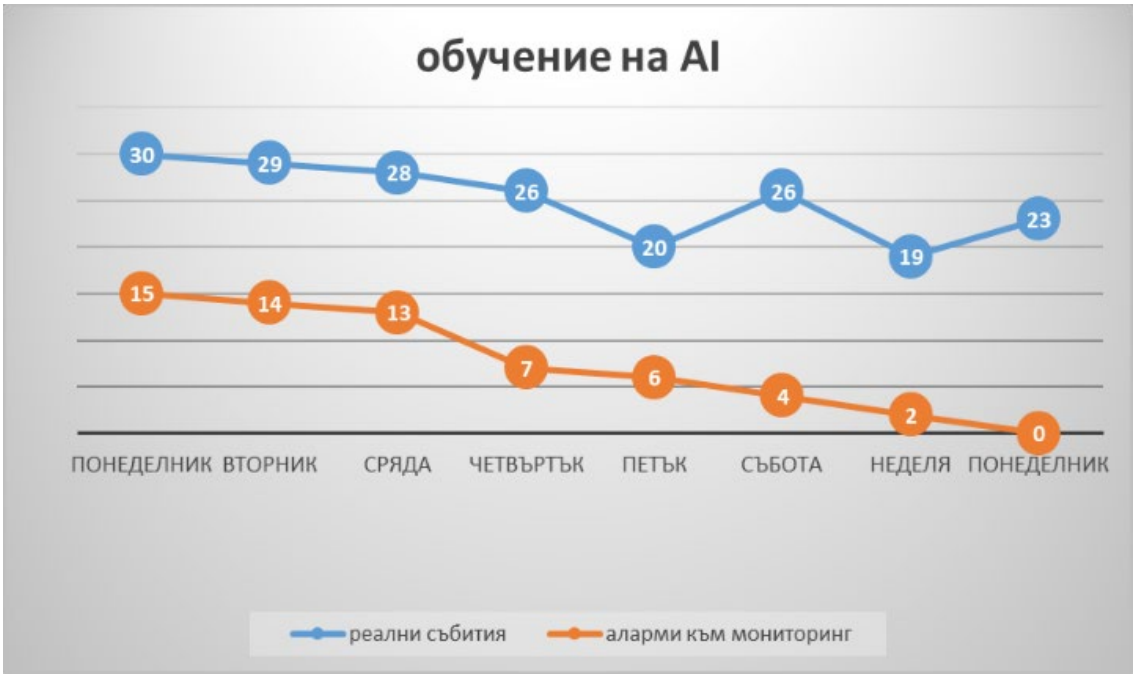
Системата работи в реални условия, като въздействието на външните климатични фактори е непредвидимо, но пренебрежимо малко, поради което не е отчетено в резултатите. През целия период на изследване се регистрират движенията на животни, птици, превозни средства и хора през охранявана от камерите зона.

В началото на изследването се забелязват високи стойности на генерираните от камерата сигнали. Нейните алгоритми засичат всяко движение в зоната съгласно производствените й параметри /фиг.3/. Коригирането на данните с машинното обучение се извършва веднъж дневно след пълен анализ на предходните събития. Целта на корекциите е да „посочи“ на AI некоректните сигнали и да намали броя на фалшивите сработвания. Човешкият фактор се свежда до промяна на данните в машинното обучение. Веднъж получила новите нареждания камерата сама коригира изходните данни /фиг. 4/.

В изследването са включени усреднените стойности от няколко типа камери, използващи AI – за движение, за проследяване на обекти и камери с термо анализ [4].




**Фиг. 3.** Брой алармени събития по дни




**Фиг. 4.** Редуциране броя на изходни сигнали след МО

Резултатите от изследването напълно и еднозначно доказват ползите от машинното обучение на изкуствения интелект във видеокамерите. За кратък период от време ефективността на използваните камери нараства експоненциално. Намесата на човешкия елемент под формата на корекции е краен брой пъти и не изисква непрекъснато следене на крайните параметри. AI се само обучава след като бъде научен как.

Броят на външните въздействия под вид на реални алармени събития остава приблизително постоянен през изследвания период, като броят на генерираните от камерите аларми към центъра за мониторинг и реакция в края на обучението клони към нула.

Изкуственият интелект (AI) и машинното обучение революционизират областта на видеонаблюдението, правейки го по-ефективно и ефикасно от всякога [9].

## 5 Заключение

Алгоритмите за машинно обучение могат непрекъснато да се обучават и подобряват с течение на времето, което ги прави по-ефективни и надеждни при откриване на заплахи за сигурността. Чрез анализиране на данни от минали инциденти и идентифициране на общи модели, AI системите могат по-добре да предвиждат и реагират на подобни ситуации в бъдеще. Тази адаптивност и способност за обучение на AI го правят ценен актив за подобряване на протоколите за сигурност.

В допълнение към откриването на заплахи, управляваните с изкуствен интелект системи за сигурност могат също така да рационализират процеса на наблюдение и охрана. Чрез автоматизиране на определени задачи, като проследяване на подозрителни дейности или наблюдение на множество зони едновременно, AI може да освободи човешкия персонал по сигурността да се заеме с по-критични задачи. Това не само подобрява цялостната ефективност на действията по сигурността, но също така намалява риска от човешка грешка в системите за сигурност. [7, 10]

**ЛИТЕРАТУРА:**

[1] Бурка, Дж. (Август 9, 2023). Ролята на AI и Big Data в подобряване на устойчивостта. https://constructive-voices.com/the-role-of-ai-and-big-data-in-enhancing-construction-sustainability/

[2] Лалев, Хр. (2008). Системи за видеонаблюдение. Троян. ВТС

[3] Милушев, Л. (2023). Сигурност и защита на обекти с масово пребиваване на хора. София. Изток-Запад

[4] Перейра Ирухо Г. 2022 г. IRimage: софтуер с отворен код за обработка на изображения от инфрачервени термокамери. PeerJ Computer Science 8 : e977 https://doi.org/10.7717/peerj-cs.977

[5] Цанов, И. (2022). Изкуственият интелект в контекста на управлението и сигурността. София. е-книга

[6] Denev, D., Tsankov, Ts. Progress and trends in machine vision smart cameras. Scientific Conference with international participation MATTEH 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 116-124.

[7] Konstantinova, E., Tsankov, Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference “Ecology and environment”, 2021, ISSN 2367-5209, pp. 109-121.

[8] Nikolova, S. Design, development and research of process efficiency in a robotic intelligent security system “TEDI”. KNOWLEDGE – International Journal Scientific Papers, Vol. 63.3, Institute of Knowledge Management, Skopje, 2024, ISSN 2545-4439, pp. 289-295.

[9] https://izkustvenintelekt.bg/?p=1187

[10] Интелигентни технологии за видеонаблюдение. (2021). Извлечено на 10.09.2024г. от https://www.tech-dom.com/bg/inteligentni-tehnologii-za-videonablyudenie/2/2315/

# SOFTWARE PROCESSING OF AUDIO SIGNALS IN DIGITAL AUDIO WORKSTATION STUDIO ONE THROUGH EFFECT PLUGINS*

**DANIEL R. DENEV, ALEKSANDRA P. DOCHEVA**

***ABSTRACT:*** *This article aims to demonstrate the capabilities and uses of Studio One digital audio processing software. In addition, the essence of the mixing and mastering processes of audio signals through the use of software effect plug-ins will be considered.*

***KEYWORDS:*** *DAW, mixing, mastering, Studio One*

***DOI: https://doi.org/10.46687/UABM5644***

# СОФТУЕРНА ОБРАБОТКА НА АУДИО СИГНАЛИ В ЦИФРОВА АУДИО РАБОТНА СТАНЦИЯ STUDIO ONE ЧРЕЗ ЕФЕКТ ПРИСТАВКИ

**ДАНИЕЛ Р. ДЕНЕВ, АЛЕКСАНДРА П. ДОЧЕВА**

***АБСТРАКТ:*** *Настоящия доклад има за цел да покаже способностите и употребата на софтуера за цифрова обработка на сигнали Studio One. В допълнение ще се разгледа и същността на процесите смесване и мастериране при обработка на аудио сигнали чрез употребата на софтуерни ефект приставки.*

## 1 Въведение

PreSonus е американска компания, специализирана в разработката на хардуер и софтуер за създаване и обработка на цифрово аудио. Фирмата е известна с внедряването на иновативни технологии в аудио приложенията, VST инструментите и ефектите, които създава. Техният софтуер използва усъвършенствана технология, която позволява интеграцията му като VST инструмент в други хост програми за аудио обработка. Той е оптимизиран за редактиране на аудио и е особено подходящ за създаване на повтарящи се сегменти от звукови сигнали. [7,8]

Всеки проект в този софтуер може да включва неограничен брой инструменти и VST приставки, които могат да бъдат пренасочвани и свързвани с прозореца на миксера (Mixer) за допълнителна обработка и добавяне на ефекти.

Процесите на смесване и мастериране представляват два взаимосвързани процеса в звукообработката, с широко приложение в радиата и звукозаписните студия. Тези дейности играят ключова роля за подобряване на аудио качеството на музикални произведения, обработка на гласови записи, аудио продукция за киноиндустрията, реклами и други аудиовизуални продукти.

Смесването представлява процес, при който множество аудио сигнали (писти) се комбинират и обработват в софтуерна среда, наречена цифрова аудио работна станция (DAW). По време на този процес всеки аудио сигнал се разпределя по канали, където се регулират параметри като сила на звука, честотен спектър, динамика и панорамна позиция. Това става чрез използването на вградени софтуерни инструменти и ефекти (plug-ins), като

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

целта е да се постигне балансирано и ясно звучене на всички елементи. Основни инструменти, използвани при смесването, включват еквилайзери (EQ), които позволяват корекция на честотния диапазон, и компресори, които регулират динамичния диапазон на звуковите сигнали. Тези и други ефекти спомагат за създаването на хармонично съотношение между различните звукови елементи. Аудио сигналите могат да бъдат моно или стерео и често се групират в подканали, които се обработват колективно чрез настройките на ефектите, преди да бъдат свързани към главния канал (Master).

След като смесването е завършено, се преминава към мастериране, чиято основна цел е да осигури финалната обработка на аудиото. Мастерирането гарантира, че крайният продукт отговаря на индустриалните стандарти за качество по отношение на амплитуда, плътност, ширина на звуковия образ и динамика. Чрез този процес се оптимизира звуковият материал, за да бъде подходящ за комерсиална дистрибуция. [5]

Макар тези два процеса да могат да бъдат изпълнени и с помощта на хардуерни устройства, съвременните практики разчитат основно на софтуерни аудио ефекти (plug-ins). Тези софтуерни решения предлагат множество възможности за обработка с различни характеристики, приложими в различни етапи на смесването и мастерирането, адаптирани към специфични нужди и цели.

## 2 Цифрова аудио работна станция Studio One

Studio One е софтуер за цифрова аудио обработка, разработен от компанията PreSonus. Програмата е достъпна в няколко различни издания, включително: Studio One Express, Beginner Edition, Producer Edition, Signature Bundle и All Plugins Bundle. Примерен интерфейс на програмата е показан на фиг. 1.

Минималните системни изисквания за работа със Studio One включват: 32-битова версия на Windows 10, процесор с честота 2,0 GHz (Intel или AMD) с поддръжка на SSE2 инструкции, минимум 1 GB оперативна памет, както и 2 GB свободно дисково пространство. Видео картата трябва да поддържа минимална резолюция от 800 × 600 (Super VGA или по-добра). Звуковата карта трябва да бъде съвместима с DirectSound драйвер и ASIO/ASIO2 за аудио запис.

Препоръчителните системни изисквания включват: 64-битова версия на Windows 10, процесор с честота 4,0 GHz, 8 GB оперативна памет, както и 6 GB свободно пространство за съхранение, особено при инсталиране на допълнителни приставки и инструменти. Програмата използва Studio One ASIO, което осигурява ниска латентност и висока точност при комуникацията между софтуера и звуковата карта. [1, 6]

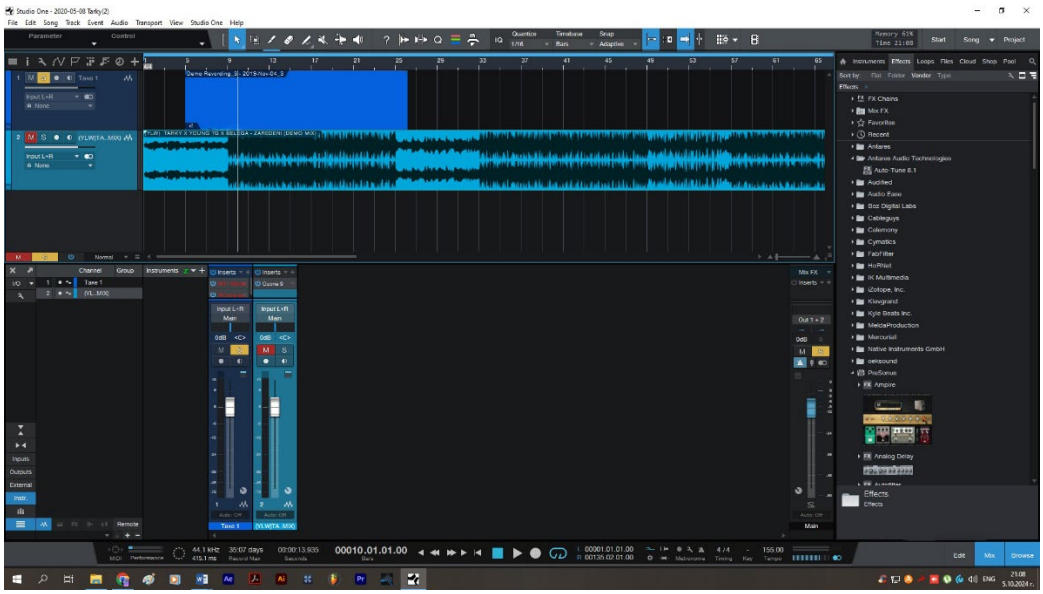
## 3 Настройка на параметри за аудио обработка

Панела за настройки от фиг. 2 служи за конфигуриране на параметрите и опциите на аудио устройството. В началото се настройва виртуалното аудио устройство, което се поддържа от компютъра, а след това и всички параметри. Параметрите включват: честота на дискретизация, качество на вземане на проба, дължина на буфера и битовата дълбочина.

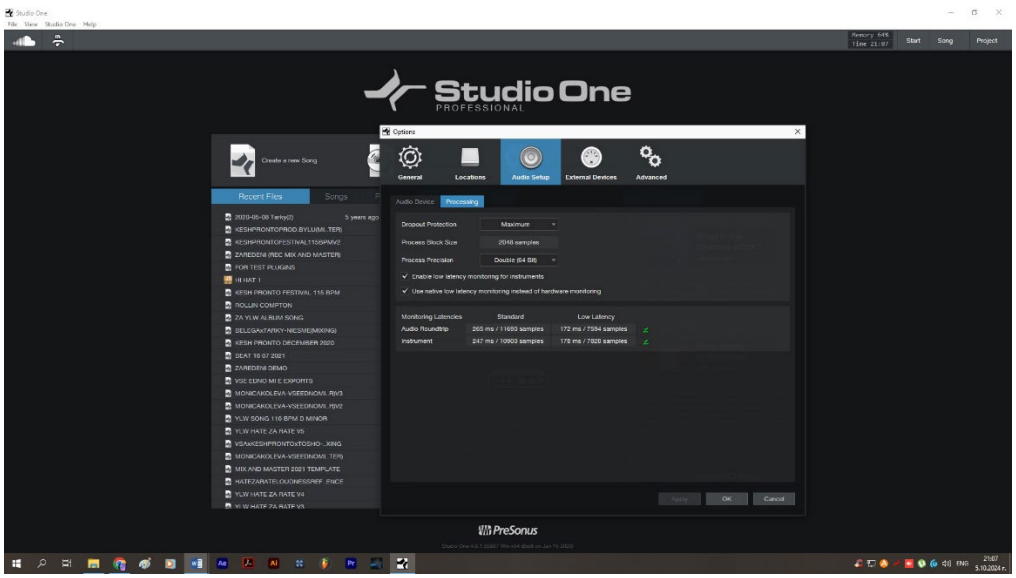
- Честотата на дискретизация (Sample rate) е средно аритметичен брой от проби получен за една секунда $fs = 1/T$. Тази величина служи за възпроизвеждане на по-реален и качествен звук.
- Качество на вземане на проба (Resampling quality) служи за подобрение на прецизността на обработващия се сигнал в процес на възпроизвеждане
- Дължина на буфера (Buffer Length) служи за запис на Audio или MIDI информация. При намаляване на дължината на буфера се установява по-малко закъснение при

запис в реално време, ако се увеличи дължината съответно и закъснението при възпроизвеждане ще нарасне.

- Битовата дълбочина (bit depth) е броя на битовете за информация за всяка проба от аудио сигнали. Практически този параметър отговаря за резолюцията на всяка проба от сигнала, като по този начин се задава качеството на звуковия сигнал.



**Фиг. 1.** Цифрова аудио работна станция Studio One 4




**Фиг. 2.** Конфигуриране на параметри за аудио обработка

## 4 Запис и корекция на аудио файлове, звуци и сигнали

Записването на аудио трак в Studio One се осъществява чрез натискане на бутона „Record“. Преди да започне записът, е необходимо потребителят да избере съответното входно устройство (например микрофон). Записаният звуков сигнал може да бъде запаметен в два формата: моно и стерео трак. Стерео тракът представлява метод за

възпроизвеждане на звук, при който се създава пространствено усещане за разпределение на звука, което симулира многопосочна звукова перспектива. В контраст, при моно трак звукът се възпроизвежда от единен източник, създавайки усещане за звукова изходна точка от една позиция. [2]

- **Ролята на приставката Melodyne в аудио обработката:**

Melodyne е мощен аудио редактор, който предоставя разнообразни инструменти за манипулиране и корекция на звукови сигнали и е показан на фиг.3. Основната му функция е да осигури подобрена визуална репрезентация на звуковите вълни, като визуализира и техния честотен спектър чрез спектрограма, която позволява наблюдение на честотните хармоники. Инструментите в Melodyne са разделени на две категории:

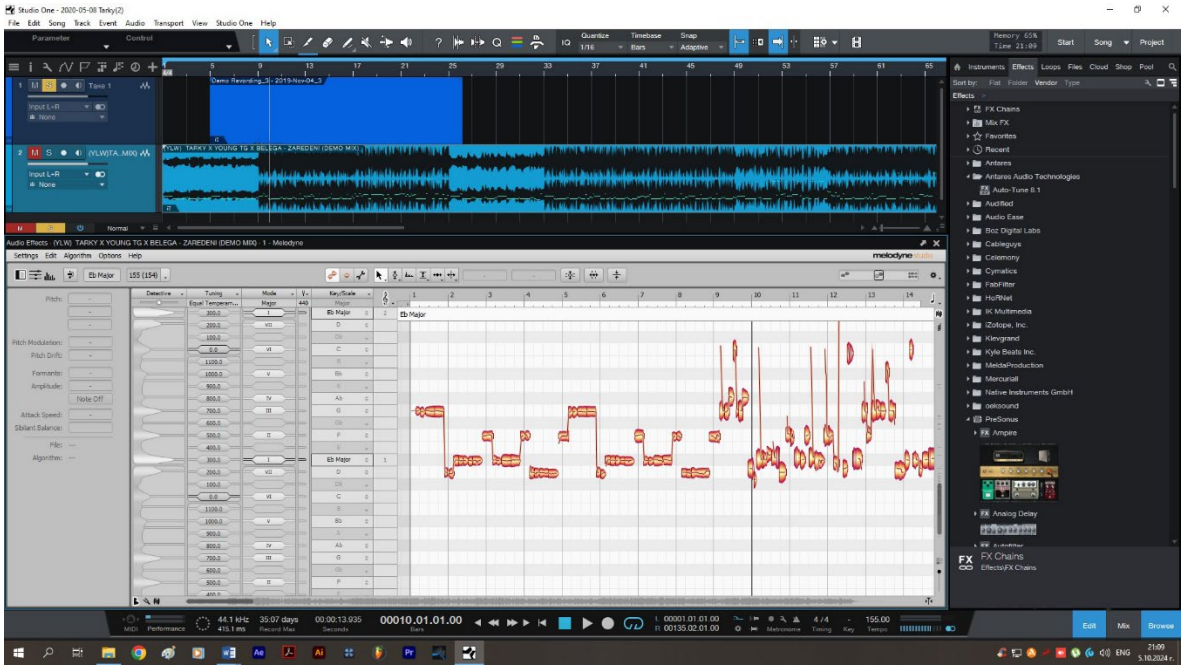
Ефектни инструменти:

- **Нормализиране на амплитудата**: Регулиране на амплитудата на сигнала до оптимални нива.
- **Шумоподтискане**: Премахване на нежелани шумове от записа.
- **Промяна на амплитудата**: Увеличаване или намаляване на амплитудата в избрани сегменти от сигнала.
- **Реверберация**: Добавяне на ефект на ехо, симулиращо акустичните характеристики на различни помещения.
- **Обръщане на сигнала**: Инвертиране на звуковия сигнал, създавайки обратен ефект.

**Музикални инструменти**:

- **Откриване на нотите:** Анализ на звуковия сигнал с цел разпознаване на използваната нотация.
- **Откриване на темпото:** Автоматично определяне на темпото на звуковия запис.
- **Запис и съхранение на аудио:** Позволява директен запис и запазване на аудио за последваща обработка.

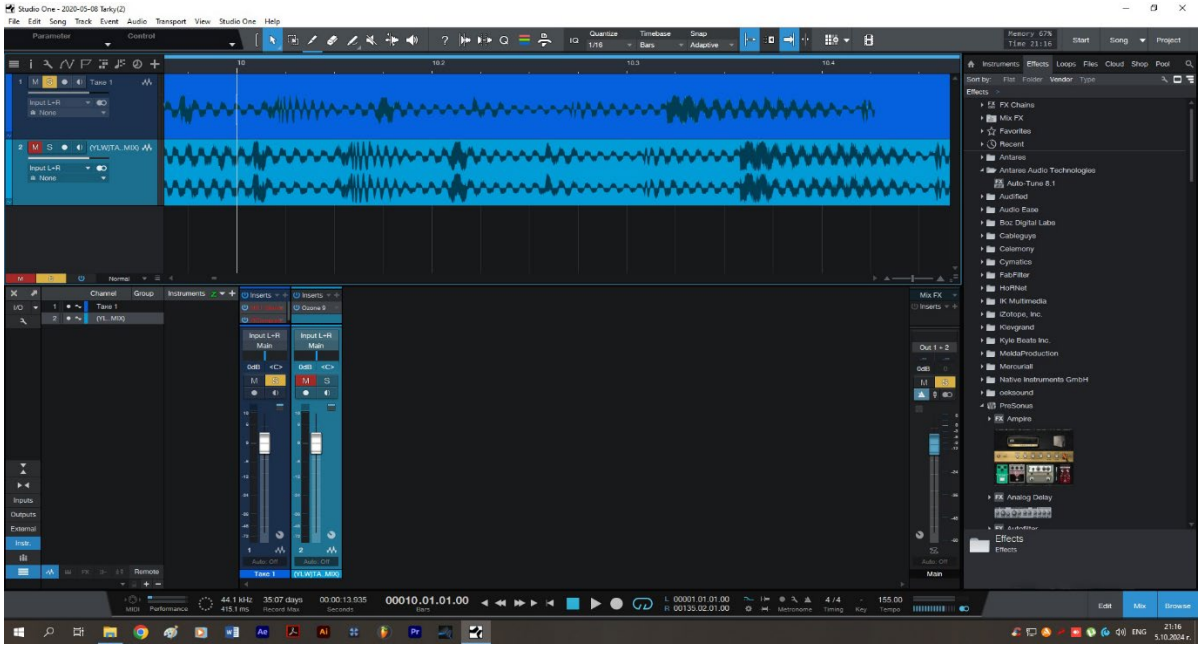
Тези функции правят Melodyne особено полезен инструмент както за технически анализ на звук, така и за творческа работа в областта на аудио и музикалната продукция.



**Фиг. 3.** Работа и корекция на моно и стерео писти

# 5 Смесване и обработка на аудио сигнали и файлове чрез ефект приставки

Аудио смесване е процес, при който множество звуци са комбинирани в един или повече канали. В този процес, нивото на обема на източника, честотното съдържание, динамика, и панорамна позиция се обработва цялостното смесване да звучи ясно и чисто. В процеса на смесване се използват ефект приставки чрез които се подобрява качеството на аудио сигнала, изчистват се ненужни честоти, увеличават се други. Могат да бъдат добавени ефекти като филтри, еквилайзери, компресори, ограничители и специални ефекти като Reverb, Delay, Chorus, Flanger. Процеса на смесване на сигнали е показан на фиг. 4. [4]

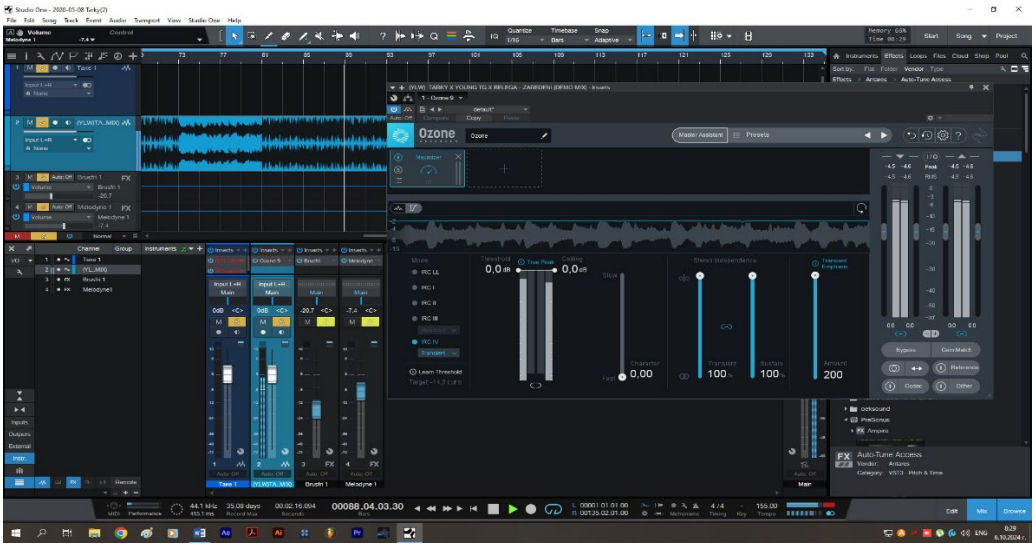


**Фиг. 4.** Процес по смесване на сигнали

# 6 Мастериране и обработка на аудио сигнали и файлове чрез ефект приставки

Мастерирането е финалният етап от аудио продукцията, при който готовото миксирано аудио се подготвя за разпространение на различни платформи. Целта на мастерирането е да се осигури последователност в качеството на звука, да се постигне максимална чистота, обем и баланс между отделните елементи в микса, и да се адаптира към изискванията на различни носители – като CD, стрийминг платформи или радио.

В този процес се използват различни ефект приставки, включително лимитери, компресори, еквалайзери и стерео-имиджери за да се постигне необходимия динамичен и честотен баланс. Лимитърът се прилага за контрол на пиковете, като по този начин се предотвратява изкривяване на сигнала при високи нива. Еквалайзерите се използват за финална корекция на честотния спектър, а стерео-имиджерите оптимизират пространственото разпределение на звука. Допълнително могат да бъдат добавени ефекти като мултибанд компресори за по-детайлно контролиране на динамиката в различните честотни диапазони. Мастерирането е от решаващо значение за постигане на професионално звучене и е показано на фиг. 5. [6]




**Фиг. 5.** Процес по мастериране на сигнали

# 7 Видове аудио ефект приставки

Софтуерните аудио ефектни приставки представляват програмни компоненти, които функционират в реално време, както самостоятелно, така и интегрирано с програми за аудио обработка и редактиране. Те се внедряват под формата на приставка и използват различни платформи като Virtual Studio Technology (VST), DirectX (DX), Real-Time Audio Suite (RTAS), AAX (Avid Audio eXtension), AU (Audio Units) и TDM (Time-Division Multiplexing). Различните типове приставки са съвместими с различни софтуерни приложения за аудио обработка. При процесите на смесване и мастериране на аудио сигнали се използват различни аудио ефекти, като еквилайзери, компресори, ограничители, както и специални ефекти като реверберация (reverb), закъснение (delay), филтри, стерео разширители (stereo imager), диесери (deesser), насищане (saturation), дисторшън (distortion), корус (chorus), фейзър (phaser) и фленгър (flanger). [3]

- **Честотен еквилайзер (фиг. 6)** – Този тип приставки контролират честотния спектър на сигнала, като позволява модифициране на честотното съдържание. Еквилайзерът може да премахва определени честотни диапазони, да усилва или намалява специфични честоти, като например намалява амплитудата на резонансните честоти и усилва други, с по-ниско ниво. Еквилайзерите се състоят от честотни ленти, които обхващат ниски, ниски средни, средни, високи средни и високи честоти. В зависимост от конкретния тип еквилайзер, броят на честотните ленти може да варира. Еквилайзерите се делят на три основни типа: графични, параметрични и параграфични. При графичните еквилайзери всяка честотна лента се регулира чрез плъзгачи, които визуално представят кривата на тон корекцията. Параметричните еквилайзери предлагат по-голяма гъвкавост, като позволяват регулиране на централната честота за всяка лента с отделен потенциометър. В някои параметрични еквилайзери е възможно и регулирането на Q-фактора, който определя ширината на честотната лента. Параграфичният еквилайзер е комбинация от графичен и параметричен. Еквилайзерите също се класифицират като линейни и нелинейни. Линейните еквилайзери запазват фазата на сигнала, докато при нелинейните се наблюдава фазово изместване на сигнала.



**Фиг. 6.** Софтуерна приставка - Честотен еквилайзер

- **Аудио компресор (фиг. 7)** – Тази приставка се използва за обработка на аудио сигнала чрез намаляване на амплитудата на по-силните звуци и усилване на по-тихите, като по този начин се намалява динамичният диапазон на сигнала. Основната цел на компресията е да направи динамиката на сигнала по-равномерна, като предотврати прекомерното усилване на пиковите стойности и намали контраста между най-силните и най-тихите звуци. Съществуват два основни типа компресори – стандартни и многообхватни (multiband). Стандартните компресират сигнала като цяло, докато многообхватните компресират отделно всяка честотна лента от спектъра, което позволява по-прецизен контрол върху различни честотни диапазони. Основните параметри на компресорите са следните:

➢ *Threshold (Праг): Определя нивото на амплитудата, при което компресорът се активира. Когато сигналът премине над зададената стойност, компресорът започва да намалява неговата амплитуда.*

➢ *Attack (Пристъп): Регулира колко бързо компресорът ще реагира, след като сигналът премине прага.*

➢ *Ratio (Съотношение): Определя степента на компресия, като указва колко пъти да се намали амплитудата на сигнала над прага. Например, съотношение 4:1 означава, че за всеки 4 децибела над прага сигналът ще бъде намален до 1 децибел.*

➢ *Sustain (Задържане): Определя колко дълго ще продължи компресирането след активирането на компресора.*

➢ *Release (Отпускане): Контролира времето, за което компресорът ще прекрати действието си, след като сигналът спадне под прага.*

➢ *Gain (Увеличаване): Позволява компенсиране на общата загуба в амплитуда, като усилва компресирания сигнал без да променя параметрите на компресията.*

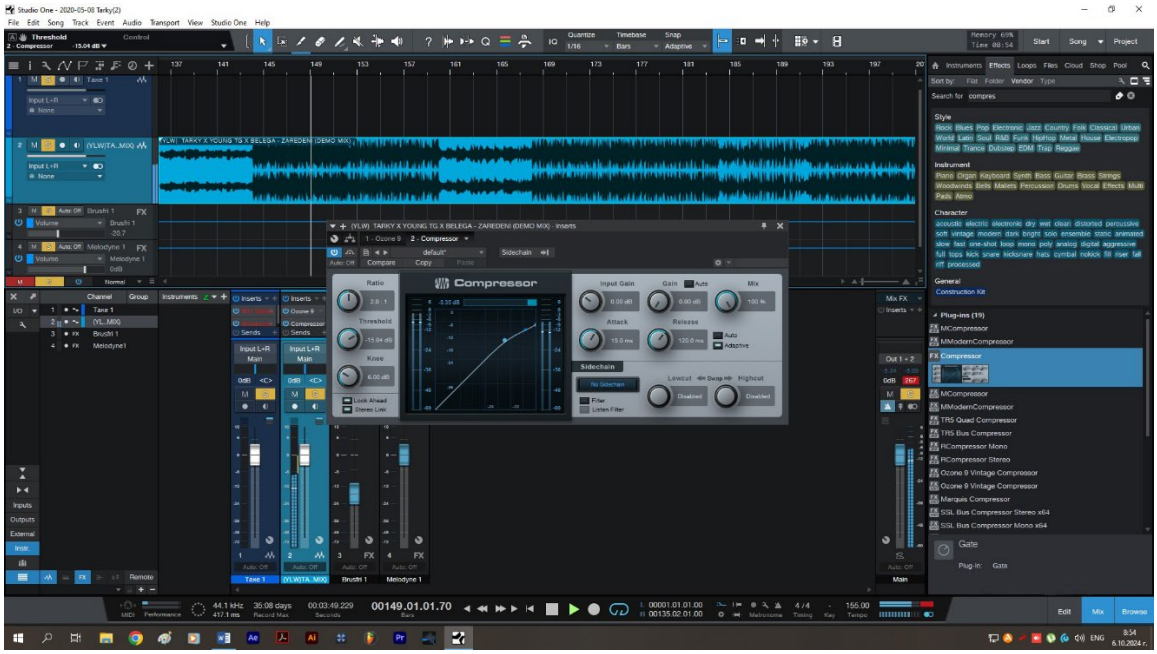
Тези параметри работят съвместно, за да контролират динамиката на звука и да създадат по-балансиран и управляем аудио сигнал. Табл. 1 показва параметрите на компресор, Табл.2 - настройките на различни аудио източници, Фиг. 7 показва компресор.

***Таблица 1:*** *Параметри и препоръчителни стойности за настройка на аудио компресор*

| Параметър | Препоръчителна стойност | Описание |
|---|---|---|
| ***Threshold*** | -20 до -10 dB | Нивото на сигнала, при което компресорът се активира. Зависи от силата на входния сигнал. |
| ***Attack*** | 1 до 10 мс (за барабани)<br>20 до 50 мс (за вокали) | Колко бързо компресорът започва да намалява сигнала след преминаването му над прага. |
| ***Ratio*** | 2:1 до 4:1 (за вокали)<br>4:1 до 6:1 (за барабани) | Степента на компресия – колко да се намали сигналът над прага. По-високо съотношение за по-агресивна компресия. |
| ***Sustain*** | 0.5 до 1.5 сек (ако е наличен) | Времето, през което компресорът поддържа компресията след като е задействан. |
| ***Release*** | 40 до 80 мс (за барабани)<br>100 до 250 мс (за вокали) | Колко бързо компресорът ще престане да действа след като сигналът спадне под прага. |
| ***Gain*** | 2 до 5 dB | Усилване за компенсиране на загубеното ниво в резултат на компресията. |

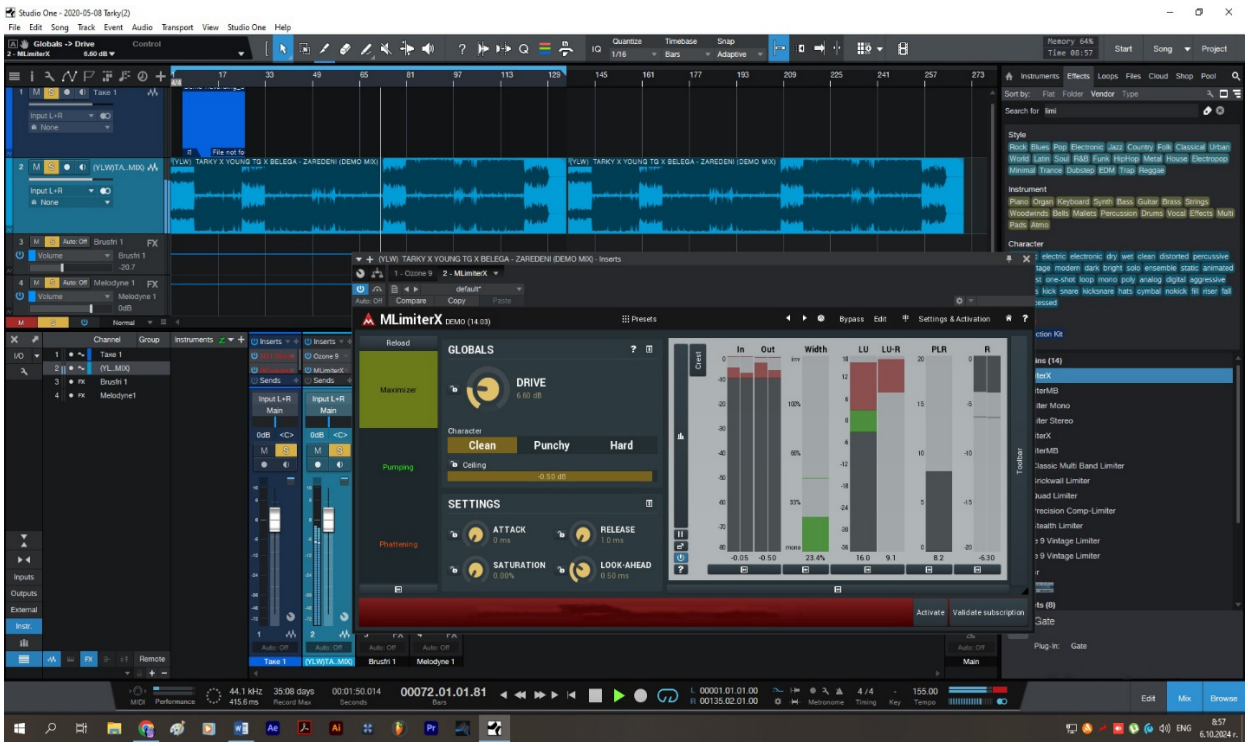
***Таблица 2:*** *Настройка на аудио източници*

| Вокали | Барабани (Snare, Kick) | Бас китара |
|---|---|---|
| *Threshold: -15 dB* | *Threshold: -10 dB* | *Threshold: -12 dB* |
| *Attack: 20 мс* | *Attack: 5 мс* | *Attack: 25 мс* |
| *Ratio: 3:1* | *Ratio: 5:1* | *Ratio: 4:1* |
| *Release: 150 мс* | *Release: 50 мс* | *Release: 100 мс* |
| *Gain: 3 dB* | *Gain: 2 dB* | *Gain: 4 dB* |




**Фиг. 7.** Софтуерна приставка - Компресор

- **Аудио ограничител (фиг. 8)** – Той е устройство, което подобно на компресора, намалява динамичния обхват на звуковия сигнал. Докато компресорът постепенно редуцира нивото на сигнала, когато то надвиши определен праг, ограничителят напълно блокира сигнала от преминаване над този праг. Основната функция на ограничителя е да повиши силата на звуковия сигнал до максимално възможния му връх, без да предизвиква изкривяване. В цифровите аудио системи този праг е фиксиран на 0 dB, което означава, че ограничителят изцяло отрязва всяка част от сигнала, която надвишава тази стойност.




**Фиг. 8.** Софтуерна приставка – Ограничител

***Таблица 3:*** *Основни параметри на аудио ограничителя*

| Параметър | Описание | Примерни стойности |
|---|---|---|
| ***Threshold (Праг)*** | *Нивото, над което сигналът се блокира* | *-6 dB, -3 dB, 0 dB* |
| ***Attack Time (Време за атака)*** | *Времето, за което ограничителят реагира на сигнал над прага* | 1 мс, 5 мс, 10 мс |
| ***Release Time (Време за освобождаване)*** | *Времето за възстановяване след намаляване на сигнала* | 50 мс, 100 мс, 200 мс |
| ***Output Gain (Изходно усилване)*** | *Усилване на обработения сигнал* | 0 dB, +3 dB, +6 dB |
| ***Ceiling (Таван)*** | *Максималното ниво на изходния сигнал* | 0 dB |

***Таблица 4:*** *Разлика между компресор и ограничител*

| Характеристика | Компресор | Ограничител |
|---|---|---|
| ***Цел*** | Намалява динамичния обхват чрез постепенно намаляване на нивото | Напълно блокира сигнали над прага |
| **Праг** | Настройва се по избор | Обикновено фиксиран на 0 dB |
| **Тип на редуциране** | Пропорционално намаляване на сигнала | Абсолютно спиране на сигнала |
| **Използване** | Регулиране на динамиката в музика и глас | Защита от клипинг и изкривяване |

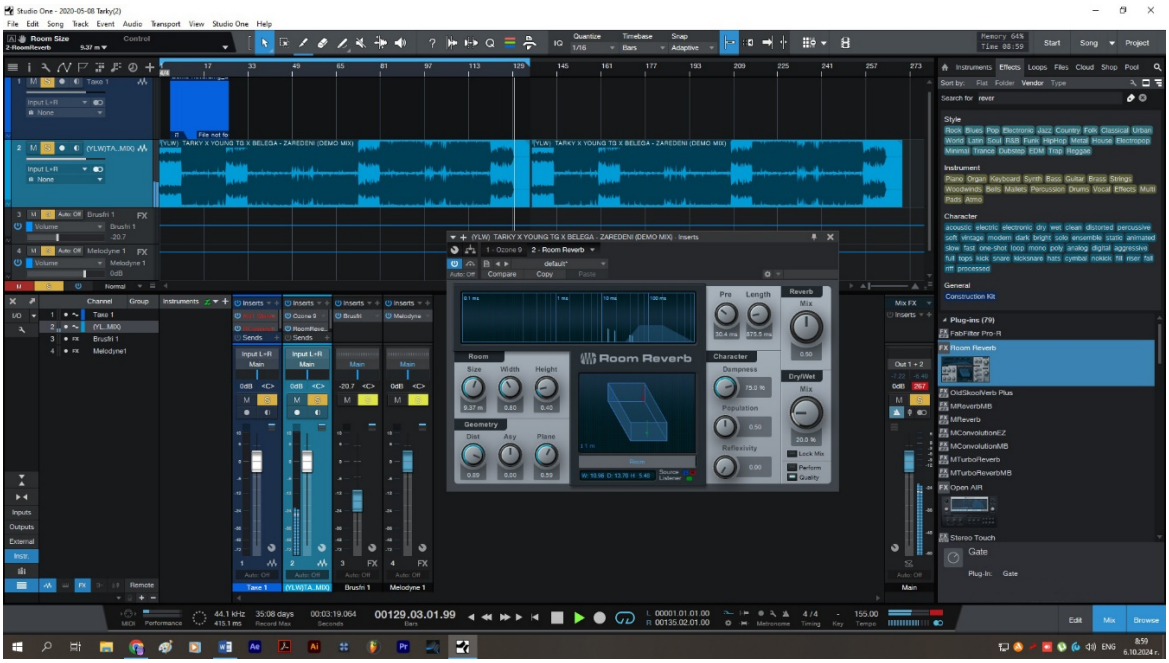
***Таблица 5:*** *Видове ограничител*

| Тип ограничител | Описание | Приложение |
|---|---|---|
| ***Brick-wall Limiter*** | Напълно блокира сигналите над прага, без възможност за преминаване | Избягване на цифрово изкривяване |
| ***Soft Limiter*** | По-плавно блокиране на сигнала над прага, с по-малко агресивност | Мастериране на музика |
| ***Lookahead Limiter*** | Използва предварително време за анализ на сигнала преди да достигне прага | Аудио продукция, Подкасти |

- **Реверберация (Reverb) (Фиг. 9) –** Този аудио ефект симулира процес на продължително отражение на звукови вълни в затворени пространства, като по този начин възпроизвежда естественото звуково поведение в различни акустични среди. Основната му цел е да създаде усещане за дълбочина и пространственост в звуковия сигнал. Ефектът предоставя контроли като "Dry" и "Wet", където "Dry" представлява директният, необработен сигнал, а "Wet" – отразеният сигнал. Освен това, могат да се регулират параметри като размер и форма на помещението, продължителността на реверберацията, времето на забавяне на отразения сигнал, както и честотния диапазон на отразения звук.

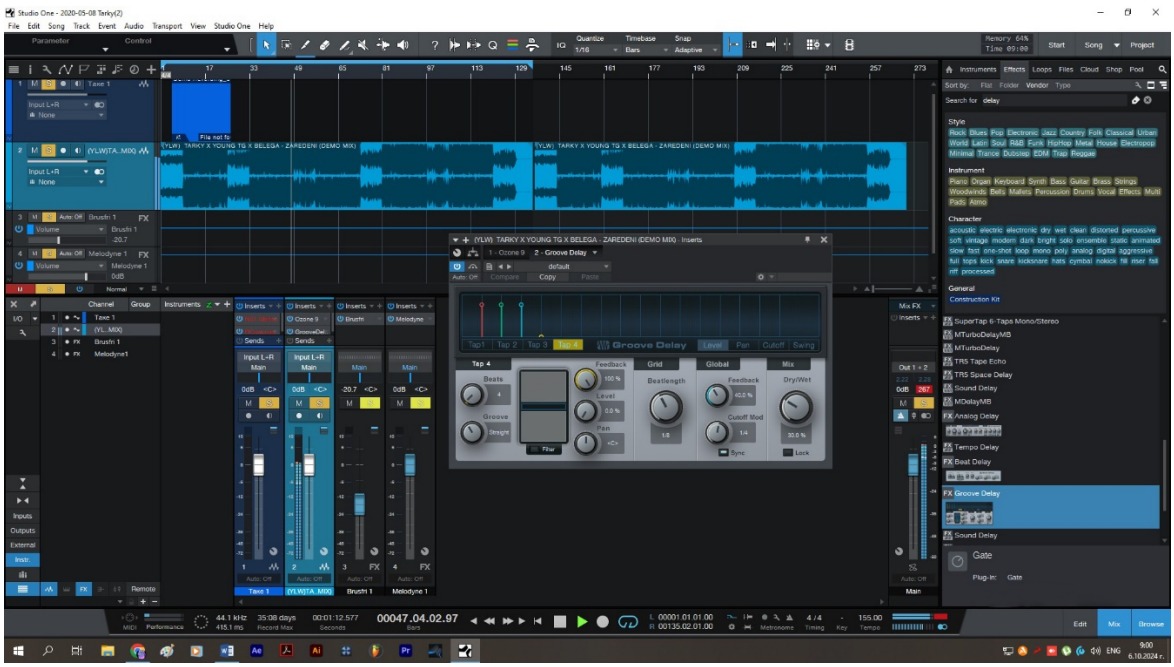
***Таблица 6:*** *Различни типове реверберация*

| Тип на реверберацията | Описание | Примерни акустични среди |
|---|---|---|
| ***Hall Reverb*** | Симулация на голяма зала | Концертна зала, Театър |
| ***Room Reverb*** | Симулация на малко помещение | Стая, Студио |
| ***Plate Reverb*** | Симулация на плоча за реверберация | Класическа реверберация на плоча |
| ***Chamber Reverb*** | Симулация на малка зала | Камерна зала |
| ***Spring Reverb*** | Симулация на механична пружина | Стари усилватели |



**Фиг. 9.** Софтуерна приставка – Реверберация

- **Аудио закъснение (Delay) (Фиг. 10) –** Този ефект създава последователни повторения на аудио сигнала през фиксирани интервали от време, като всяко повторение постепенно затихва. Повторенията могат да бъдат синхронизирани с темпото на музиката или зададени произволно. Ефектът предлага възможности за контрол на броя на повторенията, тяхната продължителност, скоростта на затихване, разположението в стерео панорамата, филтриране на определени честоти и промяна на тоналността на отразените сигнали.



**Фиг. 10.** Софтуерна приставка – Аудио закъснение

***Таблица 7:*** *Честотен диапазон на отразения звук*

| Честотен диапазон | Описание на ефекта върху звука | Примерни настройки |
|---|---|---|
| ***Ниски честоти*** | Придава по-тъмен, по-замъглен звук | 100 Hz - 500 Hz |
| ***Средни честоти*** | Подчертава естествеността на звука | 500 Hz - 2000 Hz |
| ***Високи честоти*** | Прави звука по-светъл и прозрачен | 2000 Hz - 8000 Hz |

***Таблица 8:*** *Настройки на delay в различни ситуации*

| Аудио ситуация | Delay Time | Feedback | Stereo Pan | Tone Control | Описание |
|---|---|---|---|---|---|
| ***Ритъм китара*** | 400 мс | 50% | Център | Светъл | За създаване на пространствено усещане |
| ***Вокал*** | 250 мс | 30% | Ляво-Дясно | Топъл | Подчертава емоционалното въздействие |
| ***Синтезатор (Ambient)*** | 800 мс | 70% | Широк | Среден | Атмосферен звук с дълбочина |
| ***Барабани (Snare Drum)*** | 200 мс | 20% | Център | Светъл | Леко ехо за подчертани ритми |

***Таблица 9:*** *Видове delay (закъснение)*

| Тип на delay | Описание | Примерни приложения |
|---|---|---|
| ***Analog Delay*** | Симулира закъснението, създадено от аналогови устройства | Старинен звук, топли тонове |
| ***Digital Delay*** | Прецизно и чисто закъснение с точна репликация на сигнала | Модерна електронна музика |
| ***Ping-Pong Delay*** | Редуване на повторенията между ляв и десен | Пространствен ефект в стерео |
| ***Tape Delay*** | Закъснение с характерния звук на магнитна лента | Ретро ефект |
| ***Modulated Delay*** | Включва модулация на повторенията за постигане на разнообразие | Пространствени и атмосферни ефекти |

- **Аудио филтър (Filter) (Фиг. 11)** – Филтърът е честотно селективен процесор, подобен на еквалайзера, но със специален фокус върху премахването (изрязването) на определени честотни диапазони. Когато филтърът премахва честотите от ниския честотен диапазон, като същевременно пропуска средните и високите честоти, той се нарича високочестотен филтър (high-pass filter). Обратното – когато филтърът изчиства високите честоти и пропуска ниските, той е нискочестотен филтър (low-

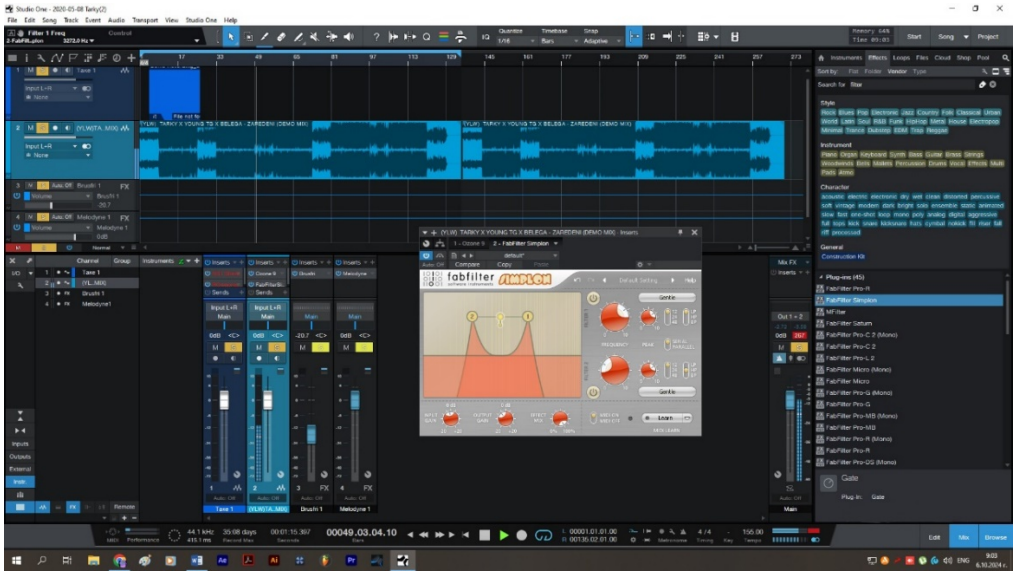
pass filter). Ако филтърът премахва както ниските, така и високите честоти, оставяйки само средните честоти, той се нарича лентов филтър (band-pass filter).

***Таблица 10:*** *Честотен диапазон при филтриране*

| Параметър | Описание | Примерни *стойности* |
|---|---|---|
| ***High-Pass Filter (HPF)*** | Филтрира ниските честоти от закъсненията | 100 Hz, 500 Hz, 1000 Hz |
| ***Low-Pass Filter (LPF)*** | Филтрира високите честоти от закъсненията | 5000 Hz, 8000 Hz, 12000 Hz |
| ***Band-Pass Filter (BPF)*** | Пропуска само честоти в определен диапазон | *300 Hz - 3000 Hz* |
| ***Tone Control (Тоналност)*** | Променя звуковия тембър на повторенията | *> 3000 Hz* |

***Таблица 11:*** Честотни характеристики на филтри

| Филтър | Честотна характеристика | Описание на поведението |
|---|---|---|
| ***High-Pass Filter*** | Пропуска честоти над честотата на изрязване | Изрязва басовите честоти |
| ***Low-Pass Filter*** | Пропуска честоти под честотата на изрязване | Изрязва високите честоти |
| ***Band-Pass Filter*** | Пропуска честоти в тесен диапазон около централна честота | Изолира средните честоти |
| ***Notch Filter*** | Премахва тесен честотен диапазон | Подтиска определена честота |




**Фиг. 11.** Софтуерна приставка – Аудио филтър

# 8 Балансиране на ефекти при създаване на професионална аудио обработка

***Казус:***

Зададена е задача да се смеси песен за рок банда. Тяхната композиция съдържа следните елементи: вокали, електрическа китара, бас китара, барабани и синтезатор. Целта

е да се създаде професионален микс, като се използва реверберация (reverb), компресори, ограничители, delay, филтри и други ефекти, за да се придаде дълбочина, яснота и енергия на песента. Основните предизвикателства са:

- Подобряване на вокалите – вокалите трябва да звучат ясно и да изпъкват в микса.
- Изчистване на звука на китарата – китарата трябва да звучи мощно, без да доминира над останалите инструменти.
- Управление на динамиката на барабаните – барабаните трябва да бъдат енергични, но не агресивни.
- Добавяне на пространственост на синтезатора – синтезаторът трябва да създава атмосфера, но да не заглушава другите елементи.
- Поддържане на ясна ниска честота на баса – бас китарата трябва да осигури стабилност, без да наводнява микса с нискочестотен шум.

***Решение:***

- ***Вокали***

- Използва се филтър (High-Pass Filter): За да се изчистят ниските честоти, които могат да се събират с баса, прилага се High-Pass Filter на вокала с Cut off Frequency на около 150 Hz и Slope от 12 dB/октава.
- Добавяне на компресор: За да се поддържа постоянна динамика и яснота, прилага се компресор с:
  Threshold: -6 dB
  Ratio: 3:1
  Attack Time: 5 мс
  Release Time: 100 мс
  Make-up Gain: +3 dB
- Реверберация: За да се придаде дълбочина на вокала се използва Reverb с:
  Dry/Wet съотношение: 40/60
  Room Size: Medium (средно)
  Decay Time: 2 секунди

- ***Електрическа китара***

- Използване на филтър (Band-Pass Filter): За да се избегне намесата на китарата с баса и високите честоти, прилага се Band-Pass Filter с честотен диапазон 500 Hz – 3000 Hz.
- Delay (Закъснение): За създаване на стерео ефект използва се Ping-Pong Delay, който редува повторенията между ляв и десен канал със следните настройки:
  Delay Time: 400 мс
  Feedback: 50%
  Stereo Pan: Ляво -> Дясно
  Wet/Dry: 30/70
- Компресор: За да се контролира динамиката, използва се компресор с:

Threshold: -8 dB
Ratio: 4:1
Attack Time: 10 мс
Release Time: 150 мс

- ***Барабани***

- Използва се ограничител (Limiter) за управление на пиковете: Прилага се ограничител, за да предотвратите клипинг на силните удари на барабаните:
  Threshold: 0 dB
  Attack Time: 1 мс
  Release Time: 50 мс
  Output Gain: +3 dB
- Филтриране на ударните (Snare Drum): Използва се Notch Filter около 200 Hz, за да премахнат нежелани резонанси.
- Reverb на барабаните: За да се добави простор и дълбочина, прилага се реверберация с по-кратък decay:
  Decay Time: 1.5 секунди
  Wet/Dry: 30/70

▪ ***Синтезатор***

- Low-Pass Filter (LPF): За да се премахнат високите резки честоти и за да се постигне по-плавен звук, използва се Low-Pass Filter с Cut off Frequency на 5000 Hz и Slope от 24 dB/октава.
- Modulated Delay: За да се добави атмосфера на синтезатора, прилага се Modulated Delay с:
  Delay Time: 800 мс
  Feedback: 60%
  Modulation Depth: 0.3
- Реверберация: Прилага се Reverb с голяма стая (large room) и Decay Time от 3 секунди, за да се придадете ефект на пространственост.

▪ ***Бас китара***

- High-Pass Filter: За да се премахнат нежеланите честоти под 50 Hz, използва се High-Pass Filter със Slope от 12 dB/октава.
- Компресор: Прилага се компресор за управление на динамиката на баса:
  Threshold: -4 dB
  Ratio: 4:1
  Attack Time: 15 мс
  Release Time: 120 мс
- Low-Pass Filter: За да се изгладят високите честоти и да се остави баса в стабилната ниска честотна лента, използва се Low-Pass Filter с Cut off Frequency от 3000 Hz.

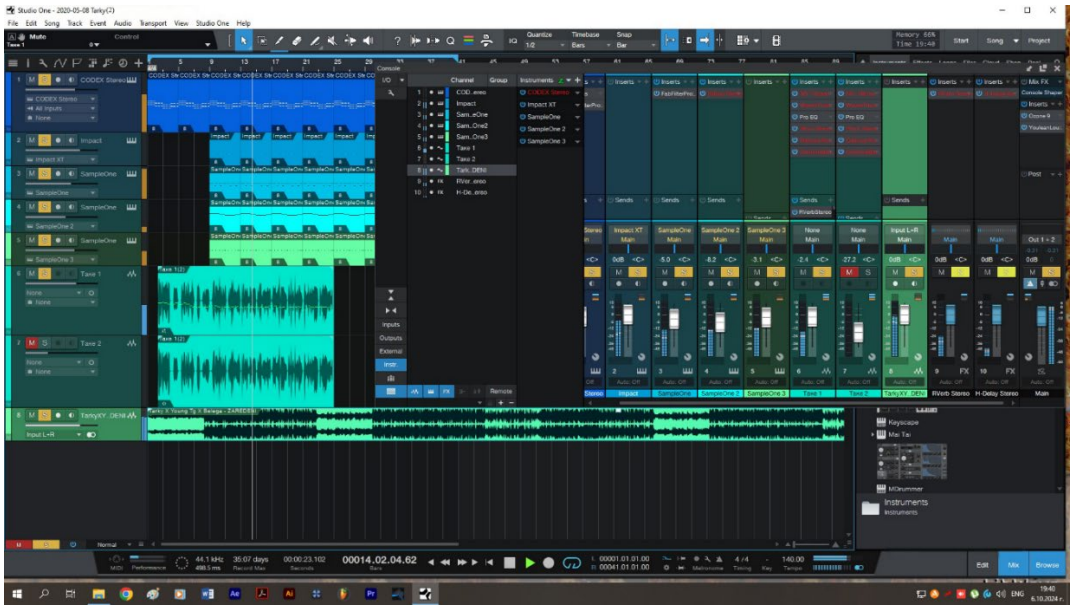
***Резултат:***

С тази комбинация от ефекти се постига чист и професионален микс в който всеки елемент заема своето място в звуковия спектър. Вокалите са ясни и отчетливи, китарата звучи мощно и балансирано, барабаните са енергични, без да доминират, синтезаторът добавя атмосфера, а басът осигурява стабилна основа. На Фиг. 12 е показан крайния резултат от казуса.

# 9 Заключение

Целта на този доклад е да демонстрира как чрез цифрова аудио работна станция може да се осъществи запис, редакция, смесване и обработка на аудио сигнал, водещи до финализирането на завършен аудио продукт. Докладът ще илюстрира процесите на смесване и мастериране на аудио сигнали, както и използването на ефектни приставки, които подпомагат обработката и подобряват качеството на крайния аудио резултат.

Представените методи и техники намират приложение в звукозаписни студиа, където аудио сигналите могат да бъдат записвани, редактирани и смесвани с помощта на хардуерни и софтуерни инструменти.



**Фиг. 12.** Краен резултат след обработка и микс

**ЛИТЕРАТУРА:**


[1] Mateus P., César Mattos C., Holanda A, 2019, Audio Plugin Recommendation Systems for Music Production, 8th Brazilian Conference on Intelligent Systems, Electronic ISBN:978-1-7281-4253-1 DOI: 10.1109/BRACIS.2019.00152, pp. 198-204

[2] McNally G., Gaskell P., Editing Digital Audio, 2019, IEEE International Conference on Acoustics, Speech and Signal Processing, DOI: 10.1109/ICASSP.1984.1172346, pp. 36-42

[3] Najduchowski E., Lewandowski M., Bobinski P., Automatic Audio Mastering System, 2018, Joint Conference – Acoustics, Electronic ISBN:978-1-5386-7114-6, DOI: 10.1109/ACOUSTICS.2018.8502427, pp. 227-232

[4] Owaki W., Takahashi K., Novel Sound Mixing Method for Voice and Background Music, 2015, IEEE International Conference on Acoustics, Speech and Signal Processing, Print ISSN: 1520-6149 DOI: 10.1109/ICASSP.2015.7177977, pp. 365-370

[5] Shah H., Jukar N., Godshalwar K., Srivastava K., User friendly Synthesizer Software, 2011, International Conference on Multimedia Technology, Electronic ISBN:978-1-61284-774-0 DOI: 10.1109/ICMT.2011.6001703, pp.101-108

[6] Lalev H., Tsankov Ts. Synthesis on computer systems of work of real time. Scientific Conference, dedicated to the 105th anniversary of the birth of the pioneers of computing John Atanasoff and John von Neumann, Shumen, 2008, ISBN 978-954-577-540-6, pp. 96-102.

[7] Săman O., Muscaliuc R., Stanciu L., Music Panel: An Application for Creating and Editing Music, 2020, 24th International Conference on System Theory, Control and Computing, Electronic ISBN:978-1-7281-9809-5 DOI: 10.1109/ICSTCC50638.2020.9259705, pp.40-49

[8] Xiangyang Y., Music Creation with Computer Music Production Software, 2022, International Conference on Electronics and Devices Computational Science, Electronic ISBN:978-1-6654-5541-1, DOI: 10.1109/ICEDCS57360.2022.00041, pp. 101-109

# SOFTWARE-DEFINED NETWORK ARCHITECTURE BASED ON PROGRAMMABLE PROTOCOL-INDEPENDENT P4 PROCESSORS*

**MUSTAFA B. UZUN, VALENTIN T. ATANASOV**

***ABSTRACT:*** *Software-Defined Networking (SDN) has emerged as a paradigm-shifting approach in network management, offering flexibility and programmability. This abstract explores the integration of P4 (Programming Protocol-independent Packet Processors) into SDN architectures, aiming to enhance network control and adaptability. P4 enables the specification of packet processing pipelines, allowing for fine-grained control over network behavior. By leveraging P4, SDN architectures can dynamically adapt to varying network conditions, optimize traffic routing, and implement innovative network services efficiently. This abstract discusses the fundamental principles of P4 and its potential applications within SDN frameworks. Additionally, it explores the problems and opportunities associated with integrating P4 into existing SDN infrastructures, including scalability, performance, and interoperability considerations. Overall, the integration of P4 into SDN architectures holds promise for enabling highly programmable, agile, and efficient networks capable of meeting the evolving demands of modern communication environments.*

***KEYWORDS:*** *P4 (Programming Protocol-independent Packet Processors), P4 programming language, SDN (Software Defined Networking), OpenFlow*

***DOI: https://doi.org/10.46687/GVTE5429***

# АРХИТЕКТУРА НА СОФТУЕРНО-ДЕФИНИРАНА МРЕЖА, БАЗИРАНА НА ПРОГРАМИРУЕМИ ПРОТОКОЛНО-НЕЗАВИСИМИ ПАКЕТНИ ПРОЦЕСОРИ P4

**МУСТАФА Б. УЗУН, ВАЛЕНТИН Т. АТАНАСОВ**

***АБСТРАКТ:*** *Мрежите, дефинирани чрез софтуер (Software-Defined Networking, SDN), се утвърдиха като подход, променящ парадигмите в управлението на мрежите, предоставяйки гъвкавост и възможности за програмиране. Този абстракт разглежда интеграцията на P4 (Programming Protocol-independent Packet Processors) в SDN архитектури, с цел подобряване на контрола върху мрежата и адаптивността ѝ. P4 позволява специфицирането на тръбопроводи за обработка на пакети, което осигурява детайлен контрол върху мрежовото поведение. Използвайки P4, SDN архитектурите могат динамично да се адаптират към променящите се условия в мрежата, да оптимизират маршрутизацията на трафика и ефективно да внедряват иновативни мрежови услуги. Този абстракт обсъжда основните принципи на P4 и потенциалните му приложения в SDN рамките. Освен това се изследват проблемите и възможностите, свързани с интеграцията на P4 в съществуващите SDN инфраструктури, включително аспекти като мащабируемост, производителност и интероперативност. Като цяло, интеграцията на P4 в SDN архитектури предоставя обещаващи перспективи за създаването на високо програмируеми, адаптивни и ефективни мрежи, които могат да отговорят на нарастващите изисквания на съвременните комуникационни среди.*

## 1 Въведение

Софтуерно-дефинираните мрежи SDN имат за цел да предоставят динамични и програмируеми решения за управление на компютърни мрежи. Общата концепция на SDN

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

парадигмата е отделянето на предаващата равнина от контролната равнина, които са характерни и за конвенционалните мрежови устройства. Тази концепция централизира всички контролни функции на SDN домейна на едно място (SDN контролер), който осигурява унифициран изглед към мрежата [1]. За постигане на тази цел в предаващата равнина, мрежовите устройства се опростяват до намален набор от операции, които се програмират с помощта на стандартизирани протоколи. OpenFlow може би е най-успешният все още разработващ се SDN стандарт за постигане на тази цел [2], но от друга страна P4 концепцията също търпи развитие (Фиг.1.) [13].




**Фиг. 1.** Историческо развитие на P4

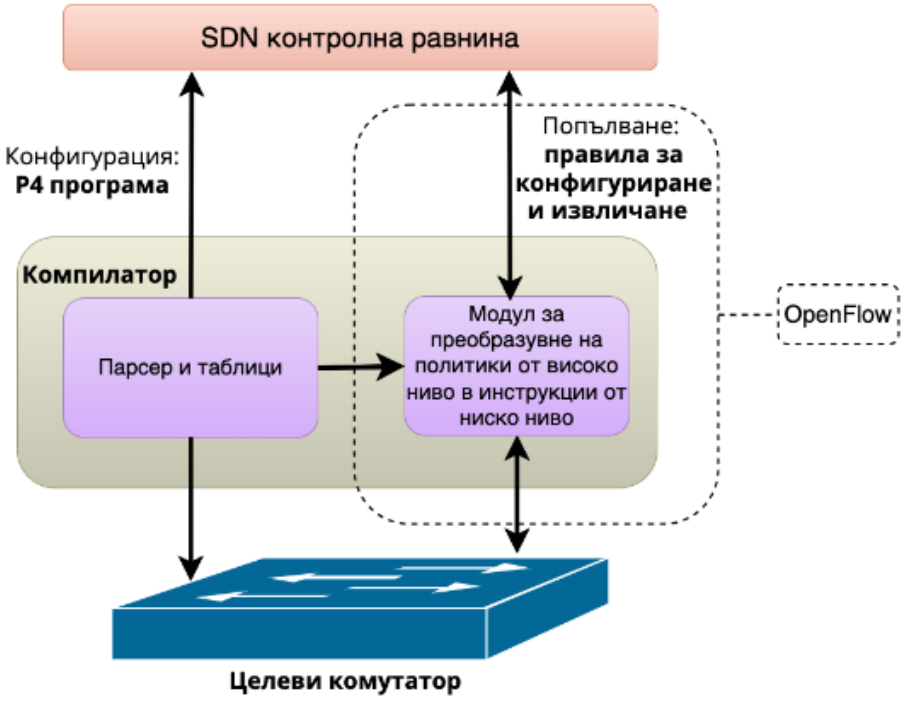
Скоро след възхода на OpenFlow обаче става ясно, че по-голямата част от гъвкавостта, предлагана от модела SDN, е ограничена от възможностите на дефинираните полета в него. Интерфейсът на OpenFlow започна просто, с абстракцията на таблици с правила, които могат да съпоставят пакети в дузина полета на заглавката (напр. MAC адреси, IP адреси, протокол, номера на TCP/UDP портове и т.н.) [2]. През последните пет години спецификацията става все по-сложна (Табл. 1.), с много повече полета за заглавки и множество етапи на обработващите конвейери [3] за обработка на таблици и за прилагане на правилата за комутиране, за да позволи на контролера да прилага по-гъвкав контрол над комутаторите при комутиране на пакети [4, 5, 6,7].

**Таблица** 1. Спецификации на OpenFlow.

| **Версия** | **Дата** | **Заглавка** | **Полета на заглавката** |
|---|---|---|---|
| OpenFlow 1.0 | Декември 2009 | 12 | Ethernet, TCP/IPv4 |
| OpenFlow 1.1 | Февруари 2011 | 15 | MPLS, inter-table metadata |
| OpenFlow 1.2 | Декември 2011 | 36 | ARP, ICMP, IPv6 и др. |
| OpenFlow 1.3 | Юни 2012 | 40 | IPv6 Extension Headers, ICMPv6, NDP, PBB, и др. |
| OpenFlow 1.4 | Октомври 2013 | 41 | IPv6 Extension Header Pseudo-Field, Packet Length Pseudo-Field, Tunnel ID Pseudo-Field, IPv6 Flow Label, и др. |
| OpenFlow 1.5 | Май 2016 | 44 | Pv6 Extension Header Flags, IPv6 Extension Header Header-Length, IPv6 Extension Header Option Header Type, PBB ISID, и др. |

Добавянето на нови заглавни полета за удовлетворяване на нуждите на бързо разрастващият се сектор не показва признаци на спиране. Например центровете за данни все повече искат да прилагат нови форми на капсулиране на пакети, например NVGRE, VXLAN и STT, поради което се прибягва до внедряване на софтуерни комутатори, които са по-лесни за добавяне на нови функционалности. Този подход обаче би довел до многократно обновяване и разширяване на спецификацията на OpenFlow, което означава бавна адаптация и имплементиране към обновените и новите протоколни заглавки.

Бъдещите мрежови устройства трябва да поддържат гъвкави механизми за анализиране на пакети и съвпадащи полета на заглавките, позволявайки на контролера да използва тези възможности. Като решение за преодоляване на това ограничение е предложен алтернативен модел наречен P4, който се базира на концепцията за програмируема равнина на данни или предаваща равнина. Основната идея зад P4 или "Програмируеми протоколно-независими пакетни процесори" е да осигури гъвкавост и програмируемост на мрежовите устройства, като им се позволи да се адаптират към различни изисквания, наложени от различни приложения. Това се постига чрез дефиниране на прецизни инструкции за обработка на мрежови пакети, които могат да се използват за създаване на мрежови функции и услуги. Те предоставят на мрежовите инженери и софтуерни разработчици възможност да програмират мрежови устройства по начин, който е независим от конкретните мрежови протоколи и стандарти. Тъй като правилата и пакетните структури са дефинирани на ниво бит и байт, P4 предлага по-подробен контрол върху мрежовия от решенията предлагани от OpenFlow (Фиг. 2.). По този начин разработчиците могат да дефинират, както основните пакетни заглавки например (Ethernet, IPv4, IPv6 и др.), така и специфични протоколи и функции за мрежово управление.

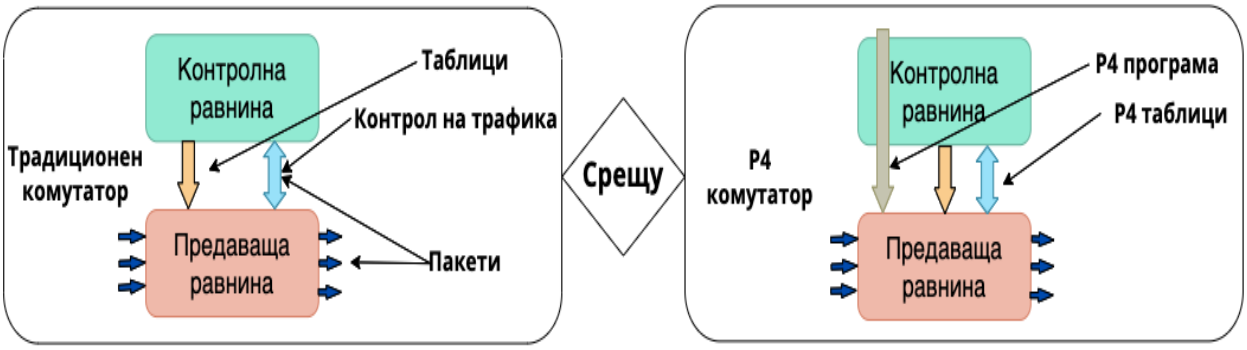



**Фиг. 2.** Съпоставяне на концепциите на OpenFlow и P4

.

# 2 P4 SDN

Основната идея на P4 (Programmable Protocol-independent Packet Processors) в контекста на SDN е да направи мрежовата инфраструктура напълно програмируема и протоколно-независима, както и да предостави гъвкавост и контрол върху обработката на мрежови пакети на по-ниско ниво в сравнение с традиционните SDN подходи. Докато основната концепция на SDN разделя контролната равнина от предаващата равнина, с цел постигне на централизирано управление на мрежата [1], P4 отива още по-далеч, като позволява програмиране на самите мрежови устройства например рутери, комутатори и други в лицето на програмируеми ASIC (Application-specific Integrated Circuit), FPGA (Field-programmable Gate Array) и SmartNIC (Smart Network Interface Card) и как те обработват пакети [12, 13]. На фиг. 3. се показва архитектурната разлика между традиционен комутатор и P4 комутатор [11].




**Фиг. 3.** Сравнение на архитектурите на традиционен комутатор и P4 комутатор

## 2.1. Основни характеристики на P4

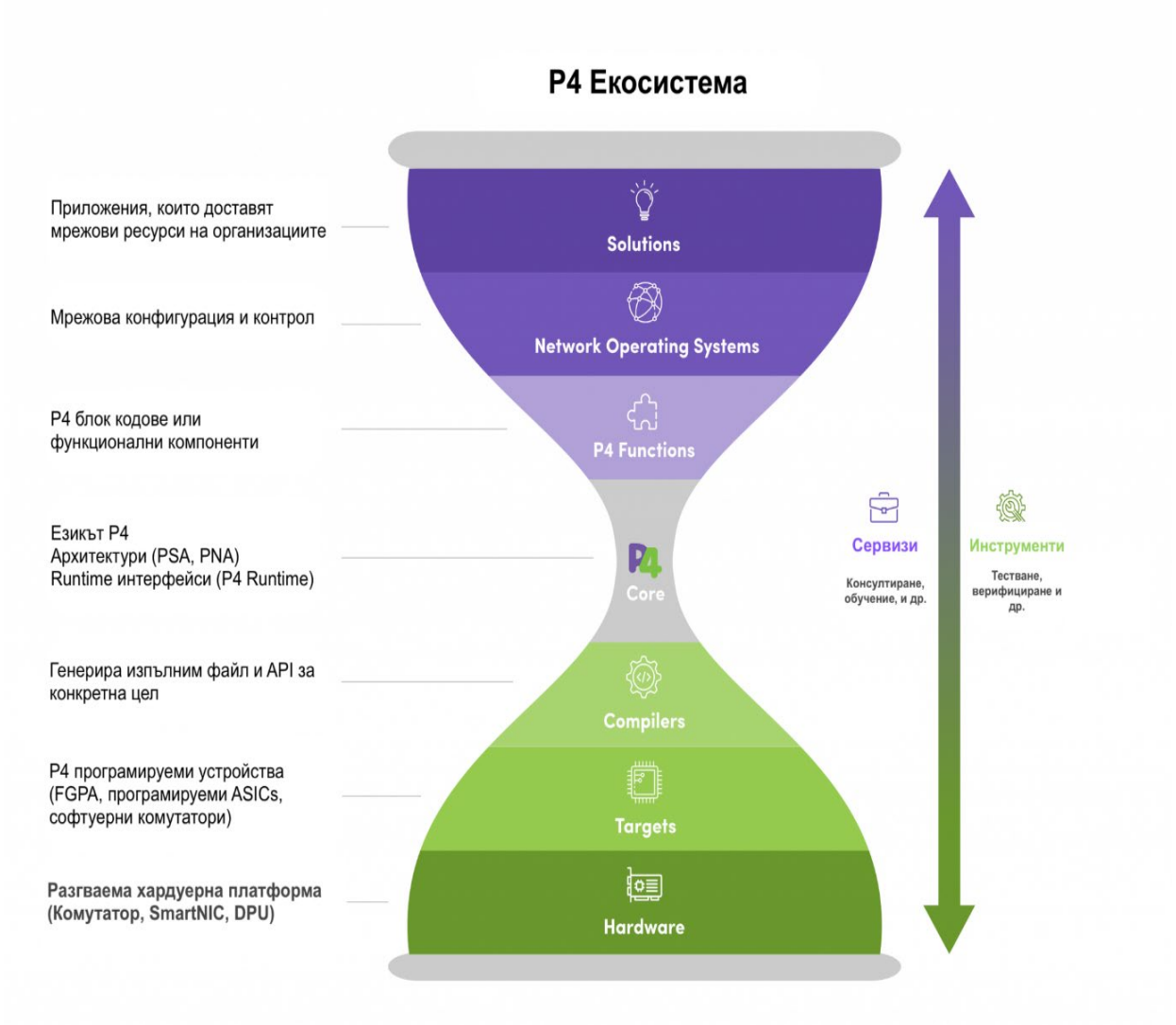
P4 притежава специализиран програмен език. Според неговия общ архитектурен модел може да се определят основните характеристики, които го отличават от другите SDN архитектури [1].

Основни характеристики на P4 [10,11,13]:

- *Протоколна независимост:* P4 не е обвързан с конкретни мрежови протоколи, като Ethernet, IP или TCP. Вместо това, разработчиците могат да програмират мрежови устройства, така че те да поддържат нови или собствени протоколи, без да се променя хардуерът.
- *Програмируема обработка на пакети:* P4 осигурява на мрежовите инженери възможност да определят как трябва да се обработват и пренасочват мрежови пакети, включително задачи, като проверка на заглавките, препращане, филтриране и модифициране.
- *Отделяне на контролната равнина от предаващата равнина:* P4 се вписва много добре в SDN, където контролната равнина е напълно програмируема и контролирана от централен контролер.
- *Хардуерна независимост:* P4 програмите могат да се изпълняват на различни видове мрежови устройства с възможност за програмиране, като те могат да бъдат ASIC, FPGA, SmartNIC и дори софтуерни симулатори като BMv2 и Mininet.

## 2.2. **P4 „екосистема“**

„Екосистемата“ на P4 се състои от различни компоненти, които работят заедно, за да осигурят разработването, симулацията, тестването и внедряването на P4 програми. На фиг. 4. са показани основните компоненти на една P4 „екосистема“ [10,12]:




**Фиг. 4.** P4 „екосистема“

*Езикът P4:* Официалната спецификация на езика P4 дефинира синтаксиса и семантиката на езика и предоставя подробни описания на начините за програмиране на мрежови устройства.

*Компилатори:* P4C е основният компилатор за P4, който превежда P4 код в целеви машинен код, подходящ за конкретни хардуерни или софтуерни платформи [11, 14].

*Референтни архитектури на P4_16 и P4_14:* Различни версии на P4 езика с малки различия в синтаксиса и функционалностите [11,14].

*Емулатори и симулатори:*

- *BMv2 (Behavioral Model version 2):* Софтуерен модел, който емулира поведението на P4 програмирани устройства. Използва се за тестване и дебъгване на P4 програми.

- *Mininet:* Симулационна среда, която позволява създаване и тестване на виртуални мрежи, използвани заедно с P4 програми.

*Контролери*:

- ONOS (Open Network Operating System): Контролер за SDN, който поддържа P4 и може да се използва за управление на P4-програмирани устройства.
- P4 Runtime: API за управление на P4 програмирани устройства, който осигурява интерфейс за контрол и конфигурация.

*Инструменти за верификация и дебъгване*:

- P4V: Инструмент за верификация на P4 програми, който помага за проверка на коректността на P4 кода преди внедряване.
- P4-DPDK: Интеграция на P4 с DPDK (Data Plane Development Kit) за високопроизводителни софтуерни базирани мрежови решения.

# 3 Програмни изисквания и спецификации на езика P4

P4 е домейн-специфичен език, който предоставя възможност за обработка на суров поток от мрежов трафик от най-ниско ниво, попадащ в предаващата равнина на общоприетата SDN концепция. Неговият синтаксис произтича от езика за програмиране C, включително запазени ключови думи, предназначени за анализ на пакети [10,11,13].

Най-важните основни абстракции, предоставени от езика P4 са:

- *Типове:* P4 работи с обработка на пакети, и често се изисква промяна на параметрите на битово ниво, който включва примитивни типове като бит *bit<N>,* който разпределя **N** бита за едно цяло (integer) число. Пакетите са съставени от заглавки и полезен товар, заглавките са от съществено значение за обработката на пакети и P4_16 има специални запазени дума за тях.

```
1 header ethernet t {
2 bit<48> dstAddr; // 48-битов MAC адрес на получателя
3 bit<48> srcAddr; // 48-битов MAC адрес на източника
4 bit<16> etherType; // 16-битово поле за тип на Ethernet
5 }
```

- *Разбор (Parcer):* Всеки P4 конвейер включва разбор, като обикновено това е първият програмен блок. Той се описва като крайна автоматика на състояния (states) и преходи (transitions). Всяко състояние представлява момент в процеса на извличане на данни от заглавките на пакета, а преходите между състоянията зависят от стойностите на вече извлечените полета, например тип на (Ethernet) заглавката. Процесът започва с начално състояние (start) и след всяко състояние програмата анализира заглавката, като извлича необходимата информация и се установява в друго състояние, докато достигне състоянието на приемане (accept) или отхвърляне (reject). Тези състояния са окончателни, а програмата преминава към следващия блок на конвейера.
- *Таблици (Tables):* Основния компонент във всяка програма за комутиране са таблиците върху които, чрез набор от ключове извършват определени действия. В този компонент могат да се дефинират набор от ключове като MAC адреси на получателя или входен порт, на база на, която да се извърши действие. Могат да бъдат дадени допълнителни аргументи, като максимален размер на таблицата за

разпределение на паметта и действие по подразбиране за пакети/кадри, които нямат никакъв запис в таблиците. Записите в таблицата могат да са статични или да бъдат актуализирани в реално време чрез Thrift интерфейс или P4 Runtime услуга, работеща на SDN контролер. Таблиците са гъвкави и могат да се адаптират към широк набор от сценарии, като прости таблици за маршрутизиране, списъци за контрол на достъпа (ACL) или дори вземане на по-сложни решения с множество променливи ключове.

- *Действия (Actions):* Основен компонент, който дефинира как трябва да се обработват мрежовите пакети при разбора, в който техните заглавки са анализирани. Всяко действие представлява блок от код, който описва конкретни операции върху пакетите или полетата на техните заглавки, като модифициране на стойности, препращане (forward), отхвърляне (drop) и други. Тези действия се изпълняват въз основа на правила за съвпадение в (Match-action) таблици.
- *Контролни потоци (Control flows):* Те дефинират логиката и последователността на обработка на пакетите след разбор. Те се използват за прилагане на действия и вземане на решения въз основа на резултатите от таблиците за съвпадение и действията върху мрежовите пакети. Контролният поток ръководи какво да се прави с пакета на всеки етап от обработката му, като може да включва логика за съпоставяне на правила, изпълнение на действия, както и указания за препращане или изтриване на пакета.
- *Външни функции и обекти (Extern):* Представлява механизъм, който позволява на мрежовите инженери да взаимодействат с функционалности на хардуерни компоненти, извън директно програмируемите елементи на P4 програмата. „Externs“ разширяват способностите на P4 езика, като предоставят достъп до специализирани мрежови функции, които не могат да бъдат описани или изпълнени директно в P4 код. Пример за това могат да бъдат хеш функции, таймери, метрики за измерване на трафика, управление на опашки (queues), CRC (Cyclic Redundancy Check) изчисления, регистри и броячи, също така и директен достъп до хардуерните ресурси, на платформи, като за FPGA или ASIC.
- *Основна декларация:* Всяка P4 програма трябва да дефинира екземпляр на архитектурата, наречена (main). Разборът и контролите се дефинират в реда, в който се изпълняват и трябва да са съгласувани с архитектурата на хардуерното устройство.
- *Основна декларация (Main Declaration):* Дефинира началната точка на програмата, в която се указват всички контролни блокове, разбор, обратен разбор и метаданни. Това е мястото, където се свързват различните компоненти на P4 програмата и се определя потокът на обработка на пакетите. Основната декларация е важна, защото тя конфигурира взаимодействието между програмируемите модули, като разбор, контролните блокове и обратен разбор.

# 4 Примерен код на P4

На примера по-долу се показва структурата на P4 код за обработка на VLAN тагове, като се извеждат основните етапи от обработката на пакети в програмируема мрежова архитектура, с обяснения за всеки етап:

```
// 1. Дефиниране на заглавките
(Headers)
header ethernet_t {
 macAddr_t dstAddr;
 macAddr_t srcAddr;
 bit<16> ethType;
}

header vlan_t {
 bit<3> pcp; // Priority Code Point
 bit<1> dei; // Drop Eligible
Indicator
 bit<12> vid; // VLAN Identifier (ID)
 bit<16> ethType;
}

// Дефиниране на структурата на
заглавките
struct headers_t {
 ethernet_t ethernet;
 vlan_t vlan;
}

// 2. Дефиниране на парсера (Parser)
parser MyParser(packet_in pkt,
 out headers_t hdr) {
 state start {
 pkt.extract(hdr.ethernet); //
Извлича Ethernet хедъра
 transition
select(hdr.ethernet.ethType) {
 0x8100: parse_vlan; // Преход към
извличане на VLAN заглавката
 default: accept;
 }
 }

 state parse_vlan {
 pkt.extract(hdr.vlan); // Извлича
VLAN заглавката
 transition accept; // Край на
парсинга
 }
}

// 3. Таблици за съвпадение и действия
(Match-Action Table)
table vlan_table {
 key = {
 hdr.vlan.vid: exact; // Сравнява по
VLAN ID
 }
 actions = {
 drop;
 forward;
```

```
// 4. Апликатор на действия (Control
Logic)
control MyIngress {
 apply {
 if (hdr.vlan.isValid()) {
 vlan_table.apply(); // Прилага
VLAN таблицата
 }
 }
}

// 5. Дефиниране на депарсера
(Deparser)
control MyDeparser(packet_out
pkt, headers_t hdr) {
 apply {
 pkt.emit(hdr.ethernet); // Добавя
Ethernet заглавката обратно
 if (hdr.vlan.isValid()) {
 pkt.emit(hdr.vlan); // Добавя VLAN
заглавката обратно (ако е валиден)
 }
 }
}

// 6. Свързване на компонентите в
pipeline
pipeline MyPipeline {
 MyParser();
 MyIngress();
 MyDeparser();
}

// 7. Програмен интерфейс (Switch
Model)
switch MySwitch {
 MyPipeline();
}
```

# 5 Заключение

P4 SDN има бъдеще като основна част от мрежовите архитектури, като същевременно предоставя гъвкавостта и адаптивността, от които се нуждаят бъдещите мрежови устройства. В комбинация с развитието на когнитивните машини и машинно обучение, P4 ще продължи да се развива и да играе ключова роля в новите мрежови среди, особено там, където изискванията за бърза адаптация и персонализация са критични. Технологията ще бъде ключов фактор за успеха на 5G/6G, облачните мрежи, и IoT инфраструктурата в бъдеще.

**ЛИТЕРАТУРА:**

[1] Göransson, P.; Black, C.; Timothy Culver., 2017. Software Defined Networks A Comprehensive Approach Second Edition. ISBN: 978-0-12-804555-8.

[2] Azodolmolkly, S., 2013. Software Defined Networking with OpenFlow. Birmingham: ISBN 978-1-84969-872-6.

[3] McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Petrson, L.; Rexford, J.; Shenker, S.; Turner, J., 2008. OpenFlow: Enabling Innovation in Campus Networks.

[4] ONF. OpenFlow Switch Specification. December 31, 2009. Available from: https://opennetworking.org/wp-content/uploads/2013/04/openflow-spec-v1.0.0.pdf.

[5] ONF. OpenFlow Switch Specification. February 28, 2011. Available from: https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.1.0.pdf.

[6] ONF. OpenFlow Switch Specification. December 05, 2011. Available from: https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.2.pdf.

[7] ONF. OpenFlow Switch Specification. June 25, 2012. Available from: https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.3.0.pdf.

[8] ONF. OpenFlow Switch Specification. October 14, 2013. Available from: https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf.

[9] ONF. OpenFlow Switch Specification. March 26, 2015. Available from: https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

[10] P4. Official site. October 06, 2024 Available from: https://p4.org.

[11] P4. Official site. October 10, 2024 Available from: https://p4.org/p4-spec/docs/P4-16-v1.2.4.pdf.

[12] P4. Official site. October 10, 2024 Available from: https://p4.org/ecosystem/.

[13] Github. P4language. October 17, 2024 Available from: https://github.com/p4lang.

[14] P4. Official site. October 22, 2024 Available from: https://p4.org/p4-spec/p4-14/v1.0.5/tex/p4.pdf

# MODEL OF THE EDUCATIONAL PROCESSES MANAGEMENT INFORMATION SYSTEMS THROUGH PYTHON AND DJANGO*

**DESISLAVA N. IVANOVA, VALENTIN T. ATANASOV**

***ABSTRACT:*** *The rapid development of technology necessitates the need for efficient and scalable management information systems, especially in the education sector. This paper examines the use of the Python programming language and Django programming framework to create an automated management information system designed for educational institutions. The system model will provide the tasks of optimizing various educational and administrative processes such as managing the activities of learners and teachers, planning the educational process. Using tools such as Python and Django, the developed model is expected to improve operational efficiency as well as offer a scalable solution that can be adapted to a wide range of needs of educational institutions.*

***KEYWORDS:*** *Django, Python, web application development*

***DOI: https://doi.org/10.46687/WGKP5885***

# МОДЕЛ НА АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ПРОЦЕСИ В ОБРАЗОВАТЕЛНАТА СФЕРА С ПОМОЩТА НА PYTHON И DJANGO

**ДЕСИСЛАВА Н. ИВАНОВА, ВАЛЕНТИН Т. АТАНАСОВ**

***АБСТРАКТ:*** *Бързото развитие на технологиите налага необходимостта от ефективни и мащабируеми информационни системи за управление, особено в образователния сектор. Този доклад разглежда използването на езика за програмиране Python и програмна работна рамка Django за създаването на автоматизирана информационна система за управление, предназначена за образователни институции. Моделът на системата ще обезпечи задачите по оптимизиране на различни учебни и административни процеси като управление на дейностите на обучаеми и преподаватели, планиране на образователния процес. Използвайки средства като Python и Django, разработваният модел се очаква да подобрява оперативната ефективност както и да предлага мащабируемо решение, което може да бъде адаптирано към широк набор нужди на образователните институции.*

## 1 Въведение

В съвременното общество потребността от надеждни и ефективни информационни системи за управление на процеси значително нараства. Образователните институции са изправени пред сериозни въпроси относно управлението на голям обем от данни, включително записи на обучаеми, учебни материали, информация за преподаватели и административни процеси. Традиционните методи за управление на тези задачи често са ръчни, отнемащи време и предполагащи възникването на грешки. За да бъдат решени тези въпроси, е необходима автоматизирана система, която да интегрира различни функции, обезпечаващи постигането на висока степен на автоматизация, редукция на човешкия вход за данни, ефективни решения за изходяща информация и комуникационни подходи, реализирани от подсистеми.

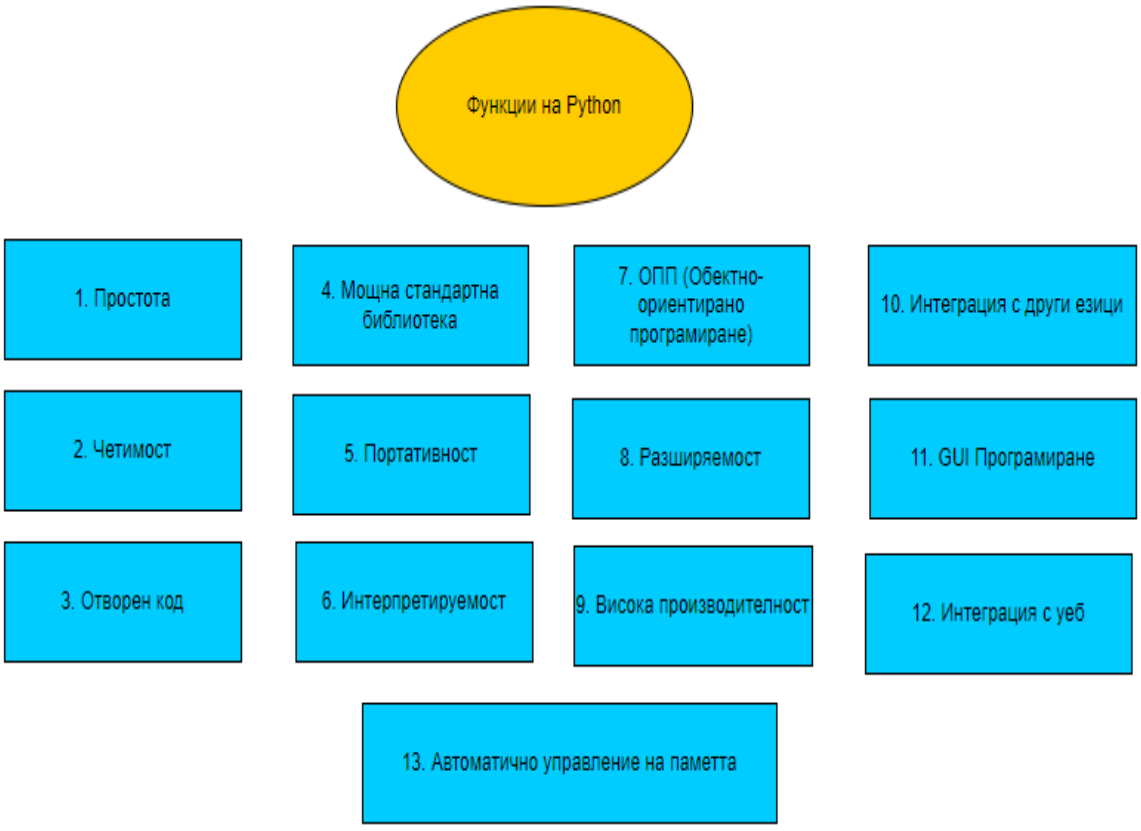
* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

Скриптовият език Python, със своята простота и универсалност, заедно с Django – технологична работна рамка от високо равнище за Python, предлагат добро решение за разработка на такива системи. Настоящия доклад разглежда модел на система, процеса на разработка и предимствата на използването на Python и Django за изграждане на автоматизирана информационна система за управление на процеси в образователната сфера.

# 2 Използвана технология

## 2.1. Python

Python е интерпретативен, интерактивен и обектно-ориентиран език за програмиране от високо ниво. Подходящ е както за обектно-ориентирано, така и за функционално програмиране. Това, че е от високо ниво означава, че е изключително лесно четим. Езикът разполага с т.нар. garbage collector, т.е. автоматичен начин за управление на паметта. Обновяван е често, като последната стабилна версия е от 6 август 2024. Дизайнът му е фокусиран върху четимостта, функционалността и простота при писането на код. Именно това стои в основата на създаването на езика – да бъде лесен за четене и минималистичен. Архитектурата на Python използва в значителна степен отстъпа, за да поддържа четливостта на кода. Основните функции на езика Python са представени на фиг.1:




**Фиг. 1.** Основни функции на езика за програмиране Python

*2.1.1. Предимства на Python*

Python е широко използван език за програмиране [9], тъй като той има уникални характеристики, които го отличават от другите програмни езици. Някой от тези характеристики са:

- отворен код и развитие на общността;
- лесен за изучаване и поддръжка;
- множество библиотеки;
- удобни за потребителя структури от данни;
- скорост и производителност;
- реални приложения;
- разработка на игри;
- изкуствен интелект и машинно обучение;
- обработка на текст и изображения;
- визуализация на данни и др.

*2.1.2. Недостатъци на Python*

Всеки програмен език има своите недостатъци и Python не прави изключение [10]. Сред тях са: по-ниската му производителност; не е широко разпространен в разработката на мобилни приложения; има по-голяма консумация на памет; несъвместимост на версиите.

Въпреки тези недостатъци, обширните библиотеки, лекотата на използване и четливостта на Python го правят популярен избор за голямо разнообразие от приложения.

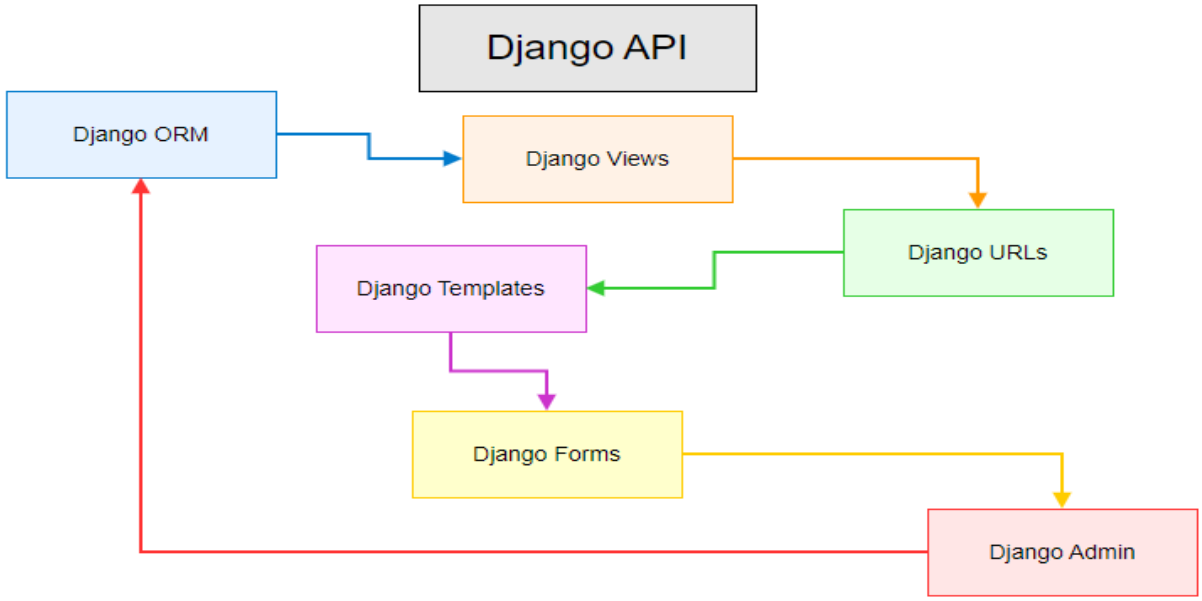
**2.2. Django**

Python е популярен език за създаване на Уеб приложения, тъй като притежава обширни рамки и системи за управление на съдържанието (CMS), които намаляват трудностите пред разработчиците. Широко се използват рамки за Уеб разработка като Django, Flask, Bottle, както и системи за управление на съдържание като Plone CMS, Django CMS и Wagtail. Използването на Python за Уеб разработка има различни предимства като сигурност, лекота и удобство на разработване. Python поддържа широк набор от Уеб протоколи, включително HTTP/HTTPS и FTP. Езикът предлага широка колекция от библиотеки, която подобрява и опростява разработката на уеб приложения [2].

В индустрията на Уеб технологиите, където споделянето на информация и комуникацията между хората е от решаващо значение, внимателният подбор на подходящи инструменти и рамки може да окаже значително влияние върху ефикасността, възможностите и сигурността на онлайн приложенията. Django е широко използвана работна рамка за конструиране на базирани на Python Уеб приложения. Неговата архитектура Model-View-Template (MVT) помага на разработчиците при процеса на разработка и рационализира конструкцията, според документацията. Django е най-ефективен, когато е свързан с Уеб приложение, предоставяйки допълнителна функционалност.

*2.2.1 Основни API елементи на Django*

API (Application Programming Interface) е набор от правила и инструменти, които позволяват на различни програмни компоненти да комуникират помежду си. По същество, API определя как различни програмни приложения трябва да взаимодействат, предоставяйки стандартизирани методи и формати за обмен на данни. Django е популярен фреймуърк за Уеб приложения на Python, който предоставя различни API елементи и инструменти, които улесняват разработката на уеб приложения. Основните API елементи на Django са представени на фиг.2:




**Фиг. 2.** Основни API елементи на Django

Django ORM (Object-Relational Mapping) е системата за работа с база данни, която позволява на разработчиците да взаимодействат с базата данни чрез Python обекти, вместо да пишат SQL(Structured Query Language) код. ORM автоматизира преобразуването между релационните таблици и Python обекти.

Django Views - управляват логиката на приложението и отговарят за обработката на HTTP заявки. Views получават заявки, обработват данни и връщат отговори на потребителите. Те свързват URL(Uniform Resource Locator) адресите с обработката на данни.

Django URLs – това е механизмът за маршрутизиране на заявки до съответните views. URL конфигурацията дефинира какви URL адреси ще бъдат обработвани и какви views ще се извикват в отговор на тези адреси.

Django Templates - шаблони, които се използват за генериране на HTML съдържание. Те позволяват на разработчиците да създават динамични уеб страници, като се използват данни от views и ORM.

Django Forms - управляват обработката на данни от формуляри, включително валидация и обработка на входни данни. Forms предлагат лесен начин за събиране и валидиране на данни от потребителите.

Django Admin - вграден интерфейс за управление на съдържанието на сайта. Той позволява на администраторите да управляват моделите на данните чрез графичен интерфейс, предоставяйки лесен начин за създаване, редактиране и изтриване на данни.

Тези елементи работят заедно, за да създадат и управляват мощни Уеб приложения, осигурявайки всичко необходимо от работа с бази данни до управление на съдържание и взаимодействие с потребителите.

*2.2.2. Предимства на Django*

Django има редица характеристики, които го правят предпочитан при разработката на Уеб приложения. Основните от тях са показани на фиг. 3:




**Фиг. 3.** Основни характеристки на Django

Използвайки работната рамка Django, разработчиците могат да създадат добро и мащабируемо Уеб приложение с удобен за потребителя интерфейс, който е лесен за поддръжка. Езикът за програмиране Python, с множеството си библиотеки и инструменти, осигурява необходимите ресурси за създаване на сложни и богати на функции програми. Езикът за програмиране Python и работната рамка Django работят добре заедно и са решение за създаване на автоматизирана информационна система за управление на процеси в образователната сфера, която да задоволява изискванията на настоящите образователни институции.

## 3 Модел на автоматизирана информационна система за управление на процеси в образователната сфера, реализирана с помощта на Python и Django

Разглежданият модел на система ще включва функции като записване на обучаеми, полагане на онлайн изпити, управление на преподаватели, проследяване на присъствие, проследяване на оценки и автоматично попълване на оценките след онлайн изпитването. Системата следва да осигурява комуникация между обучаеми, преподаватели и администратор. В обобщение автоматизираната информационна система следва да:

- поддържа множество потребителски роли, като обучаем, преподавател, администратор и родител, със съответните разрешения и нива на достъп;
- бъде мащабируема и адаптивна, за да отговори на променящите се нужди на съответната образователна институция;
- бъде проектирана с мисъл за сигурността, като се използват добри практики за криптиране на данни, контрол на достъпа и уязвимост, управление и спазване на съответните закони и разпоредби за поверителност [3].
- осигурява автоматизирано въвеждане на оценките от модула на системата за онлайн изпитване към модула с данни за обучаемите, което би спестило време и ще ограничи фактора „човешка грешка“ при ръчно въвеждане.

**Диаграми на потоците от данни**

Диаграмите на потоците на данни (Data Flow Diagrams, DFD) се използват за визуализация на потока, по който данните преминават през дадена система. Те показват как информацията се пренася между процеси, външни субекти и хранилища на данни. Диаграмите могат да бъдат разграничени на различни нива на детайлност, като се започне от общия изглед на системата и се преминава към по-подробни разглеждания на отделните процеси.

### 3.1. Context Diagram на администратор

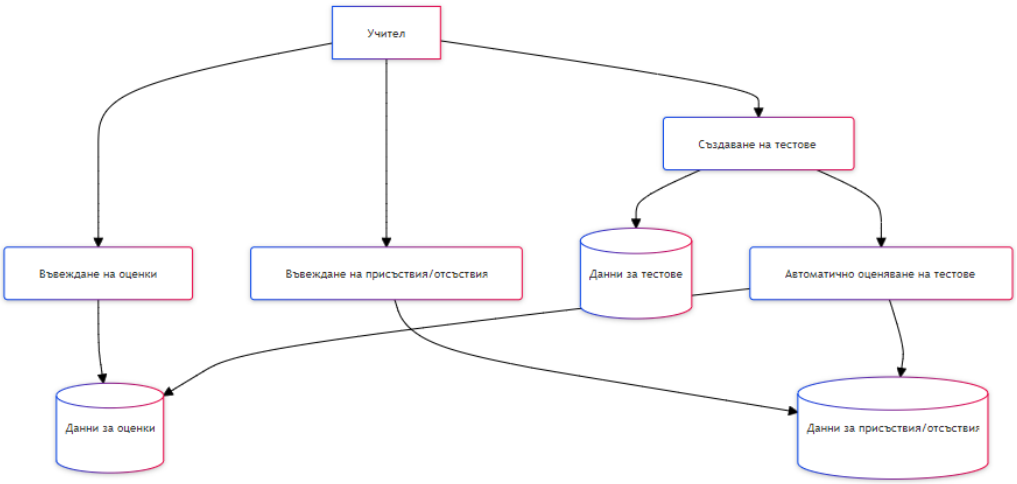
Context Diagram (контекстна диаграма) представя системата като един единствен процес, показвайки взаимодействието между системата и външните субекти. Тази диаграма не включва подробности за вътрешните процеси на системата, а вместо това се фокусира върху входящите и изходящите данни и начина, по който те взаимодействат с външните субекти. Нарича се още Ниво 0, защото представлява най-общия изглед на системата, без да навлиза в детайли. Това е първото и най-високо ниво на DFD, което дава контекста за всички последващи диаграми. Основните дейности на администратора са показани на фиг. 4:




**Фиг. 4.** Context Diagram на администратор

### 3.2. Process Decomposition Diagram на преподавател

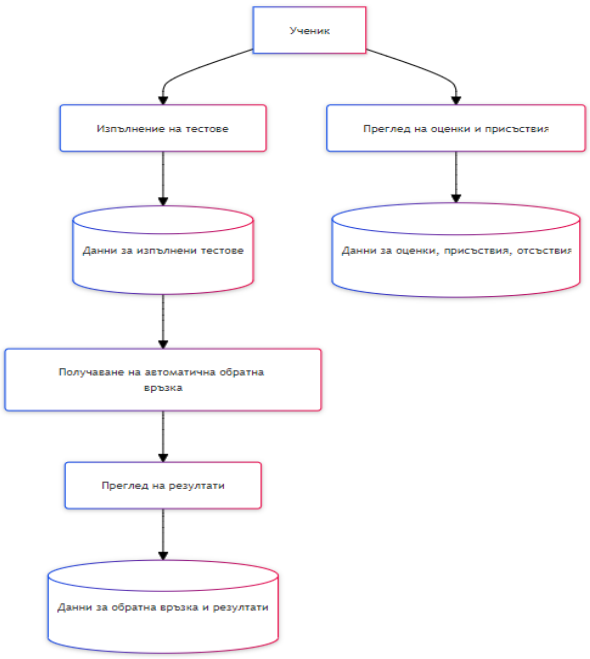
Process Decomposition Diagram или още диаграма на основните процеси разширява контекстната диаграма, като разглежда основните вътрешни процеси на системата. Нарича се Ниво 1, защото разширява и детайлизира Ниво 0, като предоставя повече информация за вътрешната структура на системата. Това ниво осигурява детайлен поглед върху основните функционални блокове на системата. Преподавателят извършва три основни действия– въвеждане на оценки, въвеждане на отсъствия/присъствия и създаване на тестове. Данните от всяко действие се записват в различни сегменти на базата данни. Автоматичното оценяване на тестове добавя оценки и може да актуализира данните за присъствия/отсъствия, ако тестът се провежда в реално време. Диаграма на основните процеси на ниво преподавател са показани на фиг.5:




**Фиг. 5.** Process Decomposition Diagram преподавател

### 3.3. Detailed Process Diagram на обучаван

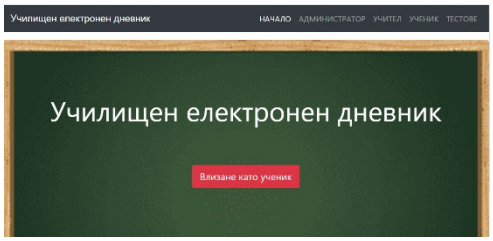
Диаграма на детайлни процеси (Detailed Process Diagram), наричана още диаграма от Ниво 2, детайлизира процесите, които са показани в Ниво 1. Това ниво показва по-задълбочено как всеки от основните процеси е съставен от по-малки подпроцеси. Тази диаграма е нужна за разбиране на конкретните стъпки и взаимодействия, които се извършват вътре в един процес. Това ниво често включва множество входни и изходни потоци на данни, които са по-малко видими на по-високите нива. Обучаваният има две основни взаимодействия със системата - изпълнение на тестове и преглед на оценки и присъствия. Данните от изпълнените тестове се записват в базата данни и автоматично се генерира обратна връзка, която се съхранява в системата. Диаграма на детайлните процеси на ниво обучаван е показана на фиг.6:



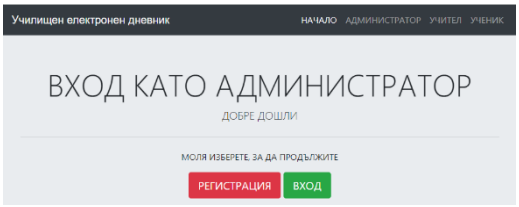

**Фиг. 6.** Detailed Process Diagram на обучаван

# 4 Проектиране на интерфейсни части в системата

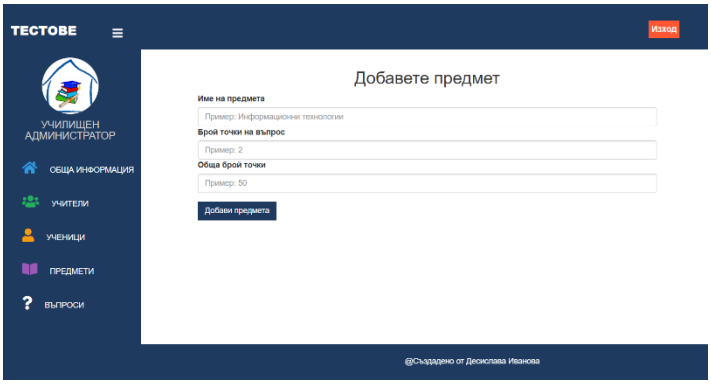
Създаването на такава система с езика за програмиране Python и Уеб работната рамка Django би предоставила по-ефективен подход за управление редица образователни дейности. Django предоставя базова работна рамка с вградени инструменти за удостоверяване на потребителя, база данни администрация и сигурност, което го прави предпочитан избор за разработване на многопотребителско онлайн приложение (система). Използването на Django и Python осигурява по-малко време за разработка и по-лесна поддръжка, тъй като тези технологии са добре документирани и имат голяма общност от разработчици, които да ги поддържат [4]. Комбинацията от Python и Django дава солидна основа за разработване на стабилна и ефективна система. Тези технологии са предпочитана алтернатива за разработване на онлайн приложения в образователната сфера. На следващите фигури са показани различни проектирани интерфейсни функционалности на моделираната система:




**Фиг. 7.** Начална страница на системата




**Фиг. 8.** Изглед за вход на администратор




**Фиг. 9.** Изгледи от модула за онлайн изпити

# 5 Заключение

Целта на автоматизираната информационна система за управление на процеси в образователната сфера е да подобри дейността на образователните институции, да подобри комуникацията между видовете потребители и да намали административната работа на

преподавателите, като помогне с автоматизиране на процеса по въвеждане на оценки от онлайн изпитвания. Автоматизираната информационна система за управление на процеси в образователната сфера, за която се избират средства за разработка програмните инструменти - Python и Уеб работна рамка Django, би могла да изгради ефективен програмен механизъм за административните и образователни процеси в образователните институции. Чрез тези програмни инструменти би могло да се реализира сигурна, ефективна и удобна за потребителя платформа за управление на данните на обучаваните. Да се въведе проследяване на техните постижения и присъствия. Освен това модулният принцип на разработка позволява интегрирането на нововъзникващи технологии, чрез които биха могли да се разширят функционалността на системата, което я прави по-адаптивна към променящите се изисквания на образователния сектор [5]. Разработването на такава система с помощта на Django би осигурило функции като удостоверяване на потребител и сигурност при съхранението на данни. Това ще гарантира степен на защита както на системата, така и на потребителските данни. Характеристиките на работната рамка Django биха осигурили лесна интеграция с различни категории бази данни, което би улеснило съхраняването, извличането и актуализирането на тези данни. Моделът на системата би подпомогнал подобряване на комуникацията между обучавани, преподаватели и администратор [6]. С използването на избраните програмни средства за разработка (Python и Django), би могло да се изгради ефективен модел на система, съответстващ на поставените към нея изисквания.

**ЛИТЕРАТУРА:**

[1] Bharamagoudar, S.R., Geeta, R.B. and Totad, S.G. (2013). Web based student information management system. International Journal of Advanced Research in Computer and Communication Engineering, 2(6), pp. 2342-2348.

[2] Devndra G. (2020). “Comparative study on Python web frameworks: Flask and Django ” Metropolia University of Applied Sciences Bachelor of Engineering Media Engineering Bachelor’s Thesis.

[3] Gore, H., Singh, R.K., Singh, A., Singh, A.P., Shabaz, M., Singh, B.K. and Jagota, V. (2021). Django: Web development simple & fast. Annals of the Romanian Society for Cell Biology, 25(6), pp. 4576-4585.

[4] Himanshu Gore1, Rakesh Kumar Singh2, Ashutosh Singh3, Arnav Pratap Singh4, Mohammad Shabaz5*, Bhupesh Kumar Singh7 (1998). Vishal Jagota8 “Django: Web Davids, D.L., Recovery effects in binary aluminum alloys, Ph.D. thesis, Harvard University.

[5] Ravindran, A. (2018). Django Design Patterns and Best Practices: Industry-standard web development techniques and solutions using Python. Packt Publishing Ltd.

[6] https://bg.wikipedia.org/wiki/Python Иванов, И., Георгиев Г., Информатика. Техника, София (1992).

[7] https://www.researchgate.net/publication/368719592_An_INTRANET-Based_Web_Application_for_College_Management_System_Using_Python_with_Django_Web_Framework://doi.org/10.22214/ijraset.2023.49151/( последно посетен на 21.09.2024 г.)

[8] https://www.tiobe.com/tiobe-index/ (последно посетен на 21.10.2024 г.)

[9] https://taglineinfotech.com/advantages-and-disadvantages-of-python/ (послено посетен на 21.09.2024 г.)

# SOME ASPECTS OF THE EDUCATIONAL PROCESSES MANAGEMENT INFORMATION SYSTEM*

**DESISLAVA N. IVANOVA, VALENTIN T. ATANASOV**

***ABSTRACT:*** *The article discusses the emerging issues related to the optimization of automation systems for the management of processes in the educational sphere. It also discusses the principle architecture of automated systems for optimizing administrative tasks, improving communication and data analysis. The need for a new system to meet the specific needs of educational institutions based on the MVC architecture is discussed, applying best practices as an effective approach for developing such a system.*

***KEYWORDS:*** *automated information systems, MVC architecture, education*

***DOI: https://doi.org/10.46687/FSEE9499***

# НЯКОИ АСПЕКТИ НА АВТОМАТИЗИРАНИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ПРОЦЕСИ В ОБРАЗОВАТЕЛНАТА СФЕРА

**ДЕСИСЛАВА Н. ИВАНОВА, ВАЛЕНТИН Т. АТАНАСОВ**

***АБСТРАКТ:*** *Настоящият доклад разглежда възникналите въпроси, свързани с оптимизиране на системи за автоматизация управлението на процесите в образователната сфера. Разглежда се и принципната архитектура на автоматизираните системи за оптимизиране на административните задачи, подобряване на комуникацията и анализ на данни. Разглежда се необходимостта от нова система, която да отговори на конкретните нужди на образователните институции, основаваща се на MVC архитектурата, прилагайки добрите практики като ефективен подход за разработка на такава система.*

## 1 Въведение

Темата за разработка и изследване на автоматизирана информационна система (АИС) за управление на процеси в образователната сфера е изключително актуална и значима в наши дни [7]. С развитието на информационните и комуникационните технологии е налице възможността да бъде прилагана автоматизацията за оптимизиране на процесите в образованието. За преминаването към автоматизирано управление на процеси в образователната сфера са налице редица предпоставки, произтичащи от широкото приложение на АИС в човешката дейност. Такива системи:

- подпомагат организирането и ефективното изпълнение на задачите в образователната сфера;
- автоматизират съществена част от административните процеси като приемане на документи и записване на обучавани, издаване на служебни бележки, оценяване на обучаваните, възможност за създаване на работни графици;
- подпомагат процеса на проследяване на напредъка на всеки обучаван. Дават възможност за анализ на неговите резултати и позволяват на преподавателите да адаптират своите усилия за нуждите на всеки обучаван с цел да бъдат осигурени оптимални възможности за неговото развитие;

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

- могат да осигурят по-добра комуникация между всички участници в образователния процес – обучаващи, обучавани, родители и администрация.
  предоставят достъп до информация, като учебни материали, графици, задачи, което подобрява комуникацията между преподавател и обучаван;
- подпомагат създаването на нови образователни методи и модели;
- позволяват съхранението и анализа на големи обеми данни, свързани с учебни планове, оценки, присъствие. Това предоставя възможност за статистически анализи, които могат да бъдат използвани от образователните институции във всички нива за подобряване на образователния процес и решаване на редица проблеми.

## 2 Предпоставки за автоматизирано управление на процеси в образователната сфера

Образователната среда се променя бързо, а автоматизацията може да помогне на образователните институции да се адаптират към тези промени. Тя може да осигурява по-бърз достъп до актуални ресурси и информация, да подпомогне комуникацията в условия на дистанционно обучение или в случай на извънредни ситуации и да осигури по-ефективно управление на ресурсите и графиците.

Глобални фактори като опазването на околната среда и климатичните промени поставят сериозни въпроси пред съвременното общество. Това налага необходимостта от разработване и реализиране на подходящи политики по отношение на здравословен и природосъобразен начин на живот. Осъществяването на цялостен подход в духа на принципите за устойчиво развитие ще спомогне за формиране на ценности и нагласи във връзка със зеления преход [8]. Използването на автоматизирана информационна система улеснява тази задача, тъй като намалява значително използването на хартия и човешки ресурси в процеса по събиране, съхраняване, обработка и използване на информация.

Дигитализацията на учебния процес е ключов елемент на съвременната образователна институция, чрез който се оптимизира процесът на обучение, повишава се неговата ефективност и се подпомага навлизането на методи и подходи, базирани на информационните и комуникационните технологии. Автоматизацията на учебния процес ще подобри значително качеството на образованието, по-лесното възприемане на учебния материал от обучаваните и ще спомогне за развитието на по-резултатни политики в тази насока. Ще предостави възможности за повишаване на ефективността, точността и прозрачността в управлението на образователните процеси, като същевременно ще се намали административната тежест върху преподавателите и администрацията.

От друга страна, в образователната сфера се търсят ефективни решения за успешно включване и трайно приобщаване на всеки обучаван, независимо от регионалните особености, социално-икономическия статус на семейството и майчиния език [1]. В днешно време все по актуален стои въпросът за задържането на обучаваните в образователните институции или предотвратяване на тяхното отпадане. Редица фактори влияят върху посещаемостта на обучаваните в образователните институции и има все по-голяма нужда от автоматизирана система, която да предупреждава, когато има обучаван застрашен от отпадане, било то поради натрупани много отсъствия, семейни причини, слаб успех или редица други фактори. Създаването на такава автоматизирана система би било от голяма полза за задържането на всеки обучаван.

В процеса на работа с една такава АИС за управление на процеси в образователната сфера би следвало да се обърне специално внимание на човешкият фактор.

Преподавателите са тези, които в голяма степен създават редица от дигиталните ресурси за проверка на знанията и уменията на обучаваните. Те са тези, които поставят критерии и оценяват работата им в това число и по отношение на онлайн изпитванията. Определянето на тези критерии, създаването на изпините тестове и материали не са обект на това изследване. Обръща се внимание на това, че всеки преподавател трябва да попълни в т. нар. електронен дневник конкретната оценка от едно такова изпитване за всеки обучаван. Това „ръчно“ вписване на резултатите винаги води до вероятност да се допусне човешка грешка. Създаване на АИС за управление на процеса на попълване на оценките на учениците от онлайн изпитванията автоматично в електронния дневник на образователната институция, без намесата на преподавател или друго упълномощено лице, би решило проблема с „човешката грешка“. Такава система предполага, че към електронния дневник на образователната институция трябва да има добре изградена система за онлайн изпитвания. Такава обща АИС би имала и още едно голямо предимство - автоматизираното попълване на оценките на обучаваните, ще спести значително време в административната работа на преподавателите, което е една от водещите тенденции към момента, т.е. да се намали административната тежест на преподавателите.

Необходимо е постоянно да се обменя информация и за целта трябва да се създаде ресурс, който да позволява да се реализира този процес. Образователният процес се състои почти изцяло от обмен на информация между участващите в него. Освен че получават знания, участниците в образователния процес обменят информация за графика, различните тестове и начините за предаването им. За успешната работа на всички участници, времето, необходимо за получаване на тази информация, трябва да бъде оптимално. В този случай е необходимо да се вземат предвид всички характеристики на институцията, организираща образователния процес.

Основните участници в училищния образователен процес са преподавател, обучаван и родител. Обменът на информация между тях е сложен процес, често зависещ от индивидуалните характеристики на участниците в него. Обучаваният не винаги е готов да съобщи за проблеми в ученето, работният график на родителите не позволява навременен контакт с преподавателят. Той от своя страна не винаги записва своевременно своите наблюдения. Социалните мрежи изместиха традиционните методи за комуникация (обаждания, лични срещи), а техни основни функционалности създават пречки при разделянето на личното и деловото общуване.

## 3 Развитие на автоматизираните информационни системи в образователната сфера

Уеб приложенията могат да служат като инструмент за решаване на проблеми с обмена на информация. Има различни дигитални образователни платформи като Moodle [2] или Blackboard Learn [3], които предоставят редица възможности за управление на образователният процес. Въвеждането на подобни решения в учебния процес изисква време за обучение на участниците и води до възникване на редица предизвикателства и проблеми.

Необходимо е да се създаде АИС, която да включва необходимите функции, и същевременно да се премахнат всички излишни. Например Moodle [2] (модулна обектно-ориентирана динамична учебна среда) е безплатна система за управление на обучението, насочена основно към организиране на взаимодействие между преподаватели и обучавани, въпреки че е подходяща и за организиране на традиционни дистанционни курсове, както и за подпомагане на обучението „лице в лице “.

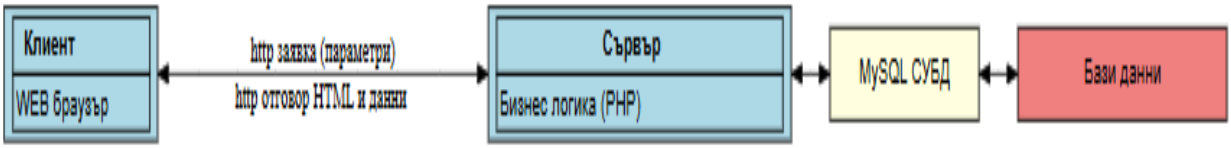
Moodle е създаден от група разработчици и е преведен на широк набор от езици, включително и на български език. Той принадлежи към класа системи LMS (Learning Management System) - системи за управление на обучението. Такава програма често се нарича и система за дистанционно обучение (DLS). Системата за управление на обучението Moodle може да се използва не само за организиране на дистанционно обучение, но ще е полезна и в образователния процес на образователните институции.

Използването на този продукт може да реши проблема, но има редица трудности:

- Модулите, преведени на съответния език, се предоставят от трети страни;
- Системата е изградена за големи образователни организации;
- Обработката на някои системни функции отнема много време;
- Обучението на ползвателите е процес, отнемащ време;
- Всички налични решения не предоставят възможност за включване в процеса на разработване на системата на нейните преки участници преподаватели, обучавани или административни работници.

Това налага необходимостта да се разработи система, която решава основните нужди на участниците в образователния процес, включително обучаваните, и уникалните нужди на образователната институция в процеса на развитие.

Решенията, разгледани по-горе, са реализирани под формата на Уеб приложения, които в момента са широко използвани. За разлика от Уеб сайта, уеб приложението е пълноценна програма, до която потребителят има достъп през Интернет, тоест не изисква инсталиране на дадено устройство. Уеб приложението работи с помощта на технологията клиент-сървър, където клиентът е браузър, Уеб сървърът обработва заявките и предоставя необходимата информация или услуги. Принципът на работа на Уеб приложение е показан на фиг. 1:




**Фиг. 1.** Принцип на работа на уеб приложение

Една от основните цели на разработваната АИС(Уеб приложението) е да се осигури бърза и надеждна комуникация между всички участници. Трябва да имат възможност да получават информация за графика, напредъка и да изпращат съобщения до конкретен потребител. Обучаваните имат възможност да наблюдават своите текущи резултати. Преподавателите трябва да могат да попълват листа с оценки, но и да е осигурена възможността за онлай изпитване и автоматично попълване на листа с оценките, да имат достъп до цялата им необходима информация и средства за комуникация в удобна за тях форма. Потребителският изглед на системата трябва да бъде внимателно разработен така, че да осигурява лесно, удобно и интуитивно използване от потребителите. Училищният администратор трябва да има възможност удобно и точно да състави график на часовете и да информира всички участници в образователния процес.

Анализирайки разгледаните принципи, подходи и методи в съществуващите системи за автоматизиране на процеси в образователната сфера, биха могли да бъдат дефинирани основните функционалности на една система, решаваща възникналите проблеми. По-долу са дефинирани основните функционални характеристики на такава система:

- Уеб базирана;
- С изградено хранилище за данни;
- С възможност за изготвяне на график на часовете;
- С възможности за записване на напредъка и присъствието на обучаваните;
- Организиран достъп на родители и обучавани до дадена информация;
- С възможност за предоставяне на становища за образователния процес;
- С възможност за изготвяне на справки на базата на наличната в системата информация.

Дадена система в образователната сфера е необходимо да дефинира следните основни категории потребители:

- обучаван;
- обучаващ;
- родител;
- институционален администратор;
- администратор на приложението.

## 4 Подходи при създаване на архитектура на АИС за управление на процеси в образователната сфера

За да се улесни разработката, поддръжката и разширяемостта на програмата чрез разделяне на отговорностите в различни компоненти, е удачно да се използва MVC архитектурата [4]. Това е програмна архитектура, в която моделът на данни на приложението, потребителският интерфейс и контролната логика са разделени на три отделни компонента, така че модификациите на един компонент да имат минимално въздействие върху другите компоненти.

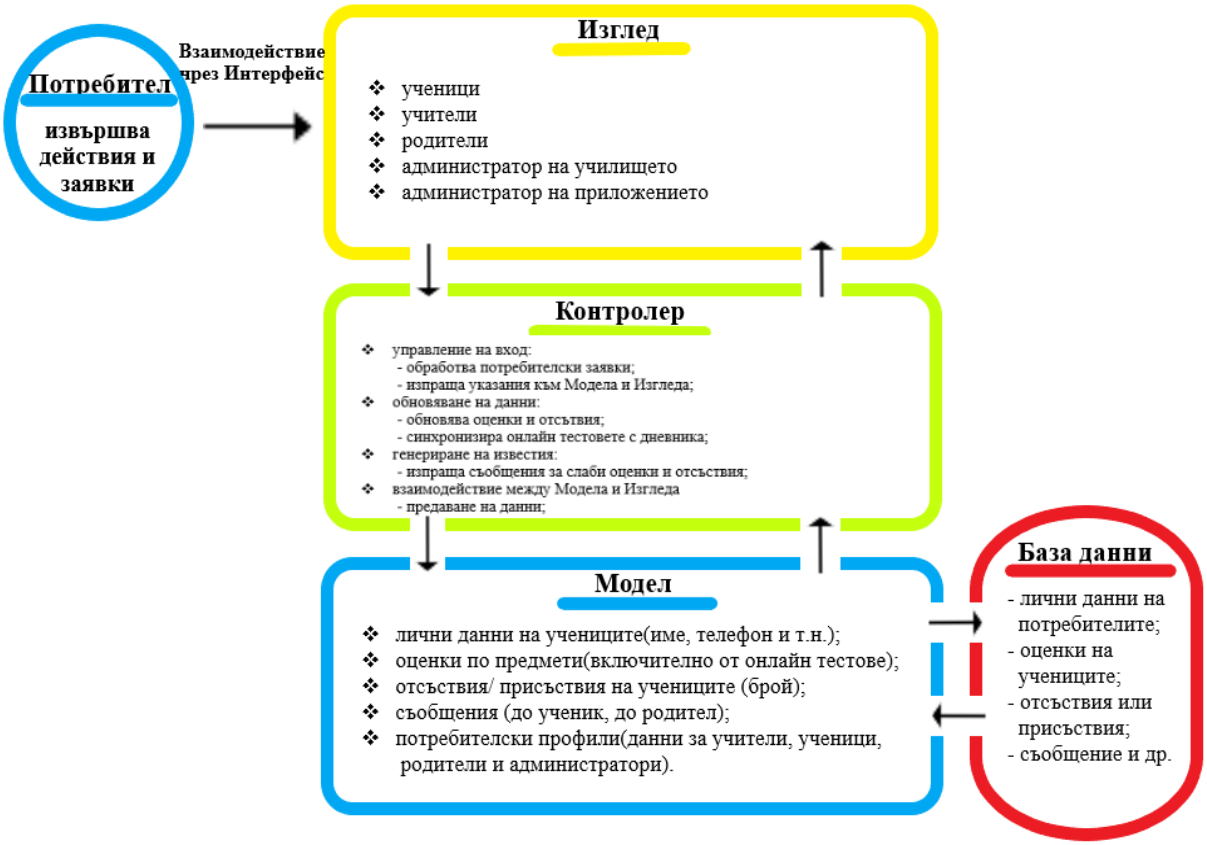



**Фиг. 2.** MVC архитектура

Моделът MVC (фиг.2) позволява да обособим обработката на данните, представянето и взаимодействието с потребителя като три отделни компонента:

- Модел(Model) - съдържа бизнес логиката и данните на приложението;
- Изглед(View) - представя потребителския интерфейс и визуализира данните;
- Контролер(Controller) - обработва входа от потребителя и управлява взаимодействието между модела и изгледа.

Автоматизираната информационна система за управление на процеси в образователната сфера, която е предмет на текущото изследване, има следната MVC архитектура (фиг.3):




**Фиг. 3.** MVC архитектура на АИС за управление на процеси в образователната сфера

**Изглед**

Изгледът е компонентът, който е отговорен за взаимодействието с потребителите. Той представя данните на потребителите по разбираем и удобен начин:

- обучавани - виждат своите оценки и отсъствия;
- преподаватели - виждат оценките на учениците и могат да въвеждат нови оценки и отсъствия;
- родители - получават информация за своето дете, включително известия за оценки и отсъствия;
- администратор на училището - управлява данните на учениците и учителите и генерира отчети;
- администратор на приложението - управлява настройките на системата и следи за системната активност.

Компонентът Изглед е основен за взаимодействието с потребителите и е отговорен за визуализацията на информацията.

**Контролер**

Контролерът е посредникът между Изгледа и Модела. Той обработва потребителските входове и изпълнява необходимите действия в системата:

- управление на входа - обработва потребителските заявки и изпраща указания към Модела и Изгледа;
- обновяване на данни - актуализира оценки и отсъствия, синхронизира онлайн тестовете с дневника;
- генериране на известия - изпраща съобщения за слаби оценки и отсъствия до родителите;
- взаимодействие между Модела и Изгледа: предава данни между тях, осигурявайки синхронизация на информацията.

Компонентът Контролер управлява логиката на приложението и гарантира, че действията на потребителите се изпълняват правилно.

**Модел**

Моделът е в основата на приложението и отговаря за обработката на данни. Той съдържа всички данни на системата и логиката за манипулиране на тези данни.

- лични данни на учениците - включва имена, контакти и друга лична информация.
- оценки по предмети - съдържа оценки от онлайн тестове, контролни и текущи изпитвания.
- отсъствия на учениците - информация за броя на отсъствията и техните детайли.
- известия и съобщения - съобщения, изпращани до родителите.
- потребителски профили -данни за учители, ученици, родители и администратори.

Този компонент е отговорен за съхраняването на данните и осигурява интерфейс за взаимодействие с тези данни.

**База данни**

База данни е физическото хранилище на всички данни на системата. Тя поддържа данните, които се използват от Модела -лични данни на учители и ученици, оценки, отсъствия, известия и съобщения, детайлна информация за потребителските профили и др. Базата данни е критична за съхраняването и управлението на данните в системата.

Предложеният модел на АИС за управление на процеси в образователната сфера автоматизира процеса по въвеждане на оценките на обучаваните, спестявайки време на преподавателите, и намалява вероятността от грешки. Някои от съществуващите платформи като Moodle и Blackboard предлагат ръчно въвеждане на оценки или ограничена автоматизация. Предложеният модел включва още автоматични известия за слаби оценки и голям брой отсъствия, което помага на родителите да следят по-ефективно напредъка на обучаваните.

# 5 Заключение

Приоритет на всяка образователна институция е да предлага високо качество на образование на обучаемите, но също така да поддържа изрядна документация, а тези отговорности изискват много време и усилия. Преподавателите и администраторите трябва да координират изискванията на планирането на уроците и проследяването на данните, а това често означава да се справят с уморителни, ръчни процеси, които отвличат вниманието от взаимодействията преподавател-обучаван.

АИС в образователната сфера могат да се доразвият чрез интегриране на дигитални работни потоци, които да автоматизират повтарящите се процеси. Когато простите задачи са напълно автоматизирани, преподавателите могат да се съсредоточат върху създаването на оптимални възможности за обучение, а автоматизираната образователна институция е по-способна да поддържа нуждите както на обучаваните, така и на преподавателите.

**ЛИТЕРАТУРА:**

[1] Adati, T., Miyazawa, T. (1977). On paracontact Riemann manifolds. TRU Math, 13 (2), pp. 27-39.

[2] Davids, D.L. (1998). Recovery effects in binary aluminum alloys, Ph.D. thesis, Harvard University.

[3] Huffman, W.C., Pless, V.S. (2003). Fundamentals of Error-Correcting Codes. Cambridge University Press.

[4] Masjukov, A.V., Masjukov, V.V., Multiscale modification of Shepard's method for multivariate interpolation of scattered data. In: Mathematical Modeling and Analysis. Proceeding of the 10th International Conference MMA2005&CMAM2, pp. 467-472.

[5] Selwyn, N., Hillman, T. (2023). Bergviken Rensfeldt, A. et al. Digital Technologies and the Automation of Education — Key Questions and Concerns. Postdigit Sci Educ 5, pp. 15–24. (https://doi.org/10.1007/s42438-021-00263-3)

[6] https://www.navet.government.bg/bg/media/strategicheska-ramka_obrobuuchene_110321-1.pdf/ (последно посетен на 21.09.2024 г.)

[7] https://moodle.org/ (последно посетен на 21.09.2024 г.)

[8] Teachers' Experience and Perceptions of Sustainable Digitalization in School Education: An Existential Phenomenological Study of Teachers in Romania, Greece, Cyprus, Iceland, and The Netherlands (https://doi.org/10.3390/su151813353) (последно посетен на 21.09.2024 г.)

# BUILDING A LAN NETWORK BETWEEN A PROGRAMMABLE LOGIC CONTROLLER AND A MICROCONTROLLER*

**DANIEL R. DENEV**

***ABSTRACT:*** *Over time, automation in industry grows more and more, simultaneously displacing the human operators. The basis of all automated processes is the programmable logic controller (PLC). This article presents an augmentation of the inputs and outputs of a Siemens Simatic S7-1500 programmable logic controller using a microcontroller Ethernet communication link. After implementing this type of communication, the number of inputs and outputs will increase exponentially and they will be able to connect different sensors. The basis of sensors hides the overall development of the industry. The amount of benefits that arise from the use of this communication are enormous, both from the financial side and from the side of flexibility and integration into different systems in the industry.*

***KEYWORDS:*** *microcontroller, Industry 4.0, programmable logic controller*

***DOI: https://doi.org/10.46687/LBMZ7342***

# ИЗГРАЖДАНЕ НА LAN МРЕЖА МЕЖДУ ПРОГРАМИРУЕМ ЛОГИЧЕСКИ КОНТРОЛЕР И МИКРОКОНТРОЛЕР

**ДАНИЕЛ Р. ДЕНЕВ**

***АБСТРАКТ:*** *С течение на времето автоматизацията в промишлеността нараства все повече и повече, като едновременно с това измества човешките оператори. Основата на всички автоматизирани процеси е програмируемият логически контролер (PLC). Този доклад представя разширение на входовете и изходите на програмируем логически контролер Siemens Simatic S7-1500, използвайки LAN комуникационна връзка към микроконтролер. След прилагането на този тип комуникация, броят на входовете и изходите ще се увеличи експоненциално и те ще могат да свързват различни сензори. В основата на сензорите се крие цялостното развитие на индустрията. Размерът на ползите, произтичащи от използването на тази комуникация, е огромен, както от финансова страна, така и от страна на гъвкавостта и интеграцията в различни системи в индустрията.*

## 1 Въведение

С развитието на мехатрониката и роботиката много технически науки започнаха да използват комуникационни протоколи. Те се намират главно сред устройствата в индустриалните системи. Дигиталната индустрия претърпява големи промени с течение на времето, особено информационните и комуникационните технологии. Тези два сектора имат голямо влияние върху всички известни технологични аспекти и са свързани с недостижими скорости през последните години. В резултат на бързото развитие разстоянието между физическия и цифровия свят става все по-малко. Този бърз прогрес ни води до нови тенденции в света на индустрията. Част от тези тенденции са Cyber-Physical Systems, Industry 4.0 и Internet of Things. Основната концепция на Индустрия 4.0 е създаването на нови правила в дигитализацията на индустриалното производство. Изискванията за използване на нови технологии ще окажат натиск върху необходимостта

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

от квалификация. Самата висока квалификация води до намиране на нови служители с превъзходни когнитивни способности и възможности. Едно от основните изисквания е дисциплинираното мислене и високият капацитет на персонала за по-лесното прилагане в практиката и тактическото разпространение на Индустрия 4.0. Основното използване на PLC в автоматизацията и мониторинга на индустриално оборудване се дължи на голямата гъвкавост във времето и дългия им живот. Със създаването на автоматизацията се уточнява, че индустриалните системи трябва да работят дълго време и с висока надеждност. Задавайки въпроса за хардуера с отворен код, Raspberry SBC Pico и микроконтролерите са устройства, които не са създадени за индустриални цели, а по-скоро за класически цели и управление. Най-познатият пример за потребителите са основно евтините платки, базирани на микроконтролер. Основна тенденция в академичните среди и изследванията превърна микроконтролерите в основен инструмент за разработване и създаване на различни индустриални приложения. По отношение на програмирането, софтуерът е основен и гъвкав и подходящ както за начинаещи, така и за напреднали потребители. По отношение на софтуера, който микроконтролерът използва, той се състои от същия IDE интерфейс, който се използва за качествено разработване на широка гама от платки. IDE е с отворен код и има удобен потребителски интерфейс. Основният език за използване и програмиране е C++, който позволява на потребителите да създават както прости, така и сложни програми. [1, 2, 3, 6, 8]

# 2 Проектиране на комуникационната хардуерна система

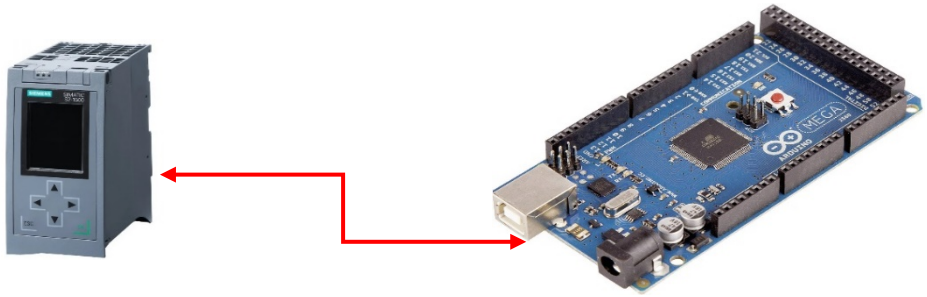
*2.1 Индустриална комуникация в перспективата на Индустрия 4.0*

За бъдещите технологии на Индустрия 4.0 инженерите трябва да подобрят всички свои професионални, социални и лични умения. Те се нуждаят от интердисциплинарни познания за производствени системи и процеси, технологии за автоматизация, информационни технологии, ергономични принципи и т.н. Бъдещият модерен инженер, който е част от Индустрия 4.0, трябва да има холистичен поглед върху сложните производствени системи. [4, 9]

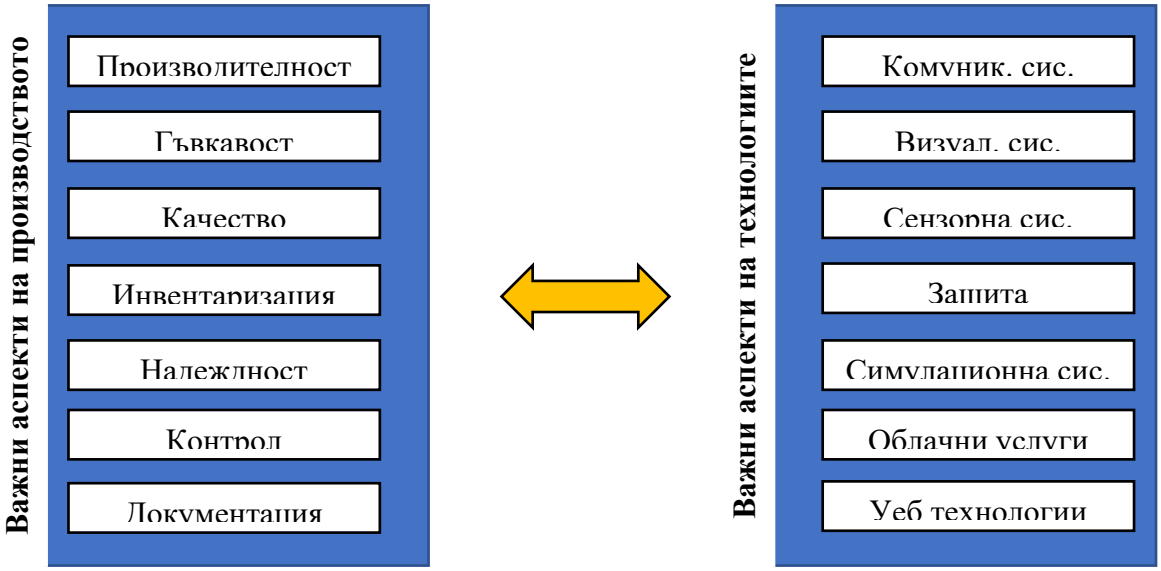
Фигура 1 показва общ преглед на комуникационна хардуерна система изградена от ПЛК и микроконтролер. Фигура 2 подчертава необходимостта от аспекти, които намират приложение в производството, технологиите и инженерните квалификации. Този доклад ще се отнася до технологията за разработване на комуникационни и индустриални интерфейси, интегрирани в Industry 4.0. В днешното съвремие техническото оборудване е обект на огромно развитие и има за цел да отстрани човека от производствената обработка. Поради този факт интегрирането на роботи в по-големи бизнеси се превръща в интензивна тенденция

*2.2 Блокова схема на комуникацията между устройствата*

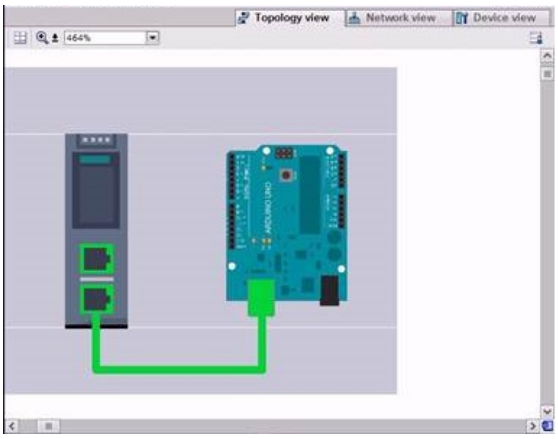
Фигура 3 показва комуникационен модел на мобилна платформа, състояща се от микроконтролерна платка и контролер Siemens S7-1500, който се използва главно в повечето промишлени предприятия. Нуждата от такава комуникация е добро решение за всеки потребител, когато иска да използва ПЛК, за да командва своите устройства или роботи. Този тип комуникация най-често се реализира чрез изпълнителни механизми. Използването на тази връзка намира широко приложение в специални сензори, по известни като жироскопични сензори. При този тип комуникация блоковите вериги се управляват от 22V Li-PO батерия с един повишаващ и един понижаващ регулатор. Повишаването се използва за захранване на ПЛК при 24V, а понижаването се използва за захранване на платката на микроконтролера при 5V.



**Фиг. 1.** Комуникационна хардуерна система




**Фиг. 2.** Аспекти свързани с производството и технологията




**Фиг. 3.** Блокова схема на комуникацията между ПЛК и микроконтролер [6]

## 3 Ethernet комуникация между ПЛК и микроконтролер

Настоящият доклад представя комуникацията между микроконтролера и ПЛК Simatic S7-1500, която се осъществява чрез Raspberry SBC Pico, тъй като предаването на данни

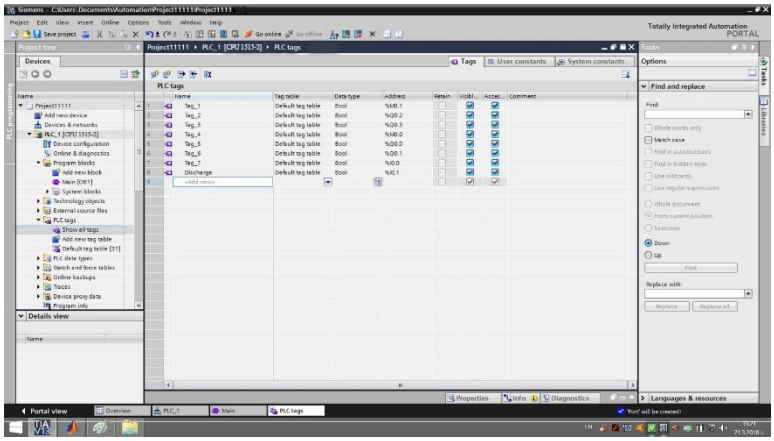
между микроконтролера и S7-1500 може да се извърши само чрез база данни, създадена в TIA Portal. Базата данни се актуализира през цялото време с нови стойности. Тъй като изчислителната мощност на платката на микроконтролера е ограничена и има доста значително забавяне. Този модел има 4 × USB 2.0 порта и разширен GPIO с 40 пина. Siemens Simatic S7-1500 PLC е индустриален програмируем контролер с 1515 DC/DC/ DC CPU −40... + 70°C с конформно покритие, базирано на 6ES7515-2AM01-0AB0. Има 2 Ethernet порта с PROFINET. Този PLC има 25 цифрови входа, 20 цифрови изхода, два аналогови входа 0–10 V и два аналогови изхода 0–20 mA. Капацитетът на паметта за програмиране е 500 KB. Една от първите стъпки в изграждането и постигането на успешна комуникация между двете устройства е инсталирането на операционна система Raspberry SBC Pico [5]. Следващата последователна стъпка е внедряването на интерфейсна програма Node-RED, която ще направи връзката между ПЛК и Raspberry SBC Pico. Node-RED е софтуерен инструмент за свързване на хардуерни устройства и програмиране. Той има прост интерфейс и предлага редактор, който позволява широк набор от възли за свързване и управление на потока от данни. След инсталиране на интерфейсната програма Node-RED е необходимо да инсталират библиотеки, специално отговорни за комуникацията с контролера Siemens Simatic S7-1500. За да инсталират такива библиотеки, са необходими няколко стъпки:

- Отворя се главната конзола за програмиране
- Изпълнява се командата cd $ HOME./node-red в Node-RED
- Командата npm install node-red-contrib-s7 и се инсталира необходимата библиотека.

След завършване на инсталационния процес е необходимо да се рестартира Raspberry SBC Pico. За успешна комуникация с PLC е необходима успешна конфигурация с добре дефиниран IP адрес. Веднага след действието е необходимо отново да се рестартира Raspberry SBC Pico. Чрез инсталиране на рутер с DHCP конфигурация е възможно да се улесни процеса на присвояване на IP. Едно от основните предимства на използването на рутер е достъпът до интернет, ако е необходимо за инсталиране на нова библиотека в Node-RED. Те могат да бъдат дефинирани като вход-изход в зависимост от това какъв тип блок е избран от Node-RED.

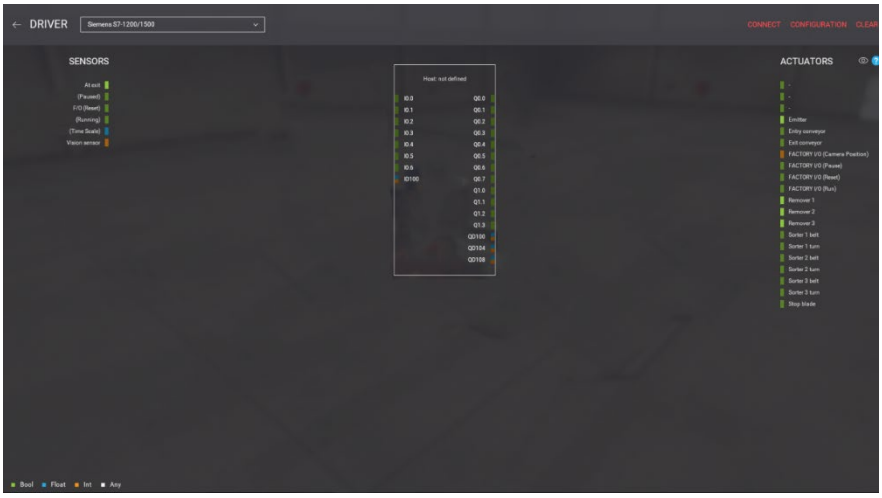
Поради факта, че Raspberry SBC Pico няма пинове предназначени за аналогови входове и изходи е необходимо да се използват по-скъпи аналогово-цифрови преобразуватели. Използването на микроконтролерна платка е изгодно за използване поради големия брой аналогови входове и изходи и цената на придобиване. Цената е ниска и софтуерната част е по-лесна за използване. Съставена е от множество специализирани библиотеки за сензори, използвани в роботиката. Комуникацията между ПЛК и микроконтролера ще се осъществява чрез Raspberry SBC Pico, използвайки цялата интерфейсна програма на Node-RED. Причината или необходимостта от такова свързване възниква поради необходимостта от интегриране в индустрията на различни видове роботи, които използват такива контролни платки за своето управление.

Микроконтролерът е по-познат на хората като микроконтролерна платка, която е проектирана с голям брой входове и изходи. Основното предимство е ниската цена, която е почти два пъти по-ниска от тази на PLC I/O модули [5]. Надеждността на този тип платки може да се увеличи чрез внедряване на стабилизирано захранване. Всеки потребител, който следва фабричните инструкции, може да използва командата npm install node-red-node-serial port, за да инсталира необходимата библиотека Node-RED. След като библиотеката за анализи е инсталирана, платката на микроконтролера се свързва чрез USB към Raspberry SBC Pico. Следващата стъпка е конфигурацията на входовете и изходите което е показано на фигура 4. [ 3, 6, 7]



**Фиг. 4.** Връзката между серийните блокове и S7 блоковете чрез тагове

Разработената микроконтролерна платка трябва да бъде програмирана с цифрова програма, която да дефинира всички входове и изходи, както и серийния порт, от който ще получава информация от PLC. В момента пин A23 действа като цифров, а пин A13 действа като аналогов. За PLC това ще бъдат входни тагове, които ще съхраняват информация от тип, подобен на IW6 и IW8. Входовете от PLC ще управляват изходите на микроконтролера. В момента тези изходи са %Q0.0, %Q0.1, %Q0.2, %Q0.3, и ще бъдат 4 класически светодиода, които ще бъдат индиректно свързани към пиновете с номера 22, 30, 38 и 46. Фигура 5 показва Активиране на връзката между серийните блокове и s7 блоковете на ПЛК. [4, 5, 6, 7, 10]




**Фиг. 5.** Активиране на връзката между серийните блокове и s7 блоковете

# 4 Заключение

Този доклад представя комуникационен модел между Siemens Simatic S7-1500 PLC и микроконтролер чрез Raspberry SBC Pico. Подобреното време за комуникация помага и улеснява за интегрирането на роботи, които не са създадени за промишлени цели в индустрията, както и предлага по-нататъшно развитие на нова концепция на Индустрия 4.0. Микроконтролерът, и Raspberry SBC Pico са евтини компоненти, които използват софтуер с отворен код и са много подходящи за научни изследвания. Подобрената комуникация

предлага на ПЛК възможността да се разшири до голям брой входове и изходи при значително по-ниски разходи, отколкото използването на специални модули за ПЛК.

**ЛИТЕРАТУРА:**

[1] Цанков Ц. С. Съвременни методи за управление на ресурси в компютърни индустриални мрежи. Университетско издателство „Епископ К. Преславски“, Шумен, 2022, 150 с., ISBN 978-619-201-618-0.

[2] Цанков Ц.С. Администриране на локални компютърни мрежи. Университетско издателство „Епископ Константин Преславски“, Шумен, 2021, 232 с., ISBN 978-619-201-472-8, COBISS.BG-ID 45390344.

[3] Ahmedova D., Konstantinova E., Tsankov Ts. The use of packet sniffing tools in computer networks security. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 401-406.

[4] Tang X., Jiang Y., System PLC programming and debugging, Chemical Industry Press, Beijing, 2017.

[5] Tsankov Ts., Staneva L., Vardeva I., Iliev D. Generalized net model of a communication network using the Port Knocking method. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 29-34.

[6] Zhang X., Man Machine Interface Equipment and Portal Software Automation Engineering Software, Chemical Industry Press, Beijing, 2017.

[7] Tudoreanu E., Designing Effective Program Visualization Tools for Reducing User’s Cognitive Effort, Proc. ACM. Software Visualization, 2003.

[8] Georgieva I., Automation Systems with Programmable Logic Controllers, Sofia, 2016.

[9] Marosan A., Constantin G., Barsan A., Crenganis M., Creating an ethernet communication between a Simatic S7-1200 PLC and Arduino Mega for an omnidirectional mobile platform and industrial equipment, IOP Conference Series Materials Science and Engineering, 2020, DOI:10.1088/1757-899X/968/1/012022.

[10] https://settimino.sourceforge.net/home.html

# THE MIMO TECHNOLOGY – MEANING, CREATION AND APPLICATION*

**ILKER A. HATIB, DANIEL R. DENEV**

***ABSTRACT:*** *This report examines the technology of MIMO (Multiple Input, Multiple Output), its essence, and its significance for modern wireless communications. MIMO utilizes multiple antennas for parallel transmission and reception of data, significantly improving the capacity, speed, and reliability of networks. The report discusses key aspects of MIMO, such as the phenomenon of multipath communication and the challenges associated with interference and signal fading. The MIMO technology was developed to address the growing demand for data, the limitations of the frequency spectrum, and the need for more stable connections in mobile networks, Wi-Fi, satellite communications, and the Internet of Things (IoT). The report presents the main applications of MIMO in 4G, 5G, Wi-Fi 6, industrial and military communications, as well as in automotive systems and autonomous vehicles. The end emphasizes the significance of MIMO for the future development of mobile networks and communication technologies as a whole, providing higher efficiency and capacity for modern and future wireless systems.*

***KEYWORDS:*** *Wi-Fi, 5G networks, MIMO*

***DOI: https://doi.org/10.46687/OGPY5143***

# ТЕХНОЛОГИЯТА MIMO – ЗНАЧЕНИЕ, СЪЗДАВАНЕ И ПРИЛОЖЕНИЕ

**ИЛКЕР А. ХАТИБ, ДАНИЕЛ Р. ДЕНЕВ**

***АБСТРАКТ:*** *Настоящия доклад разглежда технологията MIMO (Multiple Input, Multiple Output), нейната същност, както и значението ѝ за съвременните безжични комуникации. MIMO използва множество антени за паралелно предаване и приемане на данни, като значително подобрява капацитета, скоростта и надеждността на мрежите. В доклада са разгледани основни аспекти на MIMO, като феноменът многопътна комуникация и предизвикателствата, свързани с интерференцията и избледняването на сигнала. Технологията MIMO е разработена с цел да отговори на нарастващото търсене на данни, ограничеността на честотния спектър и необходимостта от по-стабилни връзки в мобилни мрежи, Wi-Fi, сателитни комуникации и Интернет на нещата (IoT). В доклада са представени основните приложения на MIMO в 4G, 5G, Wi-Fi 6, индустриални и военни комуникации, както и в автомобилни системи и автономни превозни средства. В заключение се подчертава значимостта на MIMO за бъдещото развитие на мобилните мрежи и комуникационните технологии като цяло, осигурявайки по-висока ефективност и капацитет на съвременните и бъдещи безжични системи.*

## 1 Въведение

В съвременния свят на дигитални комуникации безжичните технологии заемат централно място в развитието на глобалната свързаност. С нарастващите нужди от по-високи скорости на пренос на данни и по-ефективно използване на честотния спектър, съществува необходимост от иновативни решения, които да осигуряват по-добра производителност на мрежите. Една от най-значимите и напреднали технологии, която

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

отговаря на тези предизвикателства, е технологията MIMO (Multiple Input, Multiple Output). Тази технология използва множество антени както на страната на предавателя, така и на приемника, което позволява едновременно изпращане и получаване на данни по няколко канала.

MIMO играе ключова роля в модернизирането на мобилните и безжични комуникации. Благодарение на способността си да увеличава пропускателната способност на мрежите, без да се увеличава нуждата от допълнителен честотен спектър, MIMO се превръща в основен компонент в съвременните мрежи от четвърто и пето поколение (4G и 5G). Системите, базирани на MIMO, значително подобряват стабилността на връзката, увеличават капацитета на мрежите и минимизират смущенията. Освен това, технологията намира приложение в множество сфери – от мобилни телефони и Wi-Fi до сателитни комуникации и IoT (Интернет на нещата). [1, 3, 4, 5, 12]

Целта на настоящия доклад е да разгледа технологията MIMO и нейните ключови характеристики, да обясни как работи и какви са предимствата ѝ. Освен това ще бъде направен анализ на важността на MIMO за бъдещето на безжичните комуникации и как тя подпомага развитието на нови приложения и услуги. Технологията не само предоставя подобрени технически възможности, но и има потенциала да променя начините, по които хората и устройствата взаимодействат в глобалната мрежа.

## 2 Обща представа за технологията MIMO

MIMO (Multiple Input, Multiple Output) е иновативна технология за безжична комуникация, която позволява едновременното използване на множество антени за предаване и приемане на данни. Основната идея зад MIMO е да увеличи капацитета на безжичната мрежа чрез ефективното използване на наличния честотен спектър. Вместо данните да се предават чрез една антена, както е при традиционните системи (SISO – Single Input, Single Output), MIMO позволява използването на няколко антени на предавателя и няколко на приемника, които работят едновременно и независимо една от друга. [3]

Технологията се основава на принципите на многопътната комуникация, при която сигналите достигат до приемника по различни маршрути, като се отразяват от обекти в околната среда. Тези сигнали, макар и пренесени по различни траектории, съдържат различни части от информацията и се обработват така, че да се възстанови първоначалното съобщение. По този начин, MIMO увеличава ефективността на предаването, подобрява качеството на връзката и намалява вероятността от загуба на данниц. [2]

Една от ключовите предимства на MIMO е способността ѝ да увеличава капацитета на мрежата, без да се изисква допълнителен честотен спектър. Това е особено важно в контекста на съвременните мобилни мрежи, където честотният ресурс е ограничен. С използването на множество антени, MIMO може да постигне по-високи скорости на пренос на данни и по-голяма надеждност на сигнала, което прави технологията подходяща за приложения, изискващи големи обеми данни, като видеоконференции, стрийминг на видео с висока разделителна способност и онлайн игри.

Технологията MIMO е в основата на безжичните мрежи от ново поколение, като 4G LTE и 5G, и е една от водещите иновации, които позволяват по-висока пропускателна способност и по-добро използване на ресурсите на мрежата.

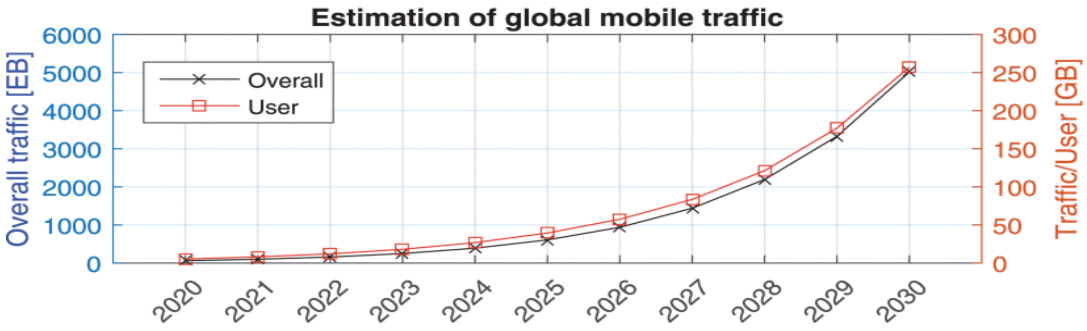
## 3 Общи причини за създаване на MIMO технологията

Наложителността на създаването на MIMO произтича от нарастващите нужди и предизвикателства пред безжичните комуникации в края на 20-ти и началото на 21-ви век. С бързото развитие на мобилните технологии, интернет, и многото свързани устройства,

традиционните комуникационни системи започнаха да срещат сериозни ограничения. Ето няколко основни причини, поради които създаването на MIMO технологията стана наложително:

- **Нарастващото търсене на капацитет и скорост**

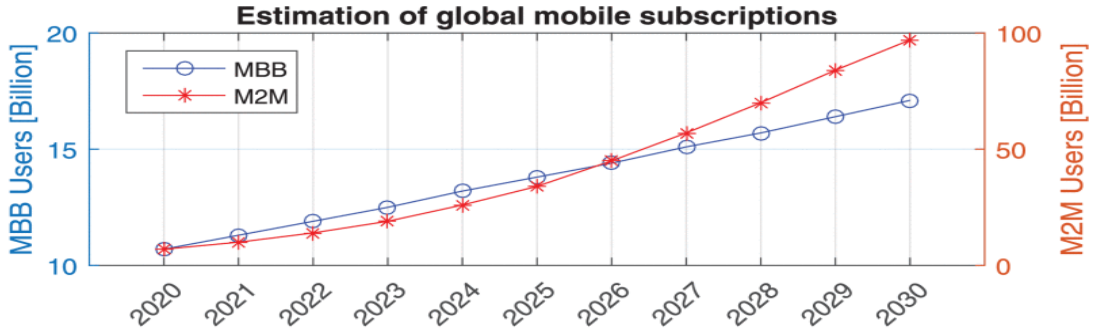
С увеличаването на броя на мобилните потребители и устройствата, както и с нарастващата популярност на приложения, създаващи голям трафик, като поточно предаване на видео, онлайн игри, видеоконференции и cloud услуги, традиционните безжични системи (SISO – Single Input, Single Output) се сблъскаха с ограничен капацитет. Един от най-големите проблеми беше ограничената скорост на пренос на данни и невъзможността да се отговори на бързо нарастващите изисквания. MIMO решава този проблем, като значително увеличава капацитета на мрежата без необходимост от допълнителен честотен спектър. Фигура 1 показва колко трафик създава индивидуален потребител през годините




**Фиг. 1.** Трафик създаден от индивидуален потребител през годините

- **Ограниченост на честотния спектър**

Безжичните комуникации зависят от определен честотен спектър, който е ограничен ресурс. С увеличаването на броя на потребителите и устройствата, наличните честотни диапазони започнаха да се запълват. Използването на по-широки честотни ленти не винаги е възможно или ефективно решение. MIMO предлага алтернативен подход, който увеличава капацитета за пренос на данни, без да изисква разширяване на използваните честотни диапазони, като използва съществуващите ресурси по-ефективно. Фигура 2 показва броят на безжично свързаните устройства. MBB(mobile broadband) са мобилни телефони, таблети, лаптопи и други, а M2M(machine-to-machine) са индустриални автоматизирани устройства, дистанционни устройства за наблюдение и други интелигентни мрежи за предаване на данни




**Фиг. 2.** Брой безжични свързвани устройства

- **Подобряване на качеството на връзката**

Един от основните проблеми на безжичните комуникации е загубата на сигнали поради интерференция, избледняване или многопътни отражения, особено в среди с много препятствия, като градски зони. Традиционните системи не можеха да се справят ефективно с тези предизвикателства, което водеше до нестабилна връзка и по-ниско качество на сигнала. MIMO използва многопътната комуникация като предимство, като обработва сигналите, получени по различни маршрути, и по този начин увеличава надеждността на връзката.

- **Еволюция на мобилните мрежи (4G и 5G)**

Преминаването от 3G към 4G и 5G изискваше значително увеличаване на скоростта на предаване и намаляване на латентността. Технологиите от следващо поколение трябваше да поддържат огромно количество свързани устройства и приложения с високи изисквания към данните (например интелигентни градове, автономни автомобили, IoT). Традиционните комуникационни методи не можеха да постигнат необходимите подобрения в производителността. MIMO, чрез множествените антени и възможността за паралелна обработка на данни, осигурява значително подобрение в ефективността на мрежите от ново поколение. [5]

- **Нуждата от енергийна ефективност**

С увеличаването на броя на безжичните устройства и предаваните данни, енергийната ефективност на мрежите стана ключов фактор. Безжичните комуникационни технологии трябваше да предложат по-добри начини за предаване на данни, като същевременно използват по-малко енергия. MIMO подобрява енергийната ефективност, тъй като позволява преноса на по-голямо количество данни за по-кратко време, намалявайки необходимостта от дълги периоди на предаване.

- **Многопътна комуникация като ресурс**

Преди разработването на MIMO, многопътните сигнали често се считаха за проблем, тъй като те можеха да предизвикат интерференция и загуба на качество на сигнала. MIMO обаче използва този феномен като предимство, като събира информацията от различните маршрути и увеличава количеството данни, които могат да се предават паралелно. Това представлява значителна технологична иновация, която преосмисля как може да се използва околната среда за подобряване на комуникационния капацитет.

# 4 Приложение на MIMO технологията

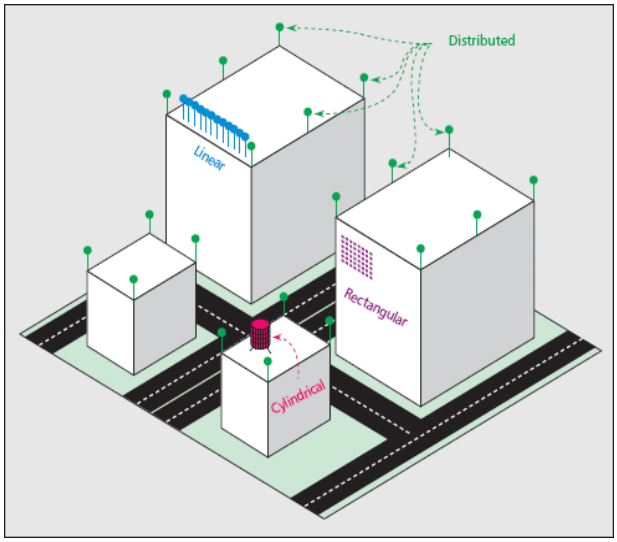
Технологията MIMO (Multiple Input, Multiple Output) намира широко приложение в съвременните безжични и комуникационни системи, благодарение на способността ѝ да увеличава капацитета, скоростта и надеждността на мрежите. Ето някои от най-изчерпателните примери за това къде и как се използва MIMO

- **Мобилни мрежи (4G, LTE и 5G):**

4G LTE (Long-Term Evolution): MIMO е в основата на 4G LTE технологията, където позволява значително увеличение на капацитета и скоростта на пренос на данни. Благодарение на MIMO, 4G мрежите могат да предоставят скорости до няколко стотин мегабита в секунда (Mbps), което прави възможни приложения като стрийминг на HD видео, видеоконференции и мобилен гейминг.

5G мрежи: В 5G мрежите MIMO играе още по-значима роля чрез използването на Massive MIMO – версия на MIMO с много повече антени (десетки до стотици антени). Това позволява обработка на голям брой едновременни връзки и значително увеличаване на капацитета на мрежата. Massive MIMO е ключов елемент за осигуряване на

висококоростен мобилен интернет и ултра-ниска латентност, необходими за приложения като автономни автомобили, виртуална реалност (VR), и Интернет на нещата (IoT).




**Фиг. 3.** Предполагаемо разполагане на множество антени в градска среда

- **Wi-Fi мрежи**

Wi-Fi 5 (802.11ac): MIMO се използва в стандартите за безжична локална мрежа (WLAN) като Wi-Fi 5, което позволява едновременното предаване на данни до множество устройства чрез технологията MU-MIMO (Multi-User MIMO). Това е изключително полезно за домакинства и офиси с много свързани устройства (смартфони, лаптопи, таблети), тъй като подобрява скоростта и стабилността на мрежата. [4]

Wi-Fi 6 (802.11ax): В новия стандарт Wi-Fi 6, MIMO е допълнително усъвършенстван. Технологията позволява по-голямо количество едновременни връзки и по-добро използване на наличния честотен спектър. Това е важно за претоварени мрежи с много свързани устройства, каквито има в големи офиси, стадиони или обществени пространства. [6]

- **Сателитни комуникации**

В сателитните комуникации MIMO се използва за подобряване на ефективността при предаване и приемане на сигнали от и до земни станции. Благодарение на многопътната комуникация и независимото предаване на различни сигнали, MIMO увеличава капацитета на сателитите, което е от полза за комуникации в отдалечени райони, морски и въздушни връзки, както и за военни и правителствени комуникации.

- **Технология за стрийминг на видео и медии**

Приложения за видео и аудиострийминг като Netflix, YouTube, и Spotify се възползват от високите скорости и стабилност, които MIMO предлага. Тази технология позволява безпроблемно предаване на видео с висока разделителна способност (HD, 4K) и аудио, дори в среди с множество свързани устройства. Това е от значение в домашни условия и за бизнес среди, където качеството на предаването е критично за потребителското изживяване.

- **Интернет на нещата (IoT)**

MIMO е ключова технология в системите за Интернет на нещата (IoT), където милиарди устройства са свързани към интернет и обменят данни в реално време. В сфери

като индустриална автоматизация, умни градове, интелигентни домове и здравеопазване, MIMO позволява по-добра свързаност и ефективност на мрежите, като увеличава капацитета за комуникация и намалява закъсненията.

- **Автомобилни системи и автономни превозни средства**

Автономни автомобили: Автомобилите от ново поколение разчитат на високоскоростни комуникации, за да се свързват с други автомобили и инфраструктурата (V2X – Vehicle-to-Everything). MIMO е жизненоважен за тези комуникации, тъй като гарантира надеждна и бърза връзка, необходима за безопасността и навигацията на автономните автомобили.

Развлекателни системи в автомобилите: MIMO също така се използва в безжичните развлекателни системи в модерните автомобили, които предоставят интернет достъп и стрийминг на медийно съдържание на пътниците. Фигура 4 Показва автомобили, които си комуникират, за да се избегне проишествие и в същото време комуникират с облак и/или интернет мрежата. [2, 6, 10, 11]



**Фиг. 4.** Комуникация на автомобили чрез облак

- **Комуникационни системи за индустриални приложения**

В индустриални среди MIMO е използвано за създаването на стабилни и високоефективни комуникационни мрежи в заводи и фабрики. Технологията помага за осигуряване на надеждност на комуникациите в среди с много смущения и препятствия, което е важно за роботизираните системи и автоматизацията на производството.

- **Военни и правителствени комуникации**

MIMO се използва широко в военни комуникации, където сигурността и надеждността на връзката са от първостепенно значение. Многопътната комуникация позволява по-надеждно предаване на сигнали дори в предизвикателни среди, като градски райони или планински терени, където обикновените системи биха срещнали трудности.

- **Телекомуникации и клетъчни базови станции**

Базовите станции в клетъчните мрежи също използват MIMO, за да подобрят качеството на връзката и да обслужват по-голям брой потребители. Технологията позволява на клетъчните оператори да увеличат капацитета на своите мрежи, без да инвестират в допълнителни честотни ресурси, което е особено важно в градските зони с висока плътност на потребителите.

- **Дронове и безпилотни летателни апарати (БЛА)**

Дроновете, използвани за наблюдение, логистика и други приложения, разчитат на стабилна безжична връзка за предаване на данни и управление. MIMO увеличава ефективността на комуникацията между дроновете и наземните станции, като осигурява надеждна връзка дори при наличие на препятствия или смущения в градска среда.

# 5 Заключение

Технологията MIMO (Multiple Input, Multiple Output) представлява съществено постижение в областта на безжичните комуникации, което е променило начина, по който се предават и приемат данни в съвременните мрежи. Тя е разработена в отговор на нарастващото търсене на по-голям капацитет, по-високи скорости и по-надеждни връзки, необходими за справяне с предизвикателствата, свързани с ограниченията на честотния спектър и многопътните интерференции. MIMO позволява ефективно използване на многопътната комуникация и дава възможност за паралелно предаване на данни през множество антени, което значително увеличава капацитета на мрежата без нужда от допълнителни честоти.

Приложенията на MIMO са разнообразни и обхващат голям брой индустрии и технологии. В мобилните мрежи, MIMO играе основна роля както в 4G LTE, така и в 5G, като допринася за осигуряване на по-високи скорости на пренос на данни, по-голяма пропускателна способност и по-ниска латентност. В Wi-Fi мрежите, технологията подобрява свързаността на множество устройства едновременно, което е критично в претоварени мрежи като обществени пространства и офиси. Освен това, MIMO намира приложение в сателитни комуникации, стрийминг на медии, Интернет на нещата (IoT), автономни превозни средства и дори в индустриални и военни комуникационни системи.

Едно от основните предимства на MIMO е способността ѝ да използва многопътната комуникация, която преди се е смятала за пречка, като я трансформира в ресурс за подобряване на комуникациите. Технологията не само увеличава скоростта на предаване, но и повишава надеждността и устойчивостта на връзките, дори в среди с голяма интерференция или препятствия. Тя също така подпомага енергийно ефективни комуникации, което е от съществено значение за съвременните мрежи с множество свързани устройства.

Развитието на MIMO стана наложително в контекста на бързо растящите нужди от данни, мобилност и сигурност, като тя осигури решения на критични предизвикателства пред комуникационните технологии. С напредъка на мобилните мрежи към 5G и нарастващото значение на свързаните устройства в IoT, MIMO ще продължи да бъде в основата на бъдещите иновации в безжичните комуникации. [7, 8, 9]

В заключение, MIMO не само подобри съществуващите комуникационни мрежи, но също така проправи пътя към нови технологични възможности и значително повиши ефективността на безжичните системи. Тя остава ключова технология за справяне с предизвикателствата на съвременния цифров свят и е основен двигател на бъдещото развитие в сферата на комуникациите.

**ЛИТЕРАТУРА:**

[1] Al-Fuqaha A., Guizani M., Mohammadi M., Internet of Things: A Survey on Enabling Technologies, Protocols and Applications, 2015, Published in: IEEE Communications Surveys & Tutorials Volume 17, Electronic ISSN: 1553-877X DOI https://doi.org/10.1109/COMST.2015.2444095, pp. 2347 – 2376.

[2] Bablu S., Sathvik B., Narendra Kh., Optimizing Communication in High-Speed Train Environments over 5G Signals through MIMO Base Station Positioning, 2024, International Conference on Advancements in Power, Communication and Intelligent Systems, Electronic ISBN:979-8-3503-6328-9 DOI https://doi.org/10.1109/APCI61480.2024.10617134, pp. 275-280.

[3] Di Renzo M., Haas H., Ghrayeb A., Spatial Modulation for Generalized MIMO: Challenges, Opportunities, and Implementation, 2014, Published in: Proceedings of the IEEE Volume 102, Print ISSN: 0018-9219 DOI https://doi.org/ 10.1109/JPROC.2013.2287851, pp. 56 – 103.

[4] Duarte M., Dick C., Sabharwal As., Experiment-Driven Characterization of Full-Duplex Wireless Systems, 2012, Published in: IEEE Transactions on Wireless Communications Volume 11, Print ISSN: 1536-1276 DOI https://doi.org/10.1109/TWC.2012.102612.111278, pp. 4296 – 4307.

[5] Gupta A., Jha R., A Survey of 5G Network: Architecture and Emerging Technologies, 2015, Published in IEEE Access Volume 3, Electronic ISSN: 2169-3536 DOI https://doi.org/10.1109/ACCESS.2015.2461602, pp. 1206 – 1232.

[6] Hristova E., Tsankov Ts. Routing in WDM networks. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 179-187.

[7] Hristova E., Tsankov Ts. WDM way to increase channel throughput. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 125-131.

[8] Jiang W., Bin H., The Road Towards Wi-Fi 6: A Comprehensive Survey, 2021, Published in: IEEE Open Journal of the Communications Society Volume 2, Electronic ISSN: 2644-125X DOI https://doi.org/10.1109/OJCOMS.2021.3057679, pp. 334 – 366.

[9] Larsson E., Edfors O., Tufvesson F., Massive MIMO for Next Generation Wireless Systems, 2014, IEEE Communications Magazine Volume: 52 Issue: 2, Print ISSN: 0163-6804 https://doi.org/10.1109/MCOM.2014.6736761, pp. 186 – 195.

[10] Rangan S., Rappaport T., Erkip E., Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges, 2014, Published in: Proceedings of the IEEE Volume 102, Print ISSN: 0018-9219 DOI https://doi.org/10.1109/JPROC.2014.2299397, pp. 366 – 385.

[11] Tsankov Ts., Hristova E. Wavelength assignment for WDM networks. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 87-91.

[12] Tsankov Ts., Hristova E. Routing and wavelength assignment for survivable networks. Annual of Konstantin Preslavski University of Shumen, Vol. XIII E, Faculty of technical sciences, 2023, ISSN 1314-8818, pp. 183-195.

# EVOLUTION AND CHALLENGES IN THE DEVELOPMENT OF 5G NETWORKS – TECHNOLOGIES, SECURITY AND FUTURE APPLICATIONS*

**ILKER A. HATIB**

***ABSTRACT:*** *The introduction of 5G networks marks a new stage in the development of wireless technologies, bringing with it the potential for significantly higher data rates, lower latency and a greater density of connected devices. The evolution of 5G networks has seen the integration of advanced technologies such as massive MIMO, millimeter waves and decentralized architecture. However, this progress is accompanied by a number of challenges related to security, as well as the complexity of the global infrastructure. 5G networks are subject to new threats, such as cyberattacks on IoT devices and vulnerabilities in communication protocols. On the other hand, their applications in industries such as autonomous vehicles, healthcare and smart cities show unprecedented possibilities for the transformation of the modern world. This article analyzes the main technological aspects of 5G, the security challenges and the expected future applications that will shape the future of the connected society.*

***KEYWORDS:*** *5G networks, IoT devices, security*

***DOI: https://doi.org/10.46687/NHRG4209***

# ЕВОЛЮЦИЯ И ПРЕДИЗВИКАТЕЛСТВА В РАЗВИТИЕТО НА 5G МРЕЖИ – ТЕХНОЛОГИИ, СИГУРНОСТ И БЪДЕЩИ ПРИЛОЖЕНИЯ

**ИЛКЕР А. ХАТИБ**

***АБСТРАКТ:*** *Въведението на 5G мрежите отбелязва нов етап в развитието на безжичните технологии, носещи със себе си потенциала за значително по-високи скорости на предаване на данни, по-ниска латентност и по-голяма плътност на свързани устройства. В еволюцията на 5G мрежите се наблюдава интеграция на напреднали технологии като масивен MIMO, милиметрови вълни и децентрализирана архитектура. Въпреки това, този прогрес е съпроводен с редица предизвикателства, свързани със сигурността, както и със сложността на глобалната инфраструктура. 5G мрежите са обект на нови заплахи, като кибератаки върху IoT устройствата и уязвимости в протоколите за комуникация. От друга страна, техните приложения в индустрии като автономни превозни средства, здравеопазване и умни градове показват безпрецедентни възможности за трансформация на съвременния свят. Този доклад анализира основните технологични аспекти на 5G, предизвикателствата в областта на сигурността и очакваните бъдещи приложения, които ще оформят бъдещето на свързаното общество.*

## Въведение

В съвременния свят, където свързаността играе все по-ключова роля в ежедневието ни, 5G мрежите представляват критичен етап в еволюцията на комуникационните технологии. Тази пета генерация на мобилни мрежи обещава да донесе фундаментални

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

промени в начина, по който комуникираме и взаимодействаме с цифровия свят. С 5G се отварят нови хоризонти за различни индустрии, включително автомобилната, здравеопазването, интелигентните градове и развлекателната индустрия, благодарение на ултрависоките скорости на предаване на данни, ниската латентност и възможността за масово свързване на милиарди устройства в реално време. [6]

Една от основните иновации, която отличава 5G от предишните поколения мобилни мрежи, е използването на нови радиочестотни спектри, включително милиметровите вълни, които позволяват значително увеличаване на капацитета и скоростта на мрежата. В допълнение, технологии като MIMO (Multiple Input Multiple Output) и beamforming играят ключова роля за подобряване на ефективността и стабилността на 5G връзките, особено в гъсто населени урбанизирани райони.

Въпреки тези технологични напредъци, внедряването на 5G мрежите не е без своите предизвикателства. Освен сложността на изграждането и поддръжката на новата инфраструктура, 5G също така поставя нови изисквания към сигурността и поверителността на данните. С увеличаването на броя на свързаните устройства и приложения, които разчитат на 5G, рисковете от кибератаки и нарушения на сигурността се увеличават значително. Това изисква прилагането на нови, по-усъвършенствани мерки за защита и регулация, които да гарантират безопасността на потребителите и устойчивостта на мрежата. Фигура 1 показва обща приложимост на 5G мрежите.

Освен технологичните и сигурностни предизвикателства, 5G също така е изправена пред социални и икономически въпроси. Въпреки че технологията обещава големи ползи, нейното внедряване е свързано с високи разходи и неравномерно разпределение на достъпа до нея, което може да задълбочи съществуващите дигитални неравенства. В същото време, бъдещите приложения на 5G, като автономните превозни средства, дистанционната медицина и виртуалната реалност, поставят допълнителни изисквания и предизвикателства пред развитието на тази технология. [2, 3, 4, 10, 11]

Този доклад има за цел да разгледа в дълбочина еволюцията на 5G мрежите, като акцентира върху технологиите, които ги правят възможни, предизвикателствата, свързани със сигурността и регулациите, както и потенциалните бъдещи приложения, които тази технология ще отключи. Чрез анализ на тези аспекти, ще се опитаме да разберем не само как 5G променя настоящето, но и как ще оформи бъдещето на глобалната свързаност.




**Фиг. 1.** Обща приложимост на 5G мрежите [9]

## 1. Еволюция на 5G

Еволюцията на мобилните мрежи е белязана от значителни скокове в технологията, като всяко ново поколение носи със себе си промени, които не само подобряват съществуващите услуги, но и отварят нови възможности за иновации и развитие. Началото на мобилните комуникации с 1G през 80-те години на миналия век осигуряваше само аналогова гласова връзка, следвана от дигиталната революция на 2G, която въведе текстовите съобщения и основните мобилни данни. 3G донесе мобилния интернет и даде тласък на първите приложения за смартфони, докато 4G LTE предостави скорости, които направиха възможно масовото стрийминг на видео, висококачествени гласови повиквания през интернет (VoIP) и разпространението на мобилни приложения, базирани на големи обеми данни. На Фиг.2 и Таб. 1 е показана еволюцията и параметрите на мрежите. [4]

С настъпването на 5G мрежите, тази еволюция достига ново ниво, което не просто надгражда съществуващите технологии, а изцяло променя парадигмата на мобилните комуникации. 5G е проектирана да се справи с нарастващите нужди за свързаност в един свят, където не само хората, но и милиарди устройства са постоянно свързани в глобална мрежа. Докато 4G LTE се фокусира върху скоростта и ефективността на предаване на данни за мобилни устройства, 5G е много по-мащабен проект, който включва внедряване на нови радиочестотни спектри, включително тези в милиметровия обхват (над 24 GHz), които предоставят значително по-голям капацитет и пропускателна способност.

***Таблица 1:*** *Основни параметри на мрежите*

| ***Поколение*** | ***Години на внедряване*** | ***Основни технологии и характеристики*** | ***Скорост на предаване на данни*** | ***Приложения и възможности*** |
|---|---|---|---|---|
| 1G | 1980-те | Аналогова гласова връзка | До 2.4 Kbps | Само гласови обаждания |
| 2G | 1990-те | Дигитализация, GSM, текстови съобщения (SMS), мобилни данни (GPRS) | До 64 Kbps | Текстови съобщения, базови мобилни данни |
| 3G | 2000-те | UMTS, HSPA, мобилен интернет | До 2 Mbps | Интернет на мобилни устройства, видео разговори, първи смартфон приложения |
| 4G LTE | 2010-те | LTE (Long-Term Evolution), високи скорости | До 1 Gbps | Видео стрийминг, VoIP, мобилни приложения с голям обем данни |
| 5G | 2020-те | Нови честоти (включително милиметрови вълни), масивен MIMO, ниска латентност | Над 10 Gbps | IoT, автономни превозни средства, умни градове, приложения с изкуствен интелект и виртуална реалност |




**Фиг. 2.** Еволюция на мрежите [8]

## 2. Хардуерните иновации

Хардуерните иновации, внедрени в 5G мрежите, са ключови за постигането на значително подобрена производителност, капацитет и ефективност в сравнение с предишните поколения мобилни мрежи. Ето някои от най-важните хардуерни технологии, които формират основата на 5G:

- **Милиметрови вълни (mmWave):** Една от най-революционните хардуерни иновации в 5G е използването на милиметрови вълни. Тези радиочестотни спектри, разположени в диапазона от 24 GHz до 100 GHz, осигуряват значително по-голям капацитет за пренос на данни в сравнение с традиционните честоти, използвани в 4G и по-ранните технологии. Милиметровите вълни обаче имат по-къс обхват и са по-чувствителни към препятствия като стени и дървета, което изисква използването на множество базови станции и малки клетки за осигуряване на достатъчно покритие.
- **Масивни MIMO (Multiple Input Multiple Output):** MIMO технологията, въведена в 4G, е значително подобрена в 5G чрез концепцията за масивни MIMO. Тази технология използва десетки, а понякога и стотици антени на една базова станция, за да предава и приема множество сигнали едновременно. Това не само увеличава капацитета на мрежата, но също така подобрява стабилността и качеството на връзката, особено в гъсто населени райони. Масивните MIMO антени могат да формират "лъчи" от сигнали, насочени към конкретни потребители или устройства, което минимизира смущенията и оптимизира използването на спектъра.
- **Beamforming (Формиране на лъчи):** Beamforming е техника, която използва масивните MIMO антени за насочване на радиовълните директно към целевото устройство, вместо да разпръсква сигнала равномерно във всички посоки. Това позволява по-добра ефективност на спектъра и намаляване на загубите при предаването на данни, особено в гъсти урбанизирани среди, където сигналите могат да се сблъскват с множество прегради и смущения. [10]
- **Small Cells (Малки клетки):** За да компенсира по-краткия обхват на милиметровите вълни, 5G мрежите използват голям брой малки клетки – компактни базови станции, които могат да бъдат инсталирани на улични стълбове, сгради и други инфраструктурни елементи. Малките клетки позволяват осигуряване на плътно покритие и поддържане на високи скорости в райони с висока плътност на потребителите. Те са особено важни за предоставянето на 5G услуги в градски условия, където традиционните макро базови станции може да не са достатъчни.
- **Edge Computing (Гранични изчисления):** Докато Edge computing не е строго хардуерна иновация, тя представлява критичен елемент в архитектурата на 5G мрежите. Граничните изчисления позволяват обработката на данни да се извършва по-близо до източника на тези данни – често директно в малките клетки или други мрежови елементи. Това значително намалява латентността и улеснява

предоставянето на приложения, изискващи почти мигновена реакция, като автономни автомобили или дистанционна хирургия.

- **Advanced Antenna Systems (AAS):** Усъвършенстваните антени в 5G мрежите са оборудвани с технологии като активни антени, които могат да регулират силата на сигнала и ъгъла на излъчване в реално време. Тези системи позволяват по-добро управление на мрежовия трафик и адаптация към динамични условия, като например движенията на потребителите или промени в околната среда. Активните антени играят ключова роля в осигуряването на стабилна и високопроизводителна 5G връзка.
- **Network Slicing (Разделяне на мрежата):** Network slicing е метод, чрез който една физическа 5G мрежа може да бъде "разделена" на множество виртуални мрежи, всяка от които е оптимизирана за специфични видове трафик и приложения. Тази технология се реализира чрез комбинация от софтуерни и хардуерни иновации, позволяващи на операторите да предоставят различни нива на услуги (например висока скорост за стрийминг или ниска латентност за игри) в рамките на една и съща физическа инфраструктура.

Тези хардуерни иновации са в основата на революцията, която 5G носи, като не само значително увеличават производителността на мобилните мрежи, но и отварят нови възможности за развитие на приложения и услуги, които преди това бяха немислими. Освен хардуерните иновации, 5G включва и значителни софтуерни промени. Софтуерно дефинираните мрежи (SDN) и мрежовата функция за виртуализация (NFV) позволяват по-гъвкаво управление на мрежовите ресурси, като същевременно намаляват необходимостта от физически хардуер. Тези технологии дават възможност за бърза адаптация на мрежата към различни сценарии и изисквания, като улесняват внедряването на нови услуги и приложения. Латентността в 5G мрежите може да бъде намалена до под 1 милисекунда, което отваря врати за нови възможности, които предишните поколения мрежи не можеха да поддържат. Също така, 5G мрежите са проектирани да поддържат изключително голям брой свързани устройства на квадратен километър – до 1 милион устройства в сравнение с около 100 000 при 4G. Това прави 5G особено подходяща за Интернет на нещата (IoT), където милиарди сензори, камери и други устройства ще бъдат свързани в реално време, създавайки нови възможности за автоматизация. На Фиг. 3 са изобразени част от хардуерните иновации. [1, 12, 13]

## 3. Технологични предизвикателства и решения

Внедряването на 5G мрежите обещава да трансформира мобилните комуникации и да създаде нови възможности за свързаност, но този процес не е без своите значителни технологични предизвикателства. Всяко от тези предизвикателства изисква иновативни решения, за да може 5G да реализира пълния си потенциал.

На Фиг.4 са показани някои от основните предизвикателства и съответните им решения:

- **Ограничен обхват и проникване на сигнала**

***Предизвикателство:*** Използването на милиметрови вълни (mmWave) в 5G мрежите осигурява по-голям капацитет и скорости на предаване на данни, но също така води до значително по-кратък обхват на сигнала и слабо проникване през физически прегради като стени и стъкло. Това прави трудно покриването на големи и вътрешни пространства с традиционните макро базови станции.

***Решение:*** За справяне с този проблем, 5G мрежите използват малки клетки (small cells), които са компактни базови станции, разположени на по-малки разстояния една от

друга, често в рамките на градска среда. Те позволяват по-плътно покритие и поддържане на високи скорости на предаване на данни в гъсто населени райони. Освен това, технологии като beamforming и масивни MIMO помагат за насочване на сигнала и минимизиране на загубите при предаването.



**Фиг. 3.** Представяне на хардуерни иновации [1]



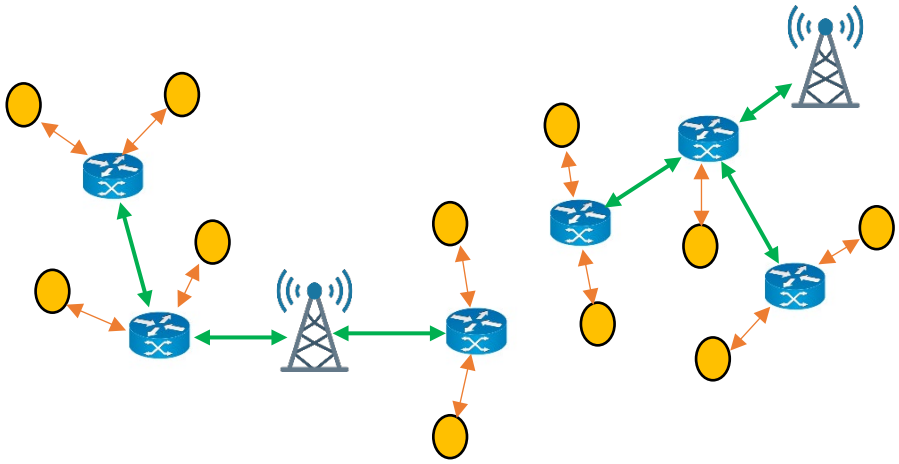

**Фиг. 4.** Схема на технологични предизвикателства

- **Високи изисквания за енергийна ефективност**

***Предизвикателство:*** 5G мрежите изискват значително повече енергия, особено при използването на технологии като масивни MIMO и beamforming, които изискват по-голяма изчислителна мощност и енергия за управление на множество антени и предаване на сигнали. Това води до увеличени оперативни разходи и въздействие върху околната среда.

***Решение:*** Енергийната ефективност на 5G може да бъде подобрена чрез използване на интелигентни системи за управление на енергията и нови материали за производство на компоненти [3]. Софтуерно дефинираните мрежи (SDN) и виртуализацията на мрежовите функции (NFV) също допринасят за по-ефективно управление на енергията, като позволяват динамично управление и оптимизация на мрежовите ресурси според текущите

нужди. Освен това, разработването на по-ефективни полупроводникови материали и компоненти, като GaN (галий нитрид) транзистори, също може да помогне за намаляване на консумацията на енергия.



**Фиг. 5.** Реализация на енергийна ефективност

- **Киберсигурност и защита на данните**

***Предизвикателство:*** С разширяването на 5G мрежите и свързването на милиарди устройства, включително критични инфраструктури и IoT устройства, рисковете за сигурността на данните и кибератаки нарастват значително [2]. Хакерите могат да използват слабости в мрежата, за да извършват атаки, което би могло да доведе до масови нарушения в услуги и данни.

***Решение:*** За да се справят с тези заплахи, 5G мрежите включват нови протоколи за сигурност и механизми за криптиране, които защитават данните както при предаването, така и при обработката им в мрежата. Мрежовото сегментиране чрез Network Slicing също допринася за подобряване на сигурността, като отделя различните видове трафик и приложения в независими виртуални мрежи. Това позволява по-добър контрол и защита на критичните услуги. Освен това, внедряването на механизми за откриване и реагиране на заплахи в реално време е ключово за поддържане на високи нива на сигурност в 5G. [5]

- **Инфраструктурни изисквания и разходи**

***Предизвикателство:*** Внедряването на 5G мрежи изисква значителни инвестиции в нова инфраструктура, включително изграждане на множество базови станции, малки клетки и нови мрежови компоненти. Освен това, интеграцията на 5G с вече съществуващите мрежи (например 4G LTE) също изисква значителни усилия и разходи, особено в селските и труднодостъпни райони, където покритието е ограничено.

***Решение:*** Едно от решенията на този проблем е сътрудничеството между мобилните оператори и правителствата за споделяне на разходите и инфраструктурата. Това включва съвместно изграждане на базови станции и споделяне на малки клетки в райони с ниска плътност на населението. В допълнение, използването на виртуални мрежи и софтуерно дефинирани технологии позволява по-гъвкаво и икономично разгръщане на 5G мрежите, като намалява необходимостта от нови хардуерни инвестиции.

- **Съвместимост и стандартизация**

***Предизвикателство:*** Един от големите предизвикателства при внедряването на 5G е гарантирането на съвместимост между различните мрежови компоненти и устройства,

особено когато става дума за глобалното разпространение на технологията. Различните региони използват различни честотни ленти и стандарти, което може да доведе до проблеми с интероперативността и ефективността на мрежата.

***Решение:*** Стандартизационни организации като 3GPP (3rd Generation Partnership Project) играят ключова роля в разработването и налагането на глобални стандарти за 5G. Те гарантират, че оборудването и устройствата от различни производители могат да работят заедно ефективно. Също така, производителите на устройства и мрежови компоненти работят в тясно сътрудничество, за да гарантират, че техните продукти отговарят на тези стандарти и са съвместими помежду си.

- **Управление на радиочестотния спектър**

***Предизвикателство:*** Радиочестотният спектър е ограничен ресурс, който трябва да бъде споделян между различни комуникационни технологии и потребители. За 5G мрежите е критично важно да имат достъп до достатъчно честотни ленти, включително нови и неизползвани досега спектри, като тези в милиметровия диапазон.

***Решение:*** Едно от решенията за ефективно управление на спектъра е динамичното разпределение на честотите, което позволява на мрежата да използва наличните ресурси по най-оптимален начин. Технологии като Dynamic Spectrum Sharing (DSS) позволяват на 5G и предишните поколения мрежи (например 4G) да споделят една и съща честотна лента, което улеснява прехода към новата технология и намалява необходимостта от допълнителни спектри.

Тези технологични предизвикателства представляват само част от комплексността на внедряването на 5G мрежите. Въпреки това, с подходящи решения и иновации, тези бариери могат да бъдат преодолени, което ще позволи на 5G да постигне пълния си потенциал и да промени начина, по който светът комуникира и използва технологиите.

## Заключение

Развитието на 5G мрежите бележи критичен момент в еволюцията на мобилните комуникации, предоставяйки възможност за значителни технологични пробиви в редица области. С възможността за по-високи скорости, минимална латентност и свързване на милиони устройства, 5G има потенциал да трансформира индустрии като здравеопазване, автомобилостроене, производство, образование и забавление, като направи възможни нови приложения и бизнес модели, които преди това бяха непостижими. Тази мрежа от пето поколение предоставя основата за бъдещи иновации, като автономни автомобили, дистанционни хирургически операции, интелигентни градове и индустриален интернет на нещата (IIoT). [5, 6, 7, 8, 9]

Въпреки огромния си потенциал, 5G технологиите срещат и значителни предизвикателства. Проблемите, свързани с изграждането на инфраструктурата, сигурността на мрежата, енергийната ефективност и социалното неравенство при достъпа до 5G, трябва да бъдат решени с цел пълноценно внедряване на технологията. Въвеждането на 5G изисква сериозни инвестиции както от страна на телекомуникационните оператори, така и от правителствата, които трябва да подкрепят процеса чрез подходящи регулации и политики за насърчаване на иновациите и конкуренцията.

От технологична гледна точка, новите решения като малки клетки, edge computing, beamforming и масивни MIMO са ключови за постигане на по-добро покритие и оптимизирана енергийна ефективност. Подобрените мерки за киберсигурност, включително криптиране и усъвършенствани протоколи за защита, са от съществено

значение за справяне с нарастващите рискове, свързани с по-голямата свързаност и увеличените обеми данни.

В заключение, докато 5G технологията предлага огромни възможности за глобална свързаност и икономическо развитие, нейното успешно внедряване и развитие зависят от съвместните усилия на индустрията, правителствата и обществото като цяло. Справянето с предизвикателствата, свързани с инфраструктурата, сигурността и достъпа, ще бъде критично за пълното разгръщане на потенциала на 5G. Въпреки че остава много работа, перспективите пред 5G са повече от обещаващи и могат да се превърнат в основен двигател на бъдещия икономически и социален прогрес.

**ЛИТЕРАТУРА:**

[1] Al-Falahy N., Omar Y., Millimetre Wave Frequency Band as a Candidate Spectrum for 5G Network Architecture: A survey, 2019, Physical Communication Volume 32, https://doi.org/10.1016/j.phycom.2018.11.003, pp. 120-144

[2] Denev D., Konstantinova E., Main Issues in the Protection of Information in the system of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.

[3] Denev D., Overview of the Modules for Building a Wireless Sensor Network, 2022, Conference with international participation MATTEH 2022, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 52-57.

[4] Denev D., Konstantinova E., Development of a 5G Model of Communication in Computer Networks, 2020, International scientific refereed online journal SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71, ISSN 2367-5721, pp. 1-10.

[5] Denev D., Modeled Security in Communication Network Coding, 2022, Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, ISSN 1311-834X, pp. 153-161.

[6] Denev D., Tsankov Ts., Use of Cisco Packet Tracer in Evaluation of Communication Networks, 2023, XVI International Scientific Conference, Belovo, ISBN 978-5-00137-315-5 (item 1), ISBN 978-5- 00137-314-8, pp. 163-171.

[7] Hristova E., Denev D., WDM Wavelength Routing Networks in Practice, 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 139-146.

[8] Hristova E., Tsankov Ts. Routing in WDM networks. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 179-187.

[9] Hristova E., Tsankov Ts. WDM way to increase channel throughput. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 125-131.

[10] Tsankov Ts., Hristova E. Wavelength assignment for WDM networks. Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, 2022, ISSN 1311-834X, pp. 87-91.

[11] Hong W., Jiang Z., Chao Y., The Role of Millimeter-Wave Technologies in 5G/6G Wireless Communications, 2021, IEEE Journal of Microwaves Volume: 1 Issue: 1, ISSN: 2692-8388, https://doi.org/10.1109/JMW.2020.3035541, pp. 101 - 122

[12] Larsson E., Edfors O., Tufvesson F., Massive MIMO for Next Generation Wireless Systems, 2014, IEEE Communications Magazine Volume: 52 Issue: 2, Print ISSN: 0163-6804 https://doi.org/10.1109/MCOM.2014.6736761, pp. 186 – 195

[13] Singh B., Bhat S., Khatri N., Optimizing Communication in High-Speed Train Environments over 5G Signals through MIMO Base Station Positioning, 2024, International Conference on Advancements in Power, Communication and Intelligent Systems, ISBN:979-8-3503-6328-9, pp. 114-120

# COMPUTER VISION – METHOD OF ACTION AND ITS APPLICATION IN THE WORLD OF TECHNOLOGY*

**KRASIMIR I. HRISTOV, TANER B. YAZADZHIEV**

***ABSTRACT:*** *Computer vision algorithms are some of the most transformative and powerful AI systems in the world today. Computer vision systems are used in autonomous vehicles, robot navigation, facial recognition systems, and more.*

***KEYWORDS:*** *AI systems, autonomous vehicles, computer vision algorithms*

***DOI: https://doi.org/10.46687/GAGW3287***

# КОМПЮТЪРНО ЗРЕНИЕ – МЕТОД НА ДЕЙСТВИЕ И НЕГОВОТО ПРИЛОЖЕНИЕ В СВЕТА НА ТЕХНОЛОГИИТЕ

**КРАСИМИР И. ХРИСТОВ, ТАНЕР Б. ЯЗАДЖИЕВ**

***АБСТРАКТ:*** *Алгоритмите за компютърно зрение са едни от най-трансформиращите и мощни AI системи в света в момента. Системи за компютърно зрение се използват в автономни превозни средства, навигация на роботи, системи за лицево разпознаване и др.*

## 1 Въведение

За да оценим напълно как работят системите за компютърно зрение, трябва да разгледаме как хората разпознават обекти. Най-доброто обяснение, което невропсихологията има за това как разпознаваме обекти, е модел, който описва началната фаза на разпознаване на обект като такъв, при който основните компоненти на обектите, като форма, цвят и дълбочина, се интерпретират първо от мозъка. Сигналите от окото, които влизат в мозъка, се анализират, за да се извадят първо краищата на даден обект и тези краища се съединяват в по-сложно представяне, което допълва формата на обекта.

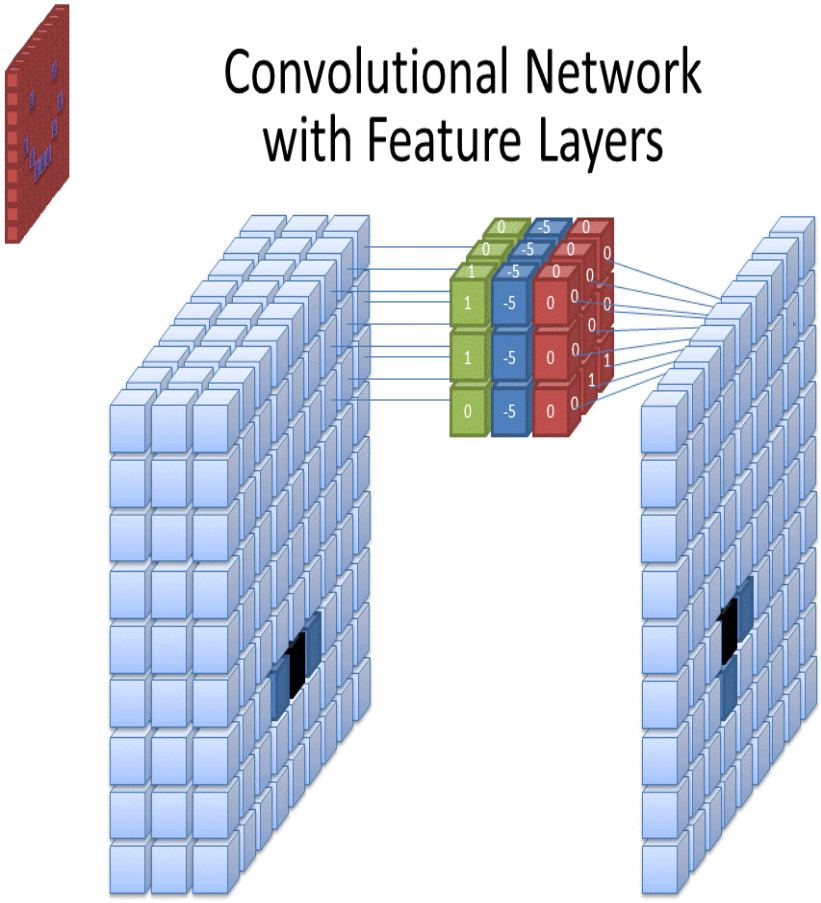
## 2 Изложение

Системите за компютърно зрение работят много подобно на човешката визуална система, като първо разпознават ръбовете на даден обект и след това съединяват тези ръбове заедно във формата на обекта. Голямата разлика е, че тъй като компютрите интерпретират изображенията като числа, системата за компютърно зрение се нуждае от някакъв начин да интерпретира отделните пиксели, които съставляват изображението. Системата за компютърно зрение ще присвои стойности на пикселите в изображението и чрез изследване на разликата в стойностите между една област от пиксели и друга област от пиксели, компютърът може да различи ръбове. Например, ако въпросното изображение е в сива скала, тогава стойностите ще варират от черно (представено от 0) до бяло (представено от 255). Внезапна промяна в обхвата на стойностите на пикселите близо един до друг ще покаже край. Този основен принцип на сравняване на стойностите на пикселите може да се направи и с цветни изображения, като компютърът сравнява разликите между различните RGB цветови канали. [1, 7, 9, 10, 12]

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

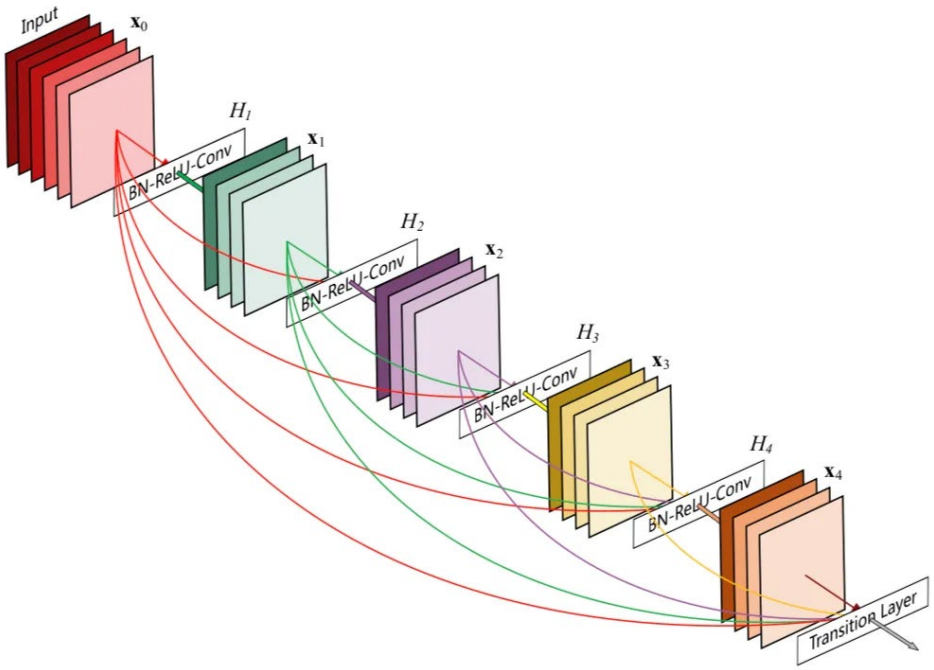
Основният тип който се използва използван в задачите за компютърно зрение, е един базирани на конволюционни невронни мрежи.

Конволюциите са математически процеси, които мрежата използва, за да определи разликата в стойностите между пикселите. Ако си представяте решетка от стойности на пиксели, представете си по-малка решетка, която се премества над тази основна решетка. Стойностите под втората мрежа се анализират от мрежата, така че мрежата изследва само шепа пиксели наведнъж. Това често се нарича техника на „плъзгащи се прозорци“. Стойностите, които се анализират от плъзгащия се прозорец, се обобщават от мрежата, което помага за намаляване на сложността на изображението и улеснява мрежата да извлича модели. Това нагледно може да се види на фиг. 1. [2]



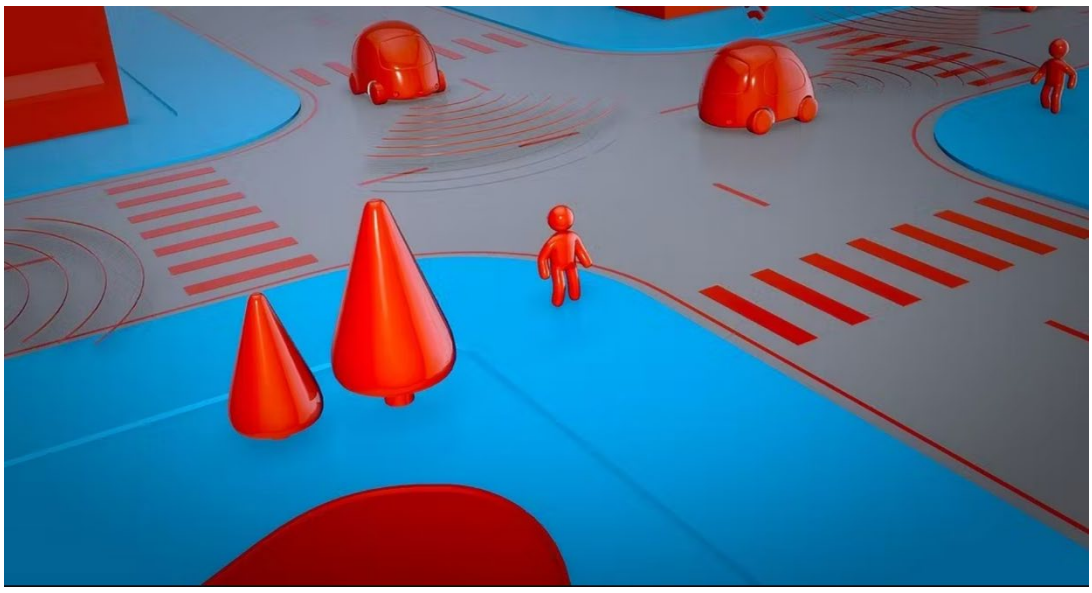

**Фиг. 1.**

Конволюционните невронни мрежи са разделени на две различни секции, конволюционната секция и напълно свързаната секция. Конволюционните слоеве на мрежата са екстрактори на характеристики, чиято работа е да анализират пикселите в изображението и да формират техни представяния, от които гъсто свързаните слоеве на невронната мрежа могат да научат модели. Конволюционните слоеве започват с просто изследване на пикселите и извличане на характеристиките на ниско ниво на изображението като ръбове. По-късните конволюционни слоеве съединяват краищата заедно в по-сложни форми, което може да бъде видяно във фиг.2. [2, 3, 8, 11]




**Фиг. 2.**

Докато конволюционната невронна мрежа може сама да извлича модели от изображения, точността на системата за компютърно зрение може да бъде значително подобрена чрез анотиране на изображенията. Анотация на изображението е процес на добавяне на метаданни към изображението, което подпомага класификатора при откриването на важни обекти в изображението. Използването на анотация на изображението е важно винаги, когато системите за компютърно зрение трябва да бъдат много точни, като например при управление на автономно превозно средство или робот (Фиг.3). [4]



**Фиг. 3.**

Има различни начини, по които изображенията могат да бъдат анотирани, за да се подобри работата на класификатора за компютърно зрение. А именно:

2.1. **Ограничаващи кутии**

Ограничаващите полета са един от най-често използваните видове анотации на изображения в цялото компютърно зрение, отчасти благодарение на тяхната гъвкавост и простота. Ограничителните кутии обхващат обекти и помагат на мрежата за компютърно зрение при локализирането на интересни обекти. Те са лесни за създаване, декларирани чрез просто указване на X и Y координати за горния ляв и долния десен ъгъл на кутията.

Ограничителната кутия може да се приложи към почти всеки възможен обект и те могат значително да подобрят точността на системата за откриване на обекти.

Обичайните употреби на ограничаващи полета включват всяка ситуация, при която обектите се проверяват за сблъсък един срещу друг.

Очевидно приложение на ограничителните кутии и откриването на обекти е автономното шофиране. Системите за автономно шофиране трябва да могат да локализират превозни средства на пътя, но те също могат да се прилагат в ситуации като маркиране на обекти в строителни обекти, за да помогнат за анализиране на безопасността на обекта и за роботите да разпознават обекти в различни среди.

2.2. **Многоъгълна сегментация**

Друг тип анотации на изображения е полигоналната сегментация и теорията зад нея е просто разширение на теорията зад ограничаващите кутии. Полигоналното сегментиране казва на системата за компютърно зрение къде да търси даден обект, но благодарение на използването на сложни полигони, а не просто кутия, местоположението и границите на обекта могат да бъдат определени с много по-голяма точност.

Предимството на използването на многоъгълна сегментация пред ограничаващи кутии е, че тя изрязва голяма част от шума/ненужните пиксели около обекта, които потенциално могат да объркат класификатора.

Полигоналното сегментиране е полезно при автономно шофиране, където може да подчертае обекти с неправилна форма като лога и улични знаци и по-точно да локализира колите в сравнение с използването на ограничаващи полета за локализиране на автомобили. Полигоналното сегментиране също е полезно за задачи, при които много обекти с неправилна форма трябва да бъдат анотирани с прецизност, като например откриване на обекти в изображения, събрани от сателити и дронове. Ако целта е прецизно откриване на обекти като водни обекти, трябва да се използва полигонално сегментиране върху ограничаващи полета.

2.3. **Анотация на линия**

Линейната анотация включва създаването на линии и сплайни, които се използват предимно за очертаване на граници между една част от изображението и друга. Линейната анотация се използва, когато област, която трябва да бъде анотирана, може да се приеме като граница, но е твърде малка или тънка, за да има смисъл ограничителна кутия или друг тип анотация.

Сплайновете и линиите са лесни за създаване на анотации и обикновено се използват за ситуации като обучение на складови роботи да разпознават разликите между части от конвейерна лента или за автономни превозни средства да разпознават ленти.

Автономното шофиране е често срещан случай на използване на анотация на линии, тъй като може да се използва за очертаване на ленти по пътя. По подобен начин анотацията

на линиите може да се използва за инструктиране на индустриални роботи къде да поставят определени обекти, като се обозначава целева зона като между две линии. Ограничителните полета теоретично биха могли да се използват за тези цели, но анотацията на линията е много по-чисто решение, тъй като избягва голяма част от шума, който идва с използването на ограничаващи полета.

2.4. **Анотация за забележителност**

Четвърти тип анотация на изображения за системи за компютърно зрение е анотация на ориентир, понякога наричана точкова анотация, поради факта, че включва създаването на точки/точки в изображение. Само няколко точки могат да се използват за етикетиране на обекти в изображения, съдържащи много малки обекти, но е обичайно много точки да се съединяват, за да представят очертанията или скелета на обект.

Размерът на точките може да варира и понякога се използват по-големи точки за разграничаване на важни/забележителни области от околните области.

Например въздушните изгледи на градове може да изискват използването на откриване на забележителности за намиране на интересни обекти като коли, къщи, дървета или езера.

Въпреки това анотацията на забележителност може да има и други приложения. Комбинирането на много забележителности заедно може да създаде контури на обекти, като пъзел за свързване на точки. Тези точкови очертания могат да се използват за разпознаване на черти на лицето или анализиране на движението и позата на хората.

2.5. **3D кубоиди**

3D кубоидите са мощен тип анотации на изображения, подобни на ограничаващите полета, тъй като те разграничават къде класификаторът трябва да търси обекти. Въпреки това, 3D кубоидите имат дълбочина в допълнение към височината и ширината. Точките за закрепване обикновено се поставят в краищата на елемента, а пространството между закрепванията се запълва с линия. Това създава 3D представяне на обекта, което означава, че системата за компютърно зрение може да се научи да разграничава характеристики като обем и позиция в 3D пространство.

Най-често 3D кубоидите се използват, когато се разработва система за компютърно зрение за автономна система, способна да се движи, тъй като трябва да прави прогнози за обекти в заобикалящата я среда.

2.6. **Семантична сегментация**

Семантичното сегментиране е форма на анотация на изображение, която включва разделяне на изображение на различни региони, присвояване на етикет на всеки пиксел в изображението.

Региони от изображение, които носят различни семантични значения/дефиниции, се считат за отделни от другите региони. Например, една част от изображение може да бъде „небе“, докато друга може да бъде „трева“. Ключовата идея е, че регионите се дефинират въз основа на семантична информация и че класификаторът на изображения дава етикет на всеки пиксел, който включва този регион.

Автономното шофиране е едно приложение на семантично сегментиране, при което AI на превозното средство трябва да прави разлика между участъци от пътя и участъци от трева или тротоар. [4]

# 3 Заключение

Компютърното зрение представлява един от най-важните напредъци в областта на изкуствения интелект и обработката на изображения. То се основава на способността на

компютрите да интерпретират и анализират визуални данни, подобно на човешкото зрение. Методът на действие на компютърното зрение включва набор от алгоритми и техники, които позволяват на машините да идентифицират и класифицират обекти, да разпознават лица и дори да проследяват движения.

Приложенията на компютърното зрение са многобройни и обхващат различни индустрии. В сферата на автомобилостроенето, технологии като автоматично шофиране зависят от способността на системите да разпознават пътни знаци, пешеходци и други возила. В производството, автоматизацията с помощта на компютърно зрение позволява на роботите да инспектират продукти и да гарантират качеството.

В заключение, компютърното зрение не само че трансформира начина, по който взаимодействаме с технологиите, но също така носи значителен потенциал за иновации в различни сфери на обществото. С развитието на алгоритмите и увеличаването на наличието на данни, можем да очакваме нови постижения, които ще продължат да променят динамиката на съвременния свят. [4, 5, 6]

**ЛИТЕРАТУРА:**

[1] Лалев Х. Л., Цанков Ц. С., Георгиева Ц. Л. Приложение на компютърното зрение в системите за ревърс инженеринг. Научна конференция МАТТЕХ 2016, Шумен, 2016, ISSN 1314-3921.

[2] Лалев Х., Цанков Ц., Николов И. 3D лазерно сканиране. Научна конференция МАТТЕХ 2010, Шумен, 2010/2011, ISSN 1314-3921.

[3] Лалев Х. Л., Цанков Ц. С., Георгиева Ц. Л. 3D сканиране с Kinect for Windows. Международна научна конференция УНИТЕХ'16, Габрово, 2016, ISSN 1313-230X.

[4] Лалев Х. Л., Цанков Ц. С., Георгиева Ц. Л. Сканиране на 3D обекти с програмна среда Skanect. Научна конференция МАТТЕХ 2016, Шумен, 2016, ISSN 1314-3921.

[5] Нелсън Д. Какво представляват CNN (конволюционни невронни мрежи)? Unite.AI, 2024.

[6] Denev D., Tsankov Ts. Progress and trends in machine vision smart cameras. Scientific Conference with international participation МАТТЕН 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 116-124.

[7] Konstantinova E., Tsankov Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference "Ecology and environment", 2021, ISSN 2367-5209, pp. 109-121.

[8] 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, 2020, ISSN 2367-7902, pp. 373-378.

[9] 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, 2020, ISSN 2367-7902, pp. 379-385.

[10] Zang J., Wang L., Liu Z., Zhang Q., Hua G., Zheng N. Attention-Based Temporal Weighted Convolutional Neural Network for Action Recognition. Artificial Intelligence Applications and Innovations. IFIP Advances in Information and Communication Technology, vol. 519, 2018.

[11] https://towardsdatascience.com/cnn-architectures-a-deep-dive-a99441d18049

[12] https://hackernoon.com/illuminating-the-intriguing-computer-vision-uses-cases-of-image-annotation-w21m3zfg

# BUILDING AN INFORMATION NETWORK WITH NETWORK NOTEPAD*

**STEFAN M. KAZAKOV**

***ABSTRACT:*** *Network notepad is a powerful network simulation program that allows a commercial application and education for creating interactive network diagrams.*

***KEYWORDS:*** *computer, network, data, model, hub, switch, traffic, information, flow, packet*

***DOI: https://doi.org/10.46687/IQZZ8063***

# ИЗГРАЖДАНЕ НА ИНФОРМАЦИОННА МРЕЖА С NETWORK NOTEPAD

**СТЕФАН М. КАЗАКОВ**

***АБСТРАКТ:*** *Network notepad е мощна симулационна програма за комерсиална и учебна цел за създаване на интерактивни компютърни и информационни мрежи.*

## 1 Въведение

Network notepad е програмен продукт, който допълва физическото оборудване в лабораторията по компютърни мрежи, като позволява да се изградят (симулират) информационни компютърни мрежи с неограничен брой устройства, извеждане на многостранични диаграми с раздели. Тази среда за симулация позволява обучаващите се да развият умения за изграждане на съвременни информационни системи и мрежи

## 2 Характеристики и възможности

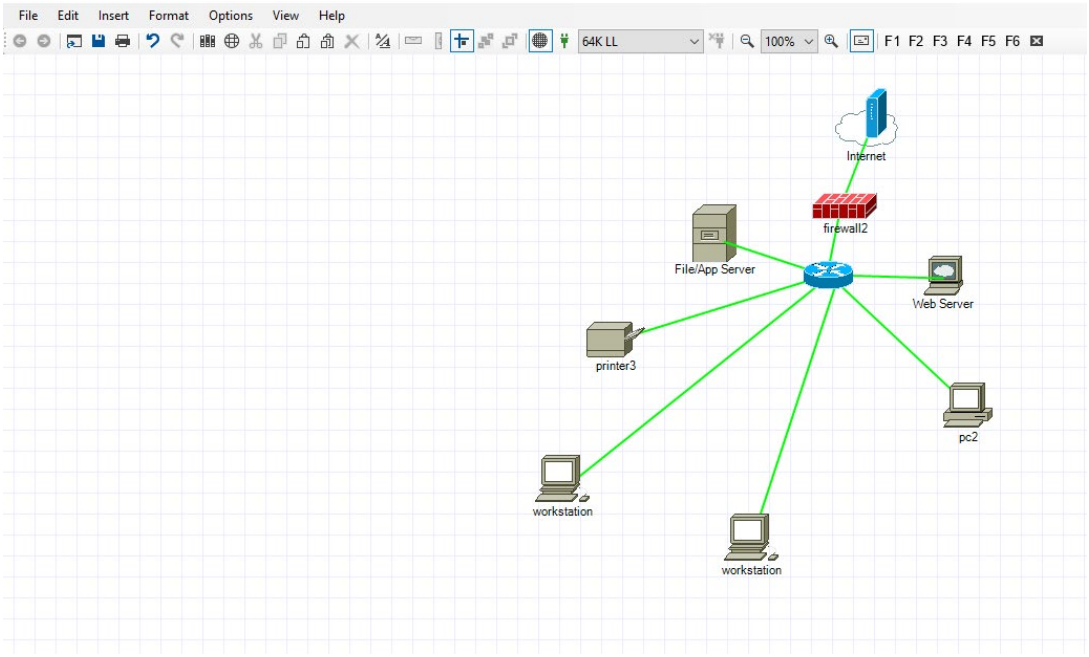
Network Notepad (предоставя следните възможности:) включва следните характеристики:

1. Съвместимост - с помощта на Microsoft.NET, така че предлага по-добра съвместимост и стабилност с най-новите операционни системи Windows.
2. Работа с диаграми на различни нива.
3. Резолюция - Режими Чернова, Фини и Суперфини за подобрена графика и печат.
4. Завъртане - Завъртане на текст и завъртане на обекти под произволен ъгъл.
5. Работно пространство - Поддържа по-голямо растерно изображение на работното пространство / по-големи диаграми.
6. Многостранични диаграми – Добавяне на толкова страници към диаграма/документ, колкото е нужно, и достъп до страниците незабавно.
7. Персонализирани форми – създаване на собствени форми.
8. Групиране и заключване – Комбиниране на два или повече обекта, за да се получат съставни обекти.

* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии“

9. Автоматично подравняване на връзки - Може да се активира за стил на връзка или за отделна връзка, така че подравняването на връзката да се поддържа хоризонтално и вертикално.
10. Търсене в библиотека - Намерете обекти във всичките си библиотеки с помощта на ключови думи. Запазете резултата като нова библиотека.
11. Подобрени стилове на връзки - Нови стилове на светкавични и извити връзки.
12. Шаблонни диаграми.
13. Неограничени дефинирани от потребителя функционални „бутони“ и неограничен брой набори от инструменти.
14. Преглед преди печат.

Програмният продукт Network Notepad (Фиг. 1) предоставя възможности предимно за създаване на прости, но интерактивни информационни мрежови диаграми и диаграми на потока от данни, а след инсталиране на допълнителни библиотеки с икони, също и по-сложни мрежови диаграми и различни видове диаграми или схеми.




**Фиг. 1.** Интерфейс на Network Notepad позволяващ конфигуриране на информационна мрежа

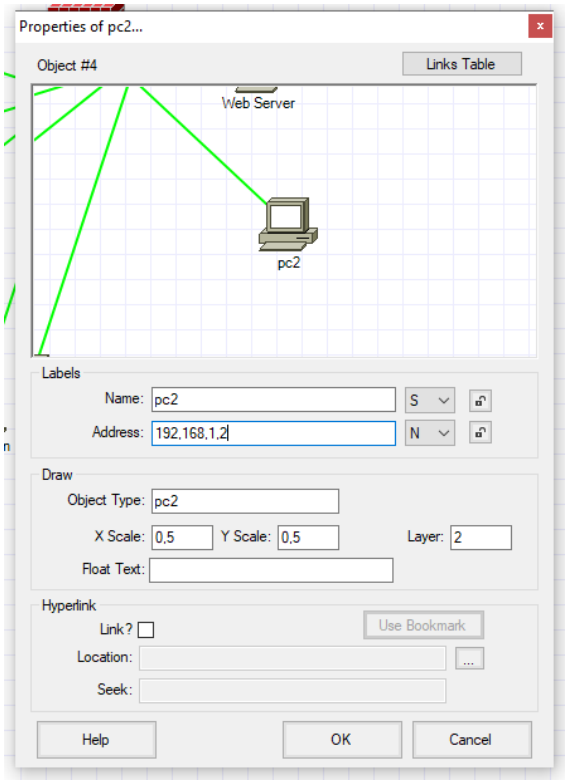
На Фиг. 1. е показан интерфейс на Network Notepad позволяващ кофигуриране на компютърна мрежа и работеща архитектура.

Network Notepad предоставя множество възможности на потребителите да направят визуална демонстрация на комплексна мрежа, концепции и конфигурации за симулиране на информационен поток от данни. Въпреки, че Network Notepad не е заместител на реално оборудване, софтуерът дава възможност на потребителите да практикуват с помощта на интерфейс с команден ред. Тази способност е основен компонент да се конфигурират маршрутизатори и работни станции. Симулационния режим в Network Notepad позволява демонстрация на информационен поток от данни. Тези симулационни способности могат да помогнат да се опрости процеса на изграждане на информационна система чрез предоставяне на таблици, диаграми, както и други визуални представяния на вътрешните

функции, като например динамичен трансфер на данни. Симулационния режим помага като замяна на бялата дъска. Network Notepad може да бъде използван чза различни цели, като например лекции, индивидуални и групови лабораторни упражнения, домашна работа, мрежово проектиране, анализ на мрежи, задачи за моделиране, казуси и състезания.

При обучаващите се, които прекарват повече време в режим на практическо обучение, симулации и интерактивни възможности, ще могат по-добре да се подготвят да прилагат концепции и конфигурации. Придобиват практически опит със задачи като конфигуриране и проектиране, те стават по-уверени в своите способности.

Network Notepad позволява проектиране и симулиране на структурата на реална мрежа чрез ръчни настройки на мрежовите адаптери (Фиг. 2).




**Фиг. 2.** Конфигуриране на мрежа с Network Notepad.

Network Notepad поддържа повечето основни команди за проверка на устройства и крайни точки. Чрез допълнителен модул NNMonitor към птофукта тези команди могат да бъдат наблюдавани. NNMonitor е програма за наблюдение на ping за използване с Network Notepad Professional Edition. Отворя се съответния файл на Network Notepad с NNMonitor и чрез щракане върху бутона Изпълнение започва да пингва всички възли в документа. NNMonitor показва състоянието на всеки възел и може да изпраща предупреждения по имейл и да възпроизвежда звукови ефекти, когато възлите променят състоянието си. Може също така да показва състоянието на всеки възел в Network Notepad и може да бъде стартиран като инструмент в Network Notepad.

Операция – NNMonitor се свързва и взема информацията от създадения файл. Структурата и връзките в създадения файл от информационната мрежа са показани на Фиг. 3.



**Фиг. 3.** Файл с адресите от създадената информационна мрежа.

Бутонът Run/Pause стартира и спира да пингва възлите. Когато работи, състоянието на всеки възел се показва в таблица (Фиг. 4):



**Фиг. 4.** Резултати от пингването на възлите.

Таблицата показва състоянието на всеки възел в диаграмата. Бутонът Log в лентата с инструменти отваря лог файла, когато е конфигуриран. Разделът Регистър(Log) показва най-новите записи в регистрационния файл в паметта.

NNMonitor може също да бъде стартиран като инструмент от Network Notepad за "pingall" възли и да показва техните статуси. Конфигурирайки инструмента, както е показано по-долу, като се запази (набора инструменти, номер на инструмента) в последователност:

Command (0,15) = "c:\Program Files (x86)\NNMonitor\NNMonitor.exe" nnhwnd: $hwnd "file:$filename" run min

```
Display(0,15)=NNMonitor
AutoMin(0,15)=False
Multiple(0,15)=False
```

Параметърът run инструктира NNMonitor да стартира автоматично при стартиране.

Параметърът min инструктира NNMonitor да работи минимизиран.

Конфигурация:

От меню File > Настройка, за да получим достъп до формуляра за настройка. Използваме разделите за достъп до различните секции за настройка:

***Настройка за Ping (Фиг. 5)***

**Interval**: Задава нормалния интервал между избирателните възли.

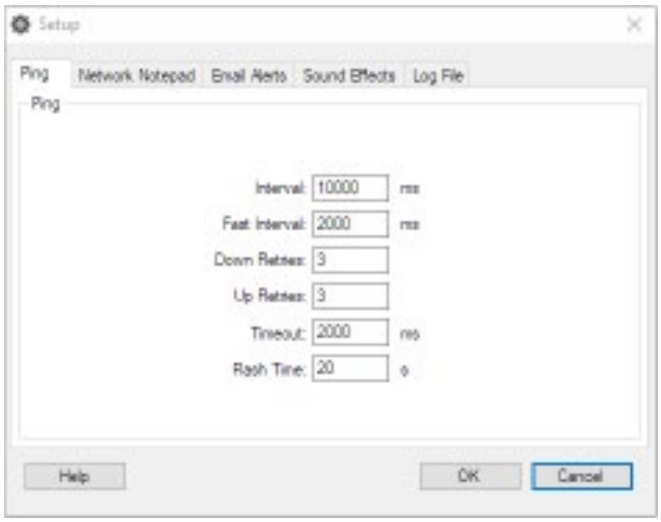
**Fastinterval**: При повторен опит за ping на възел, интервалът между ping се намалява до бързия интервал. За точно отчитане на времето стойността на бързия интервал трябва да бъде фактор на нормалната стойност на интервала.

**Down Retries**: Колко пъти се прави повторен опит за неуспешен ping, преди да се регистрира промяна на състоянието.

**Up Retries**: Колко пъти се опитва ping да потвърди, че даден възел е активен.

**Timeout**: Колко време чака всеки ping, преди да реши, че не е получен отговор.

**Flash Time**: Когато се потвърди промяна на състоянието на възел, съответната клетка от таблицата и индикаторът в Network Notead мигат за броя секунди, зададен тук.




**Фиг. 5.** Прозорец за настройка.

***Настройка Network Notepad (Фиг. 6)***

Команда за стартиране(Launch Command): Това указва изпълнимия файл, който се стартира, когато се щракне върху бутона Network Notepad в лентата с инструменти.

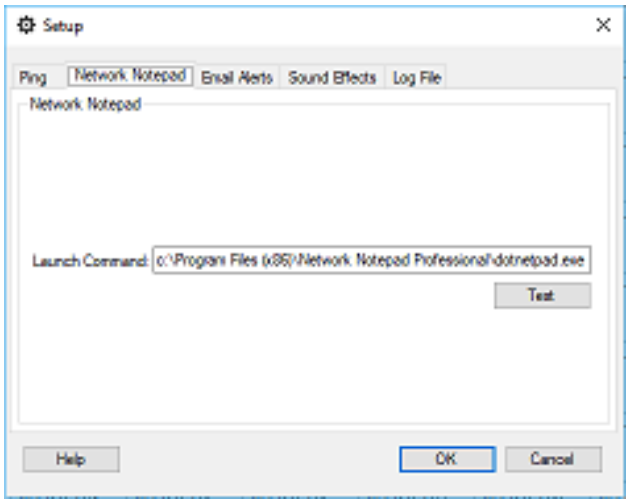
За Network Notepad Professional Edition обикновено е зададено на:

C:/Program Files (x86)/Network Notepad Professional/dotnetpad.exe

За Network Notepad Enterprise Edition обикновено е зададено на:

C:/Program Files (x86)/Network Notepad Enterprise/NNEnterprise.exe

Бутонът за тест може да се използва за тестване на стартирането на Network Notepad от този прозорец.




**Фиг. 6.** Настройка за стартиране Network Notepad

***E-mail известия (Фиг. 7)***

Тези настройки позволяват изпращането на имейл предупреждения, когато възлите променят състоянието си.

До имейл адрес: Получател(и) за известия по имейл. Използвайте "," за разделяне на няколко имейл адреса.

От имейл адрес: Посочете имейл адрес, от който да изглеждат имейлите.
Адрес на сървъра: DNS името или IP адреса за SMTP имейл сървъра, използван за изпращане на имейла.

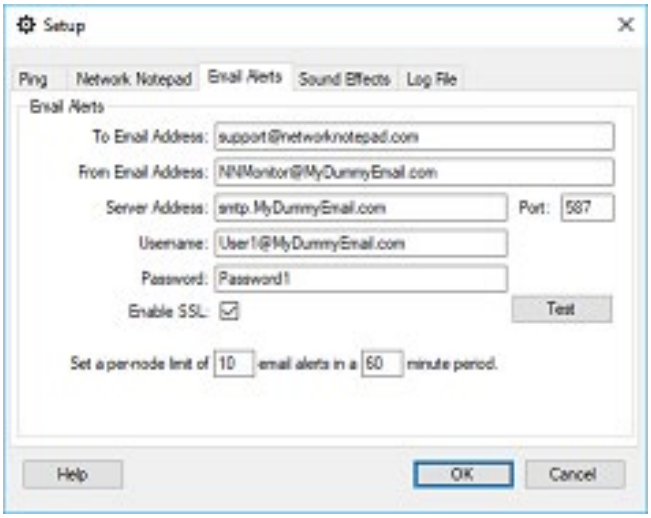
Порт: Обикновено 25, 465 или 587

Потребителско име и парола: Задължителни, ако сървърът изисква удостоверяване.

Активиране на SSL: Поставете отметка, ако сървърът поддържа криптиране.

Бутонът Тест ще се опита да изпрати тестов имейл, използвайки настройките, предоставени в този формуляр.

Може да се зададе ограничение за възел от N имейл предупреждения за период от T минути: Това задава ограничение за броя имейли, изпратени за всеки възел. Има потенциал за генериране на много имейл съобщения, ако възел започне да издава сигнали. Тези настройки определят ограничение на броя имейли, които ще бъдат изпратени.

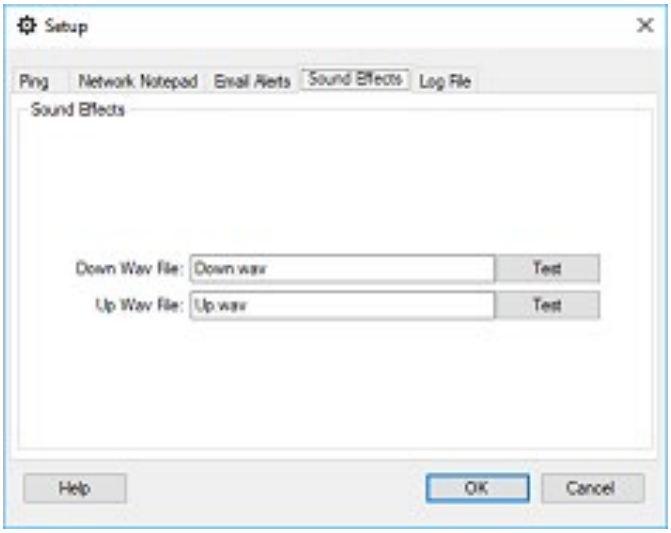



**Фиг. 7.** E-mail известяване.

***Звукови ефекти (Фиг. 8)***

Тази форма задава звуците, които се възпроизвеждат, когато даден възел промени състоянието. Изтриването на записите деактивира звука.

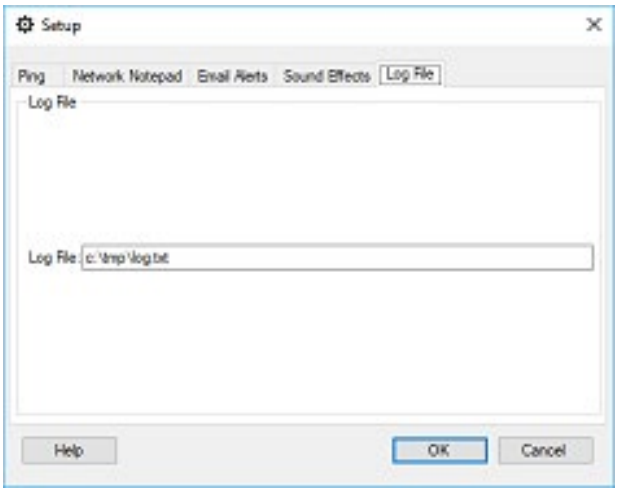
Алтернативни.wav файлове могат да бъдат инсталирани в инсталационната папка на NNMonitor.




**Фиг. 8.** Задаване на звукови ефекти.

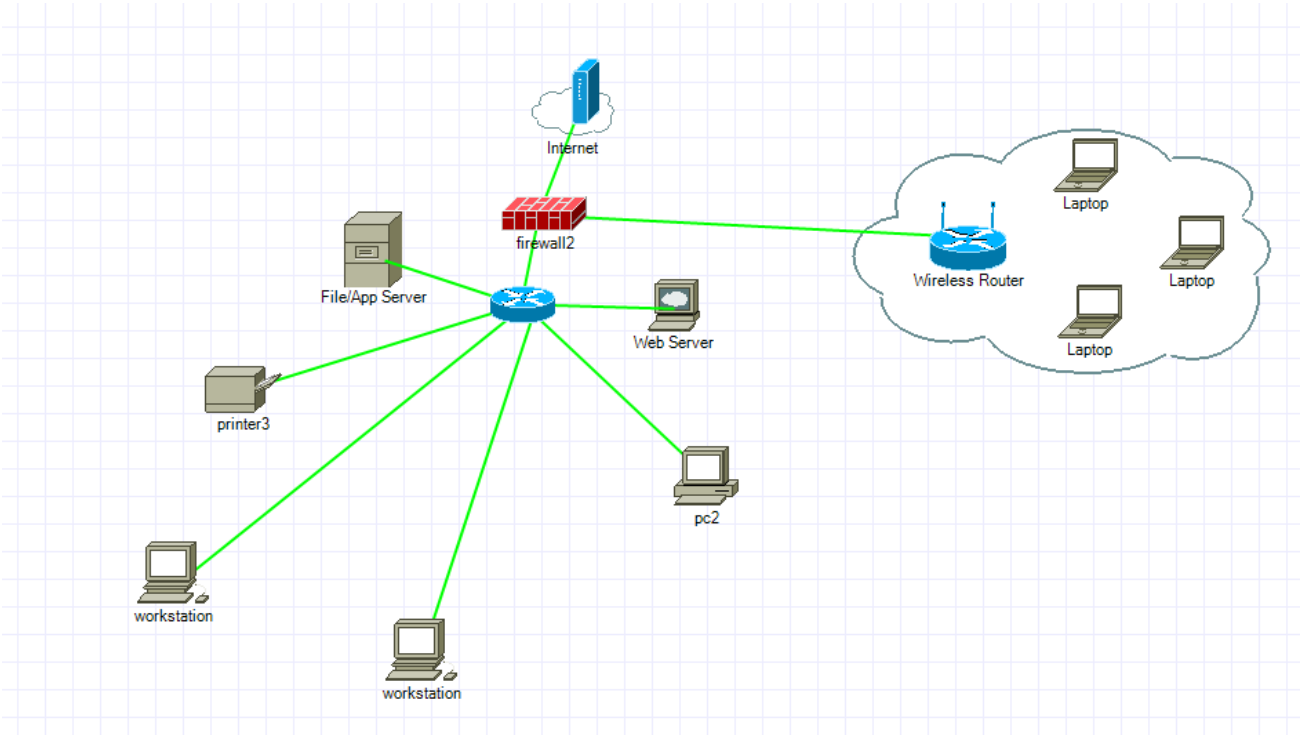
### *Log файлове (Фиг. 9)*

Промените в състоянието на възлите се записват в регистрационен(log) файл, ако е конфигуриран предварително.




**Фиг. 9.** Създаване на регистрационен(log) файл.

Проектиране на информационна мрежа е показано на Фиг. 10. Мрежата е на две нива. Като на първо ниво е изградена Firewall защита, а на второ ниво има суич и свързани към него компютри, сървъри и принтер, и безжичен рутер осигуряващ WiFi връзка.




**Фиг. 10.** Информационна мрежа създадена с Network Notepad.

# 3 Изводи

От показаните възможности на Network Notepad, може да се направят следните заключения и изводи:

1. Програмният продукт Network Notepad може да се използва за провеждане на практическо обучение.
2. Продукта дава възможност за генериране на трафика на данни и провеждане на наблюдения на комуникацията на работни станции.

Network Notepad дава възможност за проектиране и оценка ефективността на различни конфигурации информационни мрежи.

**ЛИТЕРАТУРА:**

[1] Компютърни мрежи и комуникации – Ив. Цонев, Ст. Станев, ШУ 2007

[2] Компютърни системи и мрежи – Ст. Станев, ШУ 2002

[3] Локални мрежи с равноправен достъп – Томас Мадрон, Техника 1995

[4] https://www.networknotepad.com/index.shtml, 1.10.2024г.

# EDGE COMPUTING TECHNOLOGY AND THE OPTIMIZATION OF NETWORK RESOURCES – COMPLICATIONS AND OPPORTUNITIES*

**ILKER A. HATIB, DANIEL R. DENEV**

***ABSTRACT:*** *The current report examines the technology of Edge Computing, which revolutionizes data processing by localizing the computation close to the source, significantly reducing latency and optimizing the use of network resources. The report also explores the technological foundations of Edge Computing, its advantages such as improving security and efficiency, the complications associated with integration and data security, and the future opportunities that include integration with 5G networks, IoT, and AI. Despite the challenges such as implementation and maintenance costs, Edge Computing offers significant improvements in network optimization and presents new opportunities for innovation and efficiency in various industries. This technology has the potential to change the ways that we process and transmit data, providing new solutions for more efficient, secure, and intelligent networks. Exploring these opportunities is crucial for the future development of the connected world.*

***KEYWORDS:*** *5G networks, IoT devices, Edge Computing, AI*

***DOI: https://doi.org/10.46687/FQKY8536***

# ТЕХНОЛОГИЯТА EDGE COMPUTING И ОПТИМИЗАЦИЯТА НА МРЕЖОВИТЕ РЕСУРСИ – УСЛОЖНЕНИЯ И ВЪЗМОЖНОСТИ

**ИЛКЕР А. ХАТИБ, ДАНИЕЛ Р. ДЕНЕВ**

***АБСТРАКТ:*** *Настоящият доклад разглежда технологията Edge Computing, която революционизира обработката на данни чрез локализиране на обработката близо до източника, което значително намалява латентността и оптимизира използването на мрежовите ресурси. Докладът също така разглежда технологичните основи на Edge Computing, предимствата му като подобряване на сигурността и ефективността, усложненията свързани с интеграцията и сигурността на данните, и бъдещите възможности, които включват интеграция с 5G мрежи, IoT и AI. Въпреки предизвикателствата като разходите за внедряване и поддръжка, Edge Computing предлага значителни подобрения в мрежовата оптимизация и представя нови възможности за иновации и ефективност в различни индустрии. Тази технология има потенциала да промени начините, по които обработваме и предаваме данни, предоставяйки нови решения за по-ефективни, сигурни и интелигентни мрежи. Изследването на тези възможности е от съществено значение за бъдещото развитие на свързания свят.*

## 1 Въведение

В ерата на дигитализацията и нарастващия обем от данни, концепцията за Edge Computing набира все по-голямо значение. Edge Computing или изчисления на периферията, се отнасят до обработката на данни близо до източника на тяхното събиране, вместо да бъдат изпращани до централен сървър или облак. Тази технология предлага нови възможности за оптимизация на мрежовите ресурси, като същевременно намалява латентността и подобрява ефективността на обработката на данни.

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

Обработката на данни на периферията на мрежата означава, че информацията може да бъде анализирана и вземани решения в реално време, което е изключително важно за приложения като автономни превозни средства, умни градове и IoT устройства. [7]

В този доклад ще разгледаме как Edge Computing влияе на мрежовата архитектура и какви предимства и предизвикателства предизвиква при оптимизацията на мрежовите ресурси. Ще анализираме как тази технология променя начина, по който данните се обработват и предават в периферията на мрежата, и ще обсъдим потенциалните иновации и тенденции в бъдеще. Една от основните цели на Edge Computing е да намали зависимостта от централни сървъри и облачни услуги, което може да доведе до по-бързи реакции и по-ниски разходи за мрежова инфраструктура.

Този доклад има за цел да предостави ясно и задълбочено разбиране на ролята на Edge Computing в съвременната мрежова инфраструктура и да покаже какви възможности предлага за подобряване на мрежовата производителност и ефикасност. Чрез подробен анализ на предимствата и потенциалните пречки, свързани с прилагането на тази технология, ще се опитаме да предоставим цялостна картина на нейния потенциал и бъдеще развитие. Това изследване е от съществено значение за специалистите в областта на мрежовите технологии, които търсят начини да подобрят своите системи и да се адаптират към бързо развиващата се дигитална среда.

## 2 Технологични основи на Edge Computing

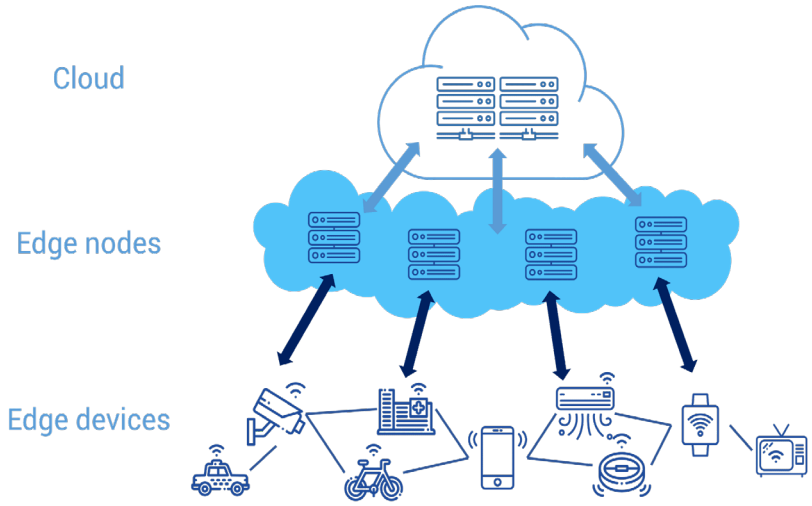
Edge Computing представлява промяна в традиционната облачна архитектура, като се стреми да обработва данни на мястото, където те се генерират, вместо да ги изпраща към централен сървър или облачна инфраструктура. Това значително намалява латентността и подобрява реактивността на системата, което е критично важно за приложения, изискващи време на реализация, като автономни превозни средства и умни фабрики.

Една от основните технологии, поддържащи Edge Computing, е децентрализираната мрежова архитектура. Вместо да се разчита на централни сървъри, данните се обработват и съхраняват на множество разпределени edge устройства, които могат да бъдат рутери, шлюзове, сензори и други IoT устройства. Тази архитектура позволява по-бърза обработка и анализ на данни, намалявайки натоварването върху централната инфраструктура и подобрявайки ефективността.

Друга ключова технология е използването на специализирани edge устройства, които са оптимизирани за изпълнение на специфични задачи на място. Тези устройства могат да включват мощни процесори, графични ускорители и AI чипове, които позволяват извършването на сложни изчисления и анализи директно на мястото на събиране на данни. Това осигурява по-висока производителност и намалява зависимостта от централизирани изчислителни ресурси. Фигура 1 показва структурата за обмен на информация. [8]

Също така, развитието на 5G мрежите играе значителна роля в успешното прилагане на Edge Computing. 5G предоставя по-високи скорости на пренос на данни и по-ниска латентност, което е от съществено значение за ефективната работа на edge устройствата и тяхната комуникация с останалата мрежова инфраструктура. Това позволява реализацията на по-сложни и взискателни приложения, като виртуална и разширена реалност, които изискват мигновена обработка на данни.

Чрез интеграция на тези технологии, Edge Computing променя начина, по който данните се обработват и предават в съвременната мрежова среда, предоставяйки нови възможности за оптимизация и ефективност.

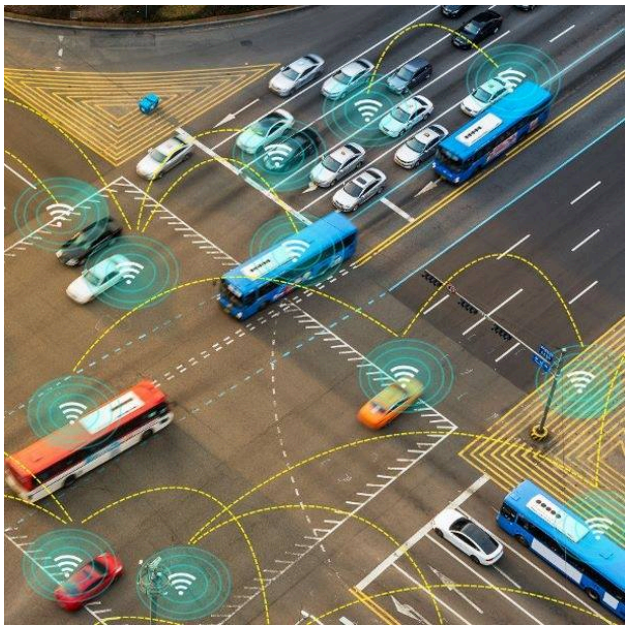



**Фиг. 1.** Структура за обмен на информация [1]

## 3 Edge Computing за мрежовата оптимизация:

Edge Computing предлага значителни предимства за оптимизация на мрежовите ресурси, които не могат да бъдат пренебрегнати в съвременната цифрова среда.

Първото и може би най-важното предимство е намаляването на латентността. Обработката на данни директно на мястото на събиране позволява мигновено вземане на решения и реакция на събития в реално време.



**Фиг. 2.** Функции за мигновеното вземане на решение [2]

Това е от критична важност за приложения като автономни превозни средства, които изискват незабавно анализиране на данните за безопасна и ефективна работа. Фигура 2 показва автомобили, за които мигновеното вземане на решение и правилно реагиране е критично важно, за да се избегне произшествие

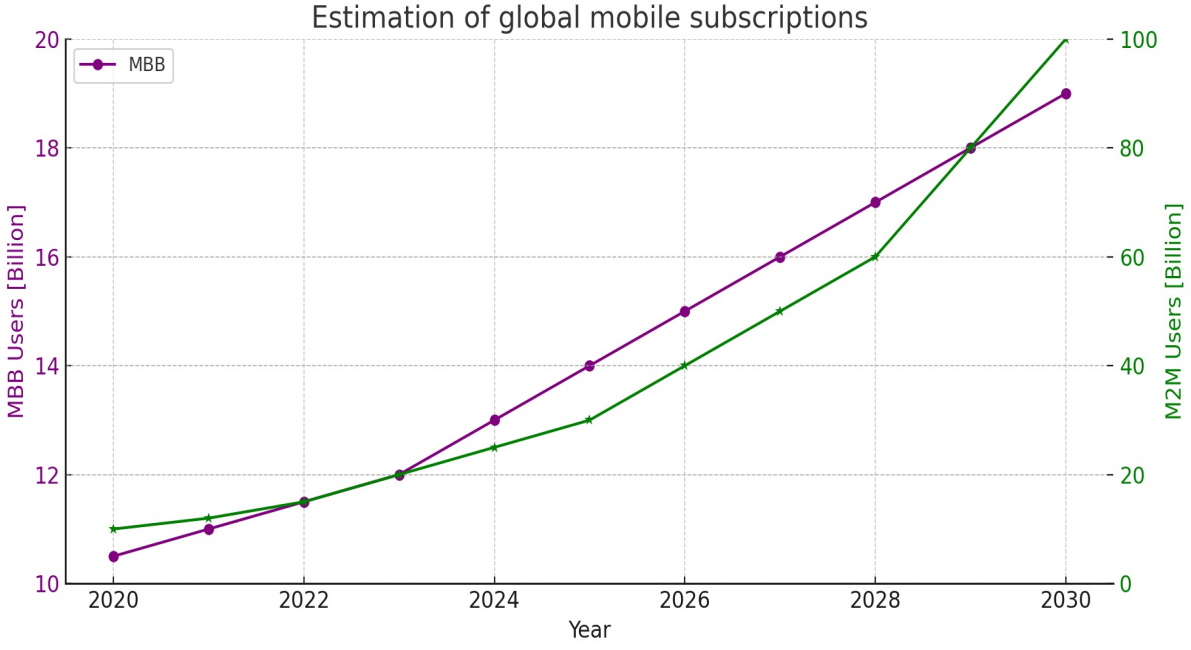
Второто основно предимство е разтоварването на централната инфраструктура. Като се обработват данни на edge устройствата, се намалява необходимостта от прехвърляне на големи обеми информация към централни сървъри или облачни центрове за обработка. Това не само намалява натоварването върху тези сървъри, но също така подобрява ефективността и надеждността на мрежата като цяло.

Подобрението на сигурността и поверителността е още едно ключово предимство. Като се обработват данните на локално ниво, се намалява рискът от загуба на чувствителна информация при прехвърляне към централни сървъри. Това е особено важно за сектори като здравеопазване и финанси, където защитата на данните е от първостепенно значение. [2]

Edge Computing също така позволява по-гъвкаво управление на ресурсите. В зависимост от нуждите на мрежата, edge устройствата могат да бъдат разпределяни и конфигурирани по начини, които оптимизират използването на наличните ресурси. Това води до по-ефективна работа и намаляване на разходите за поддръжка и експлоатация.

Накрая, подобрението на потребителското изживяване е значително предимство. Бързата обработка на данни на edge устройствата означава, че потребителите получават по-бързи и по-качествени услуги, без забавяния и прекъсвания. Това е важно за всичко от поточни видеоуслуги до онлайн игри и приложения за виртуална реалност. Фигура 3 показва броят на безжично свързаните устройства.

MBB(mobile broadband) са мобилни телефони, таблети, лаптопи и други, а M2M(machine-to-machine) са индустриални автоматизирани устройства, дистанционни устройства за наблюдение и други интелигентни мрежи за предаване на данни




**Фиг. 3.** Трафик създаден от индивидуален потребител през годините [4]

Всички тези предимства правят Edge Computing незаменим инструмент за оптимизация на мрежовите ресурси и подобряване на ефективността в разнообразни приложения и сектори.

**Таблица 1.** Предимства на Edge Computing за мрежовите ресурси

| Предимство | Полза за мрежовите ресурси |
|---|---|
| ***Намаляване на трафика*** | *Като обработват данните на edge устройствата, се намалява обемът от данни, които трябва да се прехвърлят към централната инфраструктура.* |
| ***Повишена надеждност*** | *Обработката на място означава, че мрежата не зависи от централен сървър за всяко действие, което подобрява устойчивостта при сривове.* |
| ***Оптимизирано разпределение*** | *Гъвкавото конфигуриране на edge устройствата позволява по-добро използване на мрежовите ресурси, в зависимост от нуждите на приложенията и устройствата.* |
| ***Подобрена производителност*** | *Намалената латентност и бързата обработка на данни водят до по-добра обща производителност на приложенията, използващи мрежата.* |

# 4 Усложнения и предизвикателства

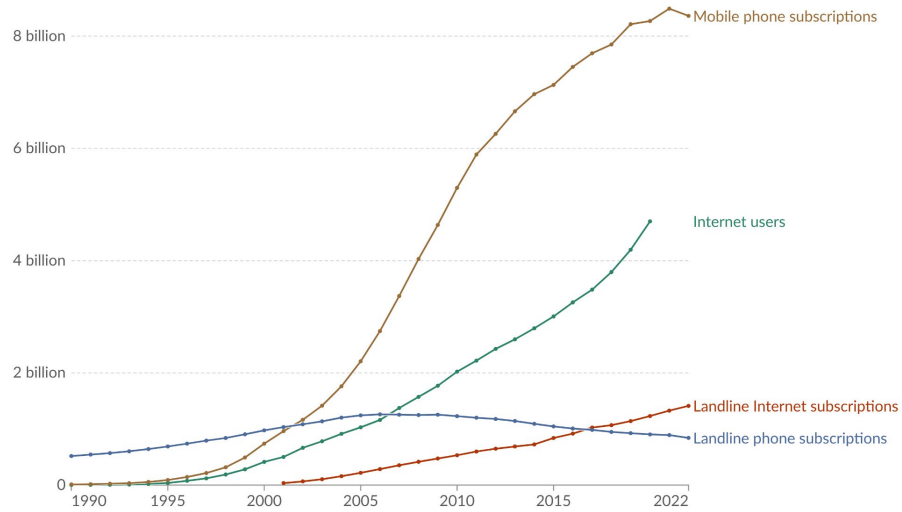
Въпреки значителните предимства на Edge Computing, съществуват редица усложнения и предизвикателства, които трябва да бъдат разгледани за успешната му имплементация.

Едно от основните предизвикателства е сигурността и защитата на данните. Обработката на данни на множество разпределени edge устройства увеличава риска от пробиви в сигурността. Всеки edge възел може да бъде потенциална точка за атака, което изисква интегриране на напреднали методи за криптиране и сигурност, за да се гарантира защитата на данните. Управлението на разпределените ресурси е друго значително предизвикателство.С разпространението на edge устройствата, е необходимо ефективно управление и координация на тези ресурси, за да се избегнат конфликти и да се гарантира оптимална работа. Това включва мониторинг и поддръжка на мрежовата инфраструктура, както и осигуряване на висока производителност и надеждност. Фигура 4 показва броят на абонаментите на телефонни и интернет услуги през годините. [3]

Интеграция с съществуващите мрежови решения също може да бъде сложно. Внедряването на Edge Computing изисква значителни промени в съществуващата мрежова архитектура и инфраструктура, което може да доведе до несъвместимости и технически проблеми. Това налага внимателно планиране и изпълнение, за да се гарантира, че новите технологии се интегрират безпроблемно със съществуващите системи.

Капиталови разходи и поддръжка също представляват предизвикателство. Въпреки че Edge Computing може да намали операционните разходи в дългосрочен план, първоначалната инвестиция за внедряване на необходимата инфраструктура може да бъде значителна. Освен това, поддръжката и управлението на разпределените edge устройства изисква допълнителни ресурси и експертиза.

Накрая, осигуряването на стандартизация и интероперативност е ключов фактор. Въпреки че Edge Computing предлага гъвкавост, липсата на общоприети стандарти може да затрудни интероперативността между различните платформи и устройства. Това изисква сътрудничество между различни участници в индустрията за разработване на стандарти, които да улеснят интеграцията и да гарантират съвместимостта на различните системи.




**Фиг. 4.** Брой абонати с edge устройства [5]

Разглеждайки и преодолявайки тези усложнения и предизвикателства, ще можем да реализираме пълния потенциал на Edge Computing и да постигнем значителни подобрения в мрежовата оптимизация и ефективност.

## 5 Възможности и бъдещи тенденции

Edge Computing предоставя множество вълнуващи възможности за бъдещото развитие на мрежовите технологии и техните приложения. Едно от основните предимства е потенциалът за драстично намаляване на времето за обработка на данни, което може да доведе до значителни подобрения в множество индустрии.

Интеграция с 5G мрежи: Развитието на 5G технологиите ще играе критична роля за разширяване на възможностите на Edge Computing. С по-висока скорост на пренос на данни и по-ниска латентност, 5G ще позволи на edge устройствата да комуникират по-ефективно и да обработват данни в реално време, което е от решаващо значение за приложения като автономни превозни средства и умни градове.

Интернет на нещата (IoT): Edge Computing ще бъде ключов фактор за развитието на IoT екосистемите. С милиарди устройства, свързани към интернет, необходимостта от обработка на данни локално става все по-голяма. Edge Computing ще позволи на тези устройства да функционират по-независимо и ефективно, като намалява натоварването на централните сървъри и подобрява реактивността.

Изкуствен интелект (AI) и машинно обучение (ML): Интеграцията на AI и ML с Edge Computing ще доведе до интелигентни edge устройства, способни да извършват сложни анализи и да вземат автономни решения на място. Това ще отвори нови възможности за автоматизация и оптимизация на процесите в различни индустрии, от производството до здравеопазването. [6]

Киберсигурност: С развитието на Edge Computing ще се появят нови решения за повишаване на сигурността на данните. Локалната обработка на данни намалява риска от кибератаки при пренос на информация към централни сървъри и предлага възможности за разработване на по-сигурни и надеждни системи.

Енергийна ефективност: Въпреки че Edge Computing изисква първоначална инвестиция в инфраструктура, тя може да доведе до по-ефективно използване на енергията в дългосрочен план. Локалната обработка на данни намалява необходимостта от постоянен пренос на големи обеми информация, което може да намали общото потребление на енергия и въглеродния отпечатък.

Бъдещи технологии и приложения: С напредъка на технологиите, Edge Computing ще открие нови възможности за иновации в различни сфери. От умни домове и интелигентни транспортни системи до усъвършенствани медицински устройства и персонализирани здравни решения, потенциалът за развитие е огромен.

В заключение на тази точка, Edge Computing представлява бъдещето на мрежовите технологии, предоставяйки нови възможности и перспективи за оптимизация и иновации. Справянето с текущите предизвикателства и използването на тези възможности ще допринесат за създаването на по-ефективни, сигурни и интелигентни мрежови решения в бъдеще.

**Таблица 2.** Предизвикателства и възможности за бъдещо развитие на Edge Computing

| Предизвикателство | Възможност за развитие |
|---|---|
| ***Управление на сигурността*** | *Разработване на нови решения за киберсигурност, които са специално предназначени за защита на edge устройства и данните, които те обработват.* |
| ***Съвместимост и стандартизация*** | *Разработване на стандарти, които позволяват различни устройства и технологии да работят заедно ефективно в edge екосистемите.* |
| ***Инвестиции в инфраструктурата*** | *Въпреки първоначалната цена, Edge Computing ще донесе дългосрочни ползи чрез подобрена ефективност и оптимизация на ресурсите.* |
| ***Енергийна ефективност на edge устройства*** | *Разработване на нови енергийно ефективни технологии за edge устройства, които да минимизират разхода на енергия и увеличат устойчивостта.* |

# 6 Заключение

Edge Computing представлява значителен напредък в технологиите, който преоткрива начина, по който данните се обработват и предават в съвременната мрежова инфраструктура. Чрез разглеждане на технологичните основи на Edge Computing, осъзнаваме колко важна е децентрализираната обработка на данни за подобряване на латентността и ефективността на мрежите.

Предимствата на Edge Computing за оптимизация на мрежовите ресурси са многобройни, като включват намаляване на натоварването върху централната инфраструктура, подобряване на сигурността и поверителността на данните, и осигуряване на по-бърза и качествена потребителска услуга.

Въпреки това, внедряването на Edge Computing не е без своите усложнения и предизвикателства. Тези включват управлението на сигурността на данните, интеграцията със съществуващите мрежови решения, и необходимостта от значителни капиталови разходи и поддръжка.

Въпреки тези пречки, възможностите и бъдещите тенденции, свързани с Edge Computing, са обещаващи. Развитието на 5G мрежите, интеграцията с IoT и AI, както и подобренията в киберсигурността и енергийната ефективност, откриват нови хоризонти за иновации и оптимизация в различни индустрии.

В заключение, Edge Computing е ключов фактор за бъдещето на мрежовите технологии, предоставяйки нови възможности за оптимизация и ефективност. Преодоляването на съществуващите предизвикателства ще позволи на тази технология да реализира пълния си потенциал и да промени начините, по които обработваме и предаваме данни в нашия свързан свят.

**ЛИТЕРАТУРА:**

[1] Al-Fuqaha A., Guizani M., Mohammadi M., Internet of Things: A Survey on Enabling Technologies, Protocols and Applications, 2015, Published in: IEEE Communications Surveys & Tutorials Volume 17, Electronic ISSN: 1553-877X DOI https://doi.org/10.1109/COMST.2015.2444095, pp. 2347 – 2376

[2] Bablu S., Sathvik B., Narendra Kh., Optimizing Communication in High-Speed Train Environments over 5G Signals through MIMO Base Station Positioning, 2024, International Conference on Advancements in Power, Communication and Intelligent Systems, Electronic ISBN:979-8-3503-6328-9 DOI https://doi.org/10.1109/APCI61480.2024.10617134, pp. 275-280

[3] Di Renzo M., Haas H., Ghrayeb A., Spatial Modulation for Generalized MIMO: Challenges, Opportunities, and Implementation, 2014, Published in: Proceedings of the IEEE Volume 102, Print ISSN: 0018-9219 DOI https://doi.org/ 10.1109/JPROC.2013.2287851, pp. 56 – 103

[4] Duarte M., Dick C., Sabharwal As., Experiment-Driven Characterization of Full-Duplex Wireless Systems, 2012, Published in: IEEE Transactions on Wireless Communications Volume 11, Print ISSN: 1536-1276 DOI https://doi.org/10.1109/TWC.2012.102612.111278, pp. 4296 – 4307

[5] Gupta A., Jha R., A Survey of 5G Network: Architecture and Emerging Technologies, 2015, Published in IEEE Access Volume 3, Electronic ISSN: 2169-3536 DOI https://doi.org/10.1109/ACCESS.2015.2461602, pp. 1206 – 1232

[6] Jiang W., Bin H., The Road Towards Wi-Fi 6: A Comprehensive Survey, 2021, Published in: IEEE Open Journal of the Communications Society Volume 2, Electronic ISSN: 2644-125X DOI https://doi.org/10.1109/OJCOMS.2021.3057679, pp. 334 – 366

[7] Larsson E., Edfors O., Tufvesson F., Massive MIMO for Next Generation Wireless Systems, 2014, IEEE Communications Magazine Volume: 52 Issue: 2, Print ISSN: 0163-6804 https://doi.org/10.1109/MCOM.2014.6736761, pp. 186 – 195

[8] Rangan S., Rappaport T., Erkip E., Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges, 2014, Published in: Proceedings of the IEEE Volume 102, Print ISSN: 0018-9219 DOI https://doi.org/10.1109/JPROC.2014.2299397, pp. 366 – 385

# A METHOD FOR MINIMIZING AND ELIMINATING AUDIO DISTORTION WHEN HIDING DIGITAL DATA IN THE DIGITIZATION PROCESS*

**DANIEL R. DENEV**

***ABSTRACT:*** *This report presents a methodology for embedding and extracting digital data within audio files using the Least Significant Bit (LSB) embedding technique. The system is designed to minimize or eliminate noise generated during the process of data steganography in audio. The primary objective of the study is to analyze the effects of sampling frequency on audio signal quality during the digitization process. The motivation arises from the sensitivity of the human auditory system (HAS) to distortions that occur during steganography, which could make the process easily detectable. The report demonstrates a method for embedding textual data into audio files through LSB techniques, utilizing an encryption key. The focus is primarily on audio signal sampling. The audio signal is further segmented using the Nyquist-Shannon sampling theorem. In conclusion, the report shows that the proposed system effectively performs audio steganography with reduced noise, as measured by the signal-to-noise ratio (SNR).*

***KEYWORDS:*** *audio, steganography, noise*

***DOI: https://doi.org/10.46687/XUDN1585***

# МЕТОД ЗА МИНИМИЗИРАНЕ И ПРЕМАХВАНЕ НА ЗВУКОВИ ИЗКРИВЯВАНИЯ ПРИ СКРИВАНЕ НА ЦИФРОВИ ДАННИ В ПРОЦЕСА НА ЦИФРОВИЗАЦИЯ

**ДАНИЕЛ Р. ДЕНЕВ**

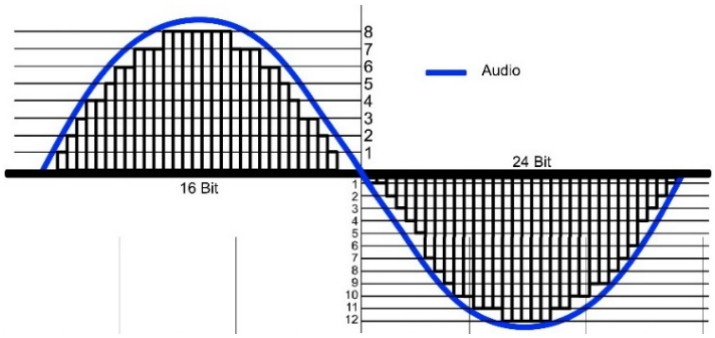
***АБСТРАКТ:*** *Този доклад представя методология за вграждане и извличане на цифрови данни в аудио файлове, използвайки техниката на най-маловажния бит (LSB) за вграждане. Системата е разработена с цел минимизиране или елиминиране на шума, който възниква по време на процеса на стеганографиране на данни в аудиото. Основната цел на изследването е да се анализират ефектите на честотата на семплиране върху качеството на аудио сигнала по време на процеса на цифровизация. Мотивацията произтича от чувствителността на човешката слухова система (HAS) към изкривяванията, възникващи при стеганография, което може да направи процеса лесно забележим. В доклада се демонстрира метод за вграждане на текстови данни в аудио файлове посредством LSB техники и използване на шифровъчен ключ. Основен акцент се поставя върху семплирането на аудио сигнала. Аудио сигналът допълнително се сегментира с помощта на теоремата за семплиране на Найкуист-Шанън. В заключение, докладът показва, че предложената система ефективно осъществява аудио стеганография с намален шум, измерен чрез съотношението сигнал/шум (SNR).*

## 1 Въведение

Стеганографията е изкуството да се скриват данни върху носител и да се правят неоткриваеми. В този доклад основните стеганографски процеси, като криптиране на текстови данни в аудио сигнал (.wav) и декриптиране, бяха извършени с помощта на техника за кодиране с най-малък значим бит (LSB), заедно с процеса на удостоверяване на шифровия ключ. Обсъжда се ясното разбиране на шума, който се добавя към аудио сигнала,

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

когато текстът е вграден чрез стеганографски процес. Този документ представя ефекта на стойността на SNR върху различна честота на дискретизация. В тази работа използва LSB техника за кодиране, която е прост и лесен начин за вграждане и по-добра незабележимост. В приемащия край вградените данни се извличат без да се знае оригиналното аудио. Предложената система е внедрена и тествана за различни размери на извадката и ефективността е оценена чрез сравнение на стойностите на SNR. Нашият основен принос е да имаме перфектна честота на дискретизация за различни аудио типове [2], [3].




**Фиг. 1.** Честота на вземане на проби(Sampling Rate) [2]

## 2 Теория за звуковите вълни

Преди да започнем да манипулираме звука, трябва да проучим какъв е характерът на звука и неговия процес на дигитализация. В този раздел се обсъждат основите на звука и неговото цифрово представяне.

- *Характеристики на музика и звукова вълна*

На фундаментално физическо ниво звукът е просто смущение на молекулите в дадено вещество [2]. Трите основни характеристики на звуковите вълни, които се използват за описване или реконструиране на сигнал, са

- **Амплитуда**: Мярка за степента на промяна в атмосферното налягане, причинена от звукови вълни. Тази амплитуда е пряко свързана с силата на звука.
- **Честота** ($\boldsymbol{f}$): Честотата на звука е скоростта на цикъла, образуван за секунда, и се представя с единица херц Hz. Честотата е право пропорционална на височината на звука.
- **Дължина на вълна**: Дължината на вълната($\lambda$) е разстоянието между два съседни върха или падината между тях. Зависи от скоростта на звука (v) представена чрез единица (m/s) и нейната честота($f$). Следователно можем да дефинираме в уравнение (1) дължината на вълната като;

$$\boldsymbol{\lambda = \frac{v}{f}} \quad \textbf{(1)}$$

- *Цифрово аудио семплиране*

В този раздел се обсъжда преобразуването на аналогов звук в поредица от битове. Устройството, използвано за този процес, е аналогово-цифров преобразувател (ADC). ADC улавя моментни снимки (проби) на електрическото напрежение хиляди пъти в секунда в аудио сигнали, използвайки устройства като микрофон. Той е представен от гледна точка на битови серии, които могат да се използват за по-нататъшна обработка. Аудио семплирането влияе върху качеството на цифровата форма на вълната по отношение на честотата на дискретизация и размера на дискретизацията.

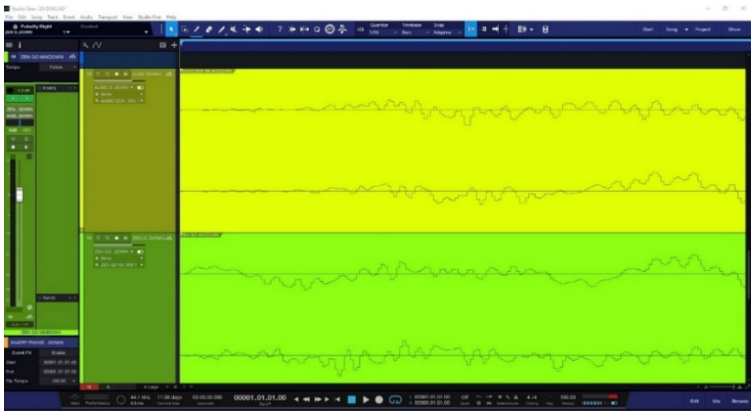
- *Качество на звука*

Звукът може да бъде класифициран като стереофоничен звук (стерео) и монофоничен звук (моно). Стереото е с повече на брой независими аудио канали, което създава впечатление за чуване от различни посоки. А Mono има един канал [4], [2].

# 3 Системен дизайн

- *Създаване на аудио проби*

Честотата на дискретизация е броят измервания на аналогов сигнал за секунда. По-високата честота на дискретизация води до по-високо качество на звука, тъй като аналоговата форма на вълната се приближава много. Изборът на честота на дискретизация зависи от приложението, възможностите на аудио интерфейсите и дестинацията на аудиото.



**Фиг. 2.** Вариации на честотата на вземане на проби

- *Аудио проби за вграждане на данни*

Когато текстовото съобщение е вградено в аудио файла, аудио файловете и текстовият файл се преобразуват в битови потоци. Първият бит от текста ще бъде вмъкнат в първата семпла от по-малко значимия бит от общата обложка. Процесът ще тече, докато цялото текстово съобщение бъде вмъкнато в аудио файла. Когато текстовото съобщение е по-голямо от аудио файла, се показва съобщение за грешка. Беше разработен интерактивен програмен анализ с помощта на функции на инструменти на Matlab като wavread (), wavwrite (), wavrecord (), wavplay (), wavinfo ().

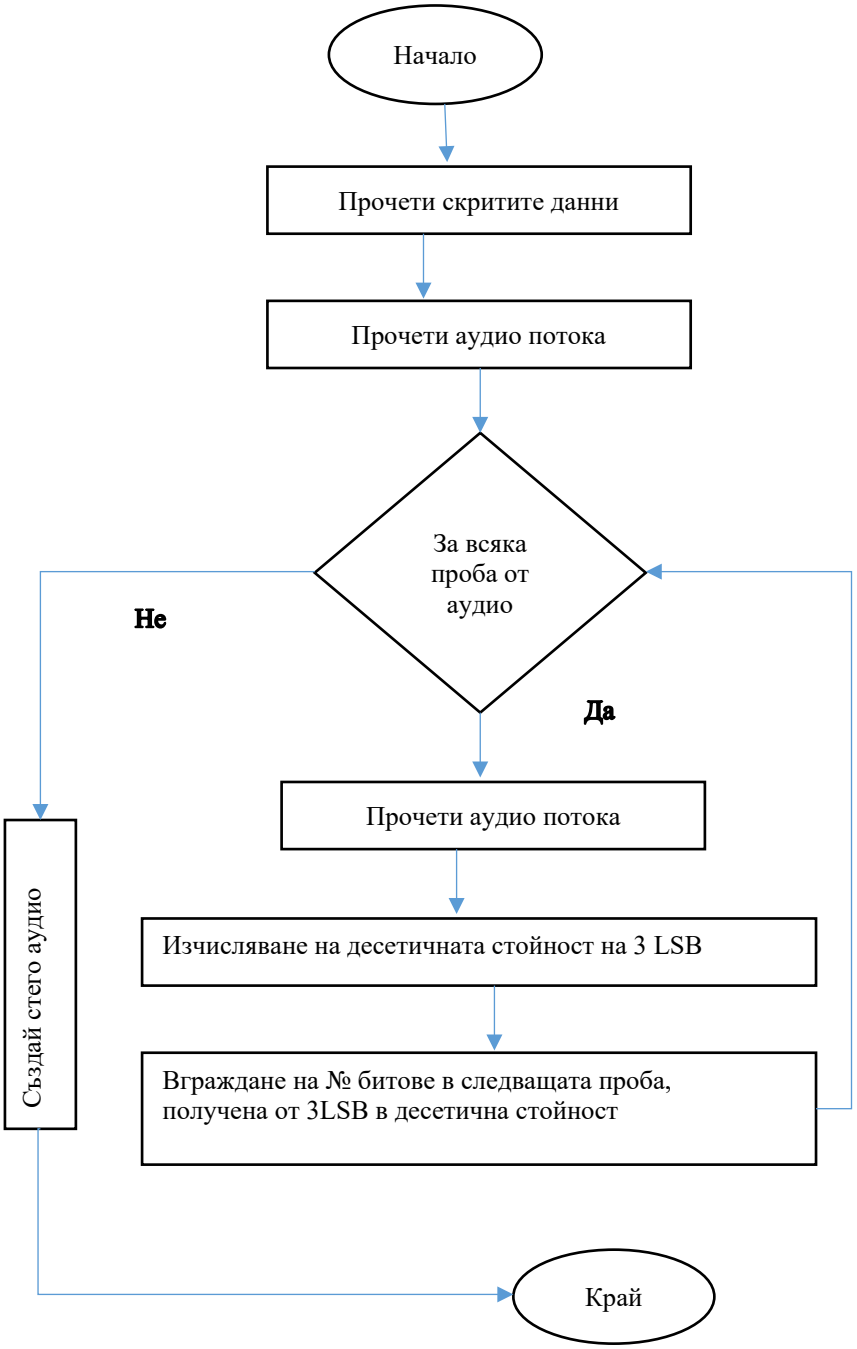
- *Аудио схема за вграждане на данни*

Схемата за вграждане на LSB се използва за скриване на текстови данни в аудио файлове. Обсъждат се каналите за кодиране и декодиране. Тук се извършва манипулация на битово ниво, за да се кодира съобщението. Текстовите данни, използвани за процеса на вграждане, са с размер 1,35 KB. Стъпките за процеса на вграждане, описани на фигура (4), са както следва: 1) В канала за кодиране се получава аудио файл, 2) Преобразува се в двоичен модел чрез семплиране. 3) Получава текстовото съобщение. 4) Преобразува всеки знак в двоичен модел. 5) Прилага се ключ за шифър. 6) При декодиране на канал съобщението се извлича чрез получаване на формат на сигнал от вълна (.wav). 7) Идентифицира се дали даден сигнал е стеганографски сигнал. 8) Оставя се некриптирания сигнал да се възпроизвежда нормално. 9) В противен случай процесът на извличане на съобщение стартира с помощта на ключа за шифър. 10) Двоичните стойности се преобразуват обратно в ASCII стойности и се реконструират обратно към оригиналното съобщение [1], [4].

Основният проблем в аудио оборудването е наличието на шум. Има различни техники за вземане на проби в аудиокартите и те се извършват чрез използване на съотношението сигнал към шум (SNR). SNR е отношението на мощността на сигнала към шума (изкривяването). Това е мярка за качеството на изходния сигнал след процеса на вграждане. Измерва се в децибели (dB). По-високите стойност на SNR носят по-чисти изходните сигнали с по-малко добавен фонов шум:

$$SNR = 10\log_{10}\frac{\sum_n A_n^2}{\sum_n (A_n - A'_n)^2} \quad \textbf{(2)}$$

Където An е оригиналният аудио сигнал An’ е изкривеният аудио сигнал




**Фиг. 3.** Вграждане на данни в аудио проби

# 4 Аудио стеганографски метод

Има много техники за скриване на информация или съобщения в аудио по такъв начин че промените, направени в аудио файла са перцептивно неразличими. Общия подход включва LSB кодиране. Много популярна методология е алгоритъмът LSB (Least Significant Bit), който замества най-малко значим бит в някои байтове от файла на аудиото, за да скрие поредица от байтове, съдържащи скрити данни [1]. Това обикновено е ефективна техника в случаите, когато заместването на LSB причиняват значително влошаване на качеството, като например при 16-битови моно аудио звуци. В изчисленията най-малко значимият бит (LSB) е битовата позиция в двоично цяло число, което дава на единиците стойност, тоест определя дали числото е четно или нечетно. Понякога се споменава LSB като най-десния бит, поради конвенцията в позиционната нотация за писане на по-малко значима цифра по-надясно.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | **1** |

**Фиг. 4.** Двоично представяне на десетично число

MSB в 8-битов двоичен файл представлява стойност от 128 десетични числа. LSB представлява стойност 1. За да скрие буквата "a" (чийто ASCII код е 01100001) като звук в аудио файл се създава осем байтов кавър и в допълнение се задава LSB на всеки байт. Описаното е показано в таблица 1.

***Таблица 1.*** *Представяне на звука "a" в аудио файл*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | **0** |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | **1** |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | **1** |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | **0** |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | **0** |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | **0** |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | **0** |

# 5 Резултати

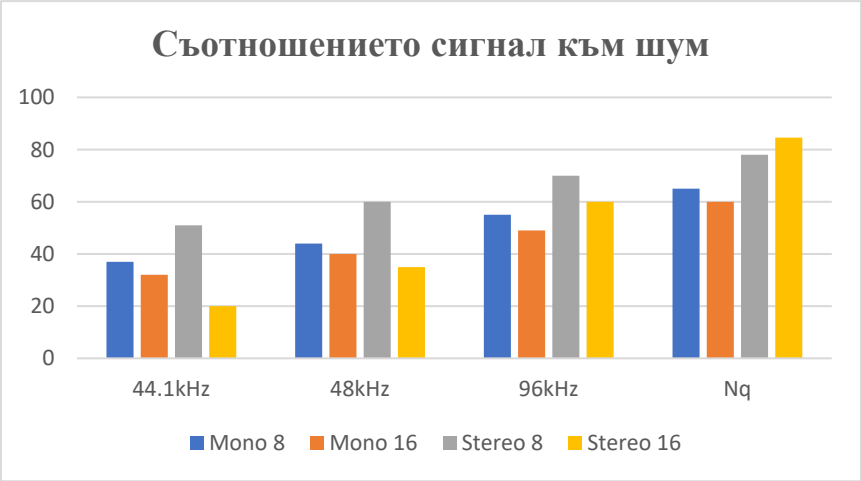
След прилагането на предложения метод в Раздел 4 се разглеждат три стъпки: Избира се аудио сигнала със скритото съобщение (добавената буквата "a") и се пробва при 44,1 KHz, 48 KHz, 96 KHz и честота на семплиране на Найкуист (Nq). Семплираният звук се обработва чрез процеса на вграждане на аудио стеганография с помощта на LSB.

Времето за изпълнение на процеса на аудио стеганография се изчислява както за моно, така и за стерео аудио, които се семплират в диапазона на честота на семплиране. Аудиото, взето при честота на дискретизация на Найкуист, също беше включено специално в теста. Резултатите са представени в таблица 2.

На фигура (5) са показани сравненията и вариациите който се изследват по отношение на SNR, когато честотата на дискретизация се променя. Моно аудиото показва по-малко вариации в сравнение със стерео аудиото. При честотата на дискретизация на Найкуист стойността на SNR е по-голяма, така че тя формира най-добра честота на дискретизация от 84,6 dB

***Таблица 2.*** *Набор от аудио данни, използвани за тестване*

| **Име на файл** | **Bits за семпъл** | **Обем на аудио** | **Качество на аудио** | **Размер след семплиране (KB)** | | | | **Съотношение сигнал – шум (dB)** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| - | | | | 44.1 | 48 | 96 | Nq | 44.1 | 48 | 96 | Nq |
| A | 8 | 866KB | Mono | 134 | 367 | 559 | 666 | 37 | 32 | 51 | 20 |
| B | 16 | 1.73MB | Mono | 782 | 700 | 1100 | 1007 | 44 | 40 | 60 | 35 |
| C | 8 | 1.34MB | Stereo | 274 | 599 | 1094 | 1211 | 55 | 49 | 70 | 60 |
| D | 16 | 1.73MB | Stereo | 300 | 1335 | 2000 | 2218 | 65 | 60 | 78 | 84.6 |




**Фиг. 5.** Съотношение сигнал-шум спрямо честота на дискретизация

## 6 Заключение

В този доклад вграждането на цифрови данни в аудио файл се развиват с помощта на LSB схема. Идеалната честота на дискретизация с помощта на техниката на Найкуист-Шанън е оправдана, така че да не се добавя изкривяване дори преди да започне процесът на вграждане. Ефектите от различната честота на дискретизация върху стойността на SNR бяха изследвани спрямо размера на семплирания аудио файл. Въз основа на резултатите от теста беше анализирана производителността на аудио стеганографията.

**ЛИТЕРАТУРА:**

[1] Cvejic N., Reduced Distortion Bit Modification for LSB Audio Steganography, Inf. Process. Lab., 2014, pp. 2318 - 2321.

[2] Howard D., Acoustics and Psychoacoustics, CRC Press, 2018, pp. 524-530.

[3] Gopalan K., Audio Steganography Using Bit Modification, CRC Press, 2013, pp. 629-632.

[4] Guoshen Yu, Jung S., Audio Classification from Time-Frequency Texture, International Conference on Acoustics, Speech and Signal Processing, ACM Digital Library, 2015, pp. 1677-1680.

# CRYPTANALYSIS – METHODS OF CRACKING CIPHERS*

**ALEKS YA. DANEV**

***ABSTRACT:*** *Cryptanalysis is the science of studying and breaking ciphers in order to extract information from encrypted content. The article discusses the main methods of cryptanalysis, including: frequency analysis, benchmarking, brute force attacks, exploitation of known vulnerabilities. The article highlights the importance of cryptanalysis in the field of security and how new technologies are changing methods for breaking ciphers.*

***KEYWORDS:*** *cryptanalysis, modeling methods, cracking ciphers*

***DOI: https://doi.org/10.46687/IXVZ7735***

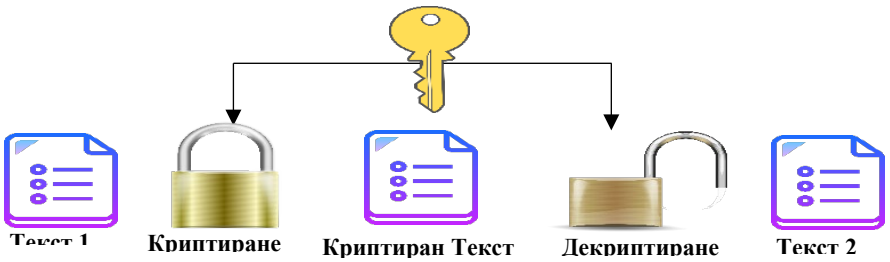
# КРИПТОАНАЛИЗ – МЕТОДИ ЗА РАЗБИВАНЕ НА ШИФРИ

**АЛЕКС Я. ДАНЕВ**

***АБСТРАКТ:*** *Криптоанализът е науката за изучаване и разбиване на шифри с цел извличане на информация от криптирано съдържание. В този доклад се разглеждат основните методи на криптоанализ, включително: честотен анализ, сравнителен анализ, атаки с брутфорс, използване на известни уязвимости. Докладът подчертава значението на криптоанализа в областта на сигурността и как новите технологии променят методите за разбиване на шифри.*

## 1 Въведение

Криптоанализът представлява научна дисциплина в рамките на криптологията, която се занимава с изследването и приложението на методи за компрометиране на криптографски шифри и системи за защита на информацията. Неговата основна цел е да се възстанови оригиналното съдържание на съобщение без никакво наличие на достъп до самия ключ, предназначен за неговото дешифриране. В криптоанализа се използват различни математически, статистически и логически подходи, за да се открият слабости в шифрите и алгоритмите за сигурност. [1, 3, 7]




**Фиг. 1.** Действието на криптоанализа

## 2 Основни видове атаки

В криптоанализа се използват различни видове атаки за разбиване на шифри. Основните от тях включват:

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

- ***Атака със статистически анализ***

Статистическият анализ представлява един от класическите подходи в криптоанализа, който се прилага за компрометиране на шифри, основаващи се на честотния анализ на символите. Той разчита на наблюдение на често срещани модели в шифрованите съобщения и сравняването им със статистическите характеристики на открития текст (естествен език или други формати). Например, в английския език буквите "E" и "T" се срещат по-често от други, което може да се използва за разбиване на шифри като Цезаровият шифър или моноалфабетни заместания. Ето и следният пример: Ако анализираме честотата на буквите в шифриран текст и забележим, че определена буква се повтаря най-често, можем да предположим, че тя съответства на често срещан символ в оригиналния текст, като "E" или "T".

- ***Атака с избран открит текст (Chosen Plaintext Attack - CPA)***

В този вид атака, криптоаналитикът има възможност да избере произволен открит текст и да го криптира, за да получи съответстващия шифрован текст. Чрез анализа на получените резултати той е в състояние да извлече информация относно използвания криптографски ключ или алгоритъм. **Пример:** При някои по-стари версии на алгоритми като DES, изследователите успяват да съберат голямо количество открит текст и съответстващи шифровани текстове и така да открият модели, които водят до компрометиране на ключа.

- ***Атака с избран шифрован текст (Chosen Ciphertext Attack - CCA)***

При атака с избран шифрован текст (Chosen Ciphertext Attack - CCA) атакуващият има достъп до шифрован текст и може да подбира определени шифровани текстове, които да подаде за декриптиране, с цел да анализира получените открити текстове и да анализира получените открити текстове и да извлече информация относно криптографския алгоритъм и неговите уязвимости. Този метод е по-сложен за осъществяване, тъй като изисква декриптиране на специфични текстове, но е особено ефективен срещу криптосистеми, които не са адекватно защитени срещу CCA атаки.

- ***Атака с познат открит текст (Known Plaintext Attack - KPA)***

Този тип атака възниква, когато криптоаналитикът има достъп до една или повече двойки от открит текст и съответстващ шифрован текст. Използвайки познанията си за структурата на откритията текст, криптоаналитикът може да приложи тази информация, за да разкрие част от криптографския ключ или да извлече данни относно криптографския алгоритъм и неговите уязвимости.

- ***Брутфорс атака (Brute-force Attack)***

Това е метод, при който атакуващият опитва всички възможни комбинации за ключа, докато не намери правилния. Въпреки че брутфорс атаките не са особено интелигентни, те могат да бъдат ефективни срещу шифър с по-къси ключове, като Цезаровия шифър. С нарастваща дължина на ключовете, времето, необходимо за изпълнение на брутфорс атака, нараства експоненциално.

- ***Диференциален и линеен криптоанализ***

Тези по-сложни математически методи се използват срещу съвременни блокови шифър като DES и AES. Диференциалния криптоанализ се фокусира върху разликите между двата шифровани текста при малки промени в откритията текст, за да открие зависимостите между тях и ключа. А пък линейният криптоанализ търси линейни зависимости между битовете на откритията и шифрования текст, които могат да бъдат използвани за отгатване на ключа. [2, 5, 6, 10]

- ***Атака по време на изпълнение (Timing Attack)***

При този тип атака атакуващият измерва времето, необходимо за изпълнението на различни криптографски операции, и използва тези данни, за да получи информация за ключа.

Тази атака може да бъде особено успешна срещу алгоритми, при които времето за изпълнение зависи от конкретни стойности на ключа.

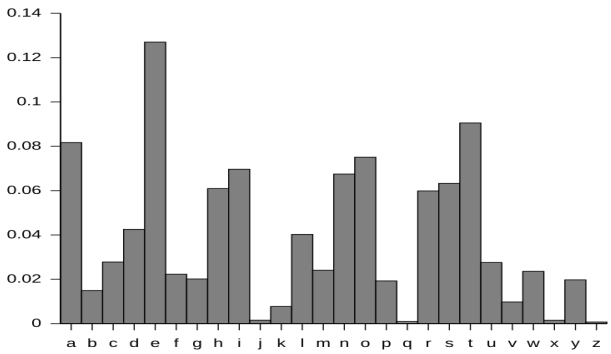
- ***Атака със страничен канал (Side-Channel Attack)***

Това са атаки, които не се фокусират върху криптографския алгоритъм сам по себе си, а върху физически фактори, като потреблението на електричество, топлина или електромагнитни излъчвания на устройството, което изпълнява криптографските операции. Тези фактори могат да предоставят информация относно ключа или структурата на алгоритъма.

Криптоанализът играе важна роля в сигурността на съвременните комуникации и защита на данните. Въпреки че съвременните криптографски системи са доста устойчиви на класическите методи за криптоанализ, продължаващото развитие на квантовите изчисления и новите математически подходи може да промени сигурността на много от настоящите алгоритми. Разбирането на различните атаки е от съществено значение за усъвършенстването и укрепването на сигурността на информационните системи.

# 3 Техники и модели за криптоанализ

Статистически анализ (Frequency Analysis) Това е един от най-старите и добре познати методи за криптоанализ, особено ефективен срещу класически шифър, като моноалфабетните заместявания. Основната идея на статистическия анализ е да се използва честотно разпределение на буквите или символите в шифрования текст и да се съпостави с честотното разпределение в естествения език. Например, в английския език буквите „E“, „T“, „A“ и „O“ се срещат най-често, докато символи като „X“ и „Q“ са редки. В редица класически шифър, като Цезаровия шифър и шифъра на Виженер, честотното разпределение на шифрованите символи запазва своята връзка с оригиналния текст, което позволява сравнително лесно пробиване, чрез прилагане на този метод. **Пример:** Статистическият анализ е използван успешно от криптоаналитиците по време на арабския Златен век, когато известният арабски учен Ал-Кинди създава метода за честотен анализ около IX век. Той е един от първите, който успява да разбие шифър чрез анализ на честотата на буквите.




**Фиг. 2.** Вероятност за разбиване на шифър [3]

Диференциален и линеен криптоанализ. Тези методи са специализирани форми на криптоанализ, които се прилагат към съвременни блокови шифри. Ето и как работят по-задълбочено:

- **Диференциален криптоанализ** - Диференциалният криптоанализ се използва като метод за анализ на ефекта от минимални изменения в открития текст и за проследяване на тези изменения през различните етапи на шифроване. Този подход изследва как разликите във входните данни (открит текст) водят до предсказуеми разлики в изходните данни (шифрован текст). Когато малки промени в откритията текст водят до предвидими изменения в шифрования текст, това дава възможност на криптоаналитика да извлече важна информация за вътрешната структура на шифъра и, при определени условия, да идентифицира криптографския ключ. Диференциалният криптоанализ е разработен през 80-те години от Ели Бихам и Ади Шамир, въпреки че придобива широка популярност през 90-те години, когато резултатите от техните изследвания стават по-достъпни и използвани. Друг супер значим аспект е усъвършенстването и укрепването на диференциалния криптоанализ, което повишава неговата ефективност и адаптивност към различни криптографски алгоритми. По отношение на влиянието върху съвременните шифри, като AES, диференциалният криптоанализ има значителен принос към техния дизайн. При разработването на AES, устойчивостта срещу диференциален криптоанализ е специално взета предвид, което води до създаването на алгоритъм, минимизиращ предвидимите зависимости, които потенциално биха могли да се използват за криптоаналитична атака.
- **Линеен криптоанализ** - търси линейни зависимости между битовете на открития текст, шифрования текст и ключа. Това означава, че криптоаналитикът се опитва да намери уравнения, които описват връзката между входа (открития текст) и изхода (шифрования текст), като използва малък брой битове от тези данни. Това е една изключително изобретателна черта за откриване на линейни зависимости.

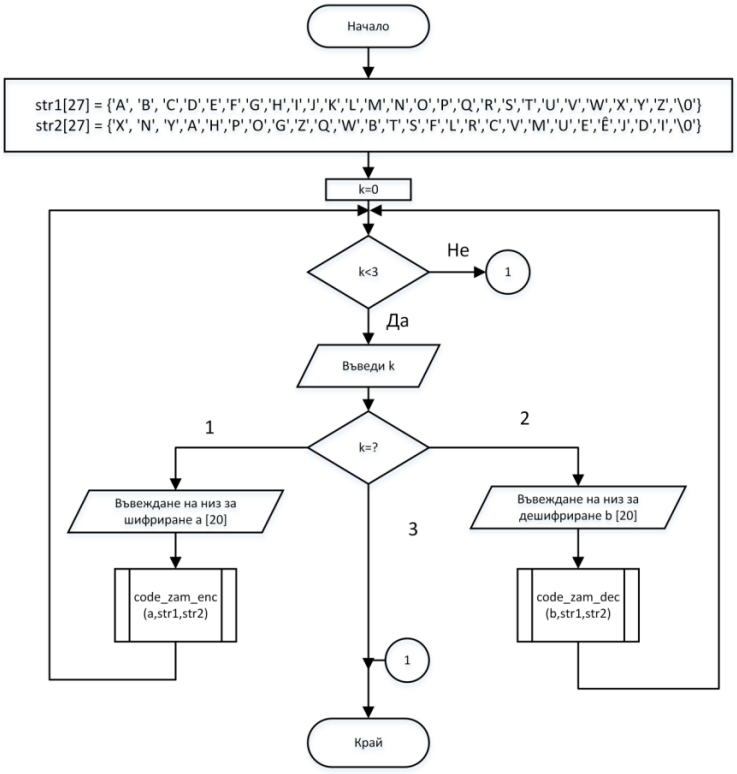
Посредством натрупване на достатъчно статистическа информация от множество шифровани текстове, криптоаналитикът може да извлече съществена информация за ключа. Тази техника се прилага предимно за разбиване на блокови шифри.

## 4 Алгоритмични атаки върху асиметрични шифри

Асиметричните алгоритми, като RSA и ECC (елиптични криви), са по-сложни за разбиване, но съществуват специфични методи за атака върху тях:

Факторизация на големи числа (RSA) - RSA се основава на трудността при факторизирането на произведение от две големи прости числа. Криптоаналитиците търсят методи за ускоряване на процеса на факторизация на тези числа в сравнение с традиционните подходи. Една от най-значимите известни атаки срещу RSA е използването на квантови компютри, които, чрез алгоритъма на Шор, могат да осъществят факторизацията значително по-ефективно, което би застрашило сигурността на RSA.

Атаки върху алгоритмите с елиптични криви - асиметричните алгоритми с елиптични криви (като ECDSA) се считат за по-сигурни и изискват по-малки ключове за същото ниво на сигурност като RSA. Въпреки това, атаки като Pohlig-Hellman могат да бъдат ефективни, ако ординалът на кривата има малки фактори. Друг метод за атака е чрез използването на винкелови атаки, където криптоаналитиците търсят слабости в параметрите на кривата. [4]




**Фиг. 3.** Алгоритъм за разбиване на асиметрични шифри [6]

**Таблица 1.** *Алгоритмични атаки върху асиметрични шифри*

| Алгоритъм | Метод на атака | Описание |
|---|---|---|
| ***RSA*** | *Факторизация на големи числа* | *Трудността на факторизацията е основа на сигурността; атаките целят ускоряване на процеса.* |
| | *Атака с квантови компютри* | *Използване на алгоритъра на Шор за ефективна факторизация на RSA.* |
| ***ECC*** | *Атака Pohlig-Hellman* | *Ефективна, ако ординалът на кривата има малки фактори.* |
| | *Винкелови атаки* | *Търсене на слабости в параметрите на елиптичната крива.* |

# 5 Криптоанализ с използване на квантови изчисления

Квантовите изчисления представляват голяма заплаха за съвременната криптография. Докато класическите компютри изискват експоненциално време за разбиване на алгоритми като RSA и ECC, квантовите компютри с алгоритъма на Шор могат да решат тези задачи полиномиално бързо. Това означава, че съвременните криптографски алгоритми могат да бъдат компрометирани, ако квантовите компютри станат реалистична заплаха в бъдеще.
Друг основополагающ фактор. Хомоморфно криптиране и атаки върху него Хомоморфното криптиране позволява операции върху криптирани данни, без те да бъдат разкривани. Въпреки че това представлява революционна технология за защита на данните, криптоаналитиците могат да търсят методи за компрометиране на тези системи чрез атаки с избран шифрован текст или чрез странични канали, при които се анализират допълнителни фактори, като например времето за обработка на данните. [4, 8, 9]

Квантовото изчисление представлява приложение на фундаменталните принципи на квантовата механика за осъществяване на високосложни изчислителни операции. По-конкретно, то използва квантовите състояния на субатомните частици, като суперпозиция и квантово заплитане, за създаването на квантови компютри. Когато се прилагат върху квантови компютри с достатъчна изчислителна мощност, специфични алгоритми могат да извършват изчисления многократно по-бързо от класическите компютри и дори да решават проблеми, които са извън обхвата на съвременната компютърна технология. В резултат на това наблюдаваме всеотдаен, изключително силен и повишен интерес за съществена информация от страна на правителствата и индустриалните среди по целия свят относно разработването на квантови компютри. Последните постижения в областта на квантовите изчисления, като процесора Quantum Heron на IBM, значително подобриха точността чрез намаляване на грешките, демонстрирайки бърз напредък в тази област. Представянето на IBM Quantum System Two, оборудвана с тези усъвършенствани процесори, бележи важен етап към създаването на практически квантово-центрични суперкомпютри.

- **Уязвимости на съвременните криптографски системи**

Много от съвременните криптографски системи зависят не само от математическите алгоритми, но и от правилното им прилагане. Основни уязвимости могат да възникнат от:

Неправилно управление на ключовете – Проблеми като повторно използване на ключове, слаба генерация на случайни числа или неправилно съхранение на ключовете могат да компрометират сигурността на системата.

Човешки грешки – Често слабостите в криптографските системи се дължат на неправилна употреба от страна на потребителите. Например, използването на слаби пароли или изтичането на чувствителна информация могат да предоставят на криптоаналитиците възможност за достъп до критични данни.

Остаряване на алгоритмите – Алгоритми, които някога са се считали за сигурни, като DES, вече са разбити и се смятат за уязвими. С времето и напредването на криптоанализа дори съвременните алгоритми като RSA може да станат уязвими.

Криптоанализът представлява динамична област, която постоянно се развива в съответствие с напредъка на технологиите. Въпреки че съвременните криптографски алгоритми предлагат висока степен на сигурност, новите методи за криптоанализ и развитието на квантовите изчисления налагат необходимост от продължаващо усъвършенстване на криптографските протоколи.

- **Атаки с избран открит текст**

При този метод криптоаналитикът има възможността да избере конкретни открити текстове (нешифровани данни), които да бъдат криптирани с цел последващ анализ на резултатите и извличане на информация за ключа или използвания криптографски алгоритъм. Според мнозина енциклопедисти, по този начин се изгражда основата за изучаването на уязвимостите в криптографските системи. Тази техника е особено ефективна, когато атакуващият разполага с ограничен достъп до криптографската система.

- **Квантови атаки**

С развитието на квантовите изчисления, криптографските системи като RSA са изправени пред нови заплахи. Алгоритъмът на Шор, функциониращ на квантов компютър, би могъл значително да ускори процеса на факторизация на големи числа, което би компрометирало сигурността на RSA.

Както се и предполага, без съмнение това е уникално предизвикателство за съвременната криптография. Квантовите атаки представляват сериозна заплаха за асиметричните

криптографски системи, докато симетрични криптографски методи като AES остават по-устойчиви на този вид атаки.

Квантовата заплаха е сериозна загриженост, тъй като популярността на квантовите изчисления нараства и коренно променя цифровия пейзаж. Квантовото изчисление, което някога беше интелектуално любопитство от средата на 20-ти век, сега е обещаващ факт. Идеите, които правят тази технология толкова мощна, произлизат от сложната област на квантовата физика. [7]

**Таблица 2.** *Криптографски алгоритъм*

| Алгоритъм | Методи за атака | Описание |
|---|---|---|
| ***RSA*** | *Алгоритъм на Шор* | *Позволява полиномиално бърза факторизация на големи числа, заплашвайки сигурността на RSA.* |
| ***ECC*** | *Pohlig-Hellman атаки* | *Използване на уязвимости в параметрите на елиптичните криви.* |
| ***Хомоморфно криптиране*** | *Атаки с избран шифрован текст* | *Извършване на операции върху криптирани данни без разкритие; възможност за анализ на странични канали.* |

**Таблица 3.** *Квантово обозначение*

| Метод | Описание | Приложимост |
|---|---|---|
| ***Атаки с избран открит текст*** | *Позволява на криптоаналитика да избира текстове за криптиране с цел анализ и извличане на информация.* | *Висока, при ограничен достъп* |
| ***Квантови атаки*** | *Използване на квантови компютри за ускоряване на криптоанализа, особено на RSA.* | *Асиметрични алгоритми* |

# 6 Заключение

Криптоанализът е съществена част от науката за информационната сигурност, която играе критична роля при оценката и усъвършенстването на устойчиви криптографски системи. През последните десетилетия областта на криптоанализата претърпя значителна еволюция – от класически подходи като честотен анализ и анализ на ключови думи до съвременни методи, изградени на базата на статистически модели, алгоритми и машинно обучение. Разработването на криптоанализаторски методи не само поставя на изпит сигурността на съществуващите системи, но също така предоставя ценни сведения за техните уязвимости, които следва да бъдат адресирани за изграждане на по-устойчива защита.

С нарастващата сложност на цифровата среда и потенциала за развитие на квантовите компютри, криптоанализът е изправен пред нови предизвикателства и изисква непрекъснати иновации, за да противодейства на възникващите заплахи. Квантовите изчисления, например, притежават способността да направят традиционните криптографски системи като RSA и ECC уязвими, което налага неотложното търсене на квантово-устойчиви алгоритми. Същевременно, с напредъка на квантовата механика, криптоанализът се превръща в специализиран и комплексен процес, който все повече разчита на квантови принципи за осъществяване на прецизни криптоаналитични атаки и разработване на адаптивни решения. [1, 4, 5, 9, 10]

Криптоанализът се утвърждава като динамична и всеобхватна дисциплина, която остава от основно значение за защитата на данните в съвременния цифров свят. Методите и подходите в тази област продължават да се развиват, като отговарят на технологичните нововъведения и поставят основите за бъдещето на информационната сигурност.

**ЛИТЕРАТУРА:**

[1] Антонов П., Малчев С., Криптография в компютърните комуникации, 2000, Варна, ТУ

[2] Беджев Б., Комплект лекции по Криптология, 2013, Университетско издателство „Еп. К. Преславски", Шумен

[3] 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, 2011, ISBN 978-954-577-620-5.

[4] Ariyur K., Achieving Altshuller's Dream: Going from Heuristics to Algorithms to make Creativity Scientific, 2018, Conference: TRIZCON West Lafayette, Indiana, USA, pp. 130-145

[5] Denev D., Tsankov Ts. A Survey of Data Quality in Digital Processing of Acoustic Signals. 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, ISBN 978-1-6654-9149-5, pp. 1–5,

[6] Konstantinova E., Tsankov Ts. Quantum prime factorization with Shor's algorithm. Annual of Konstantin Preslavski University of Shumen, Vol. IX E, Faculty of technical sciences, 2019, ISSN 1311-834X, pp. 10-14.

[7] Nikolov N., Ivanov G., Ducheva V., Generation of Substitution Tables with Good Cryptographic Properties using Artificial Immune system, 2014, International Scientific Conference MATTEX, Shumen. ISSN 1314-3921

[8] Salil V., Alon R., Private-Key Encryption: Perfect Secrecy, 2006, Sydney, Australia

[9] https://vlab.1avto.com/?f=page1

[10] https://www.ssl.com/bg/

# INFLUENCE OF QUANTUM COMPUTERS OVER RSA ALGORITHM*

**GEORGI D. DIMITROV**

***ABSTRACT:*** *Research of the growing influence and problems of quantom computers over RSA algorithms. The power of security RSA is in unableness of factorising big binary numbers from todays normal computers. They are needed thousand of years for calculating of the algorithm numbers, even if its quantom. There are researches for calculating of RSA algorithm with quantom computes with the help of different algorithms for factoring of prime numbers, which can conclude to its full cracking. Scientists are researching new crypt algorithms which can work with quantom computers, but they are still not in use and are only in the drawing board.*

***KEYWORDS:*** *RSA algorithm, quantum computers, cryptology*

***DOI: https://doi.org/10.46687/ZSOD7807***

# ИЗСЛЕДВАНЕ НА ВЛИЯНИЕТО НА КВАНТОВИТЕ КОМПЮТРИ ВЪРХУ RSA АЛГОРИТЪМА

**ГЕОРГИ Д. ДИМИТРОВ**

***АБСТРАКТ:*** *Изследване на все по-нарастващото влияние и проблеми на квантовите компютри върху RSA алгоритъма. Сложността на RSA е в невъзможността за факторизиране на големи числа от обикновените битови компютри. За изчислението на числата от криптиращите ключове са нужни няколко хиляди години от мощен компютър, дори и квантов. Съществуват стъпки за изследвания на пресмятане на алгоритъма RSA от квантов компютър с помощта на различни алгоритми за разлагане на цели числа, което е предпоставка за по-нататъшни разработки за пълното му разбиване. Разработват се нови алгоритми за криптиране, които да работят с квантовата технология, но са все още в период на изследвания.*

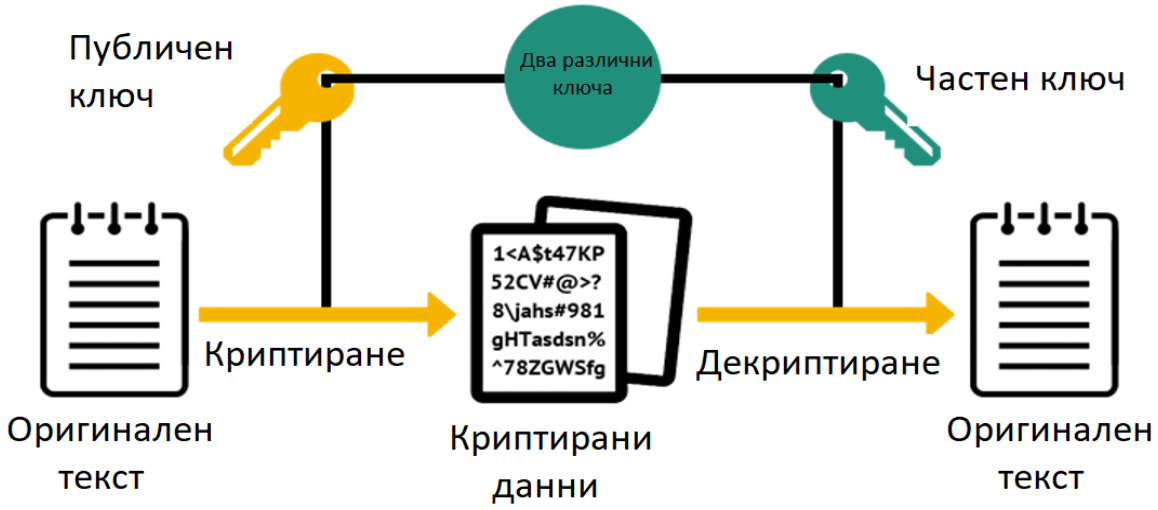
## 1 Въведение

RSA Алгоритъмът е алгоритъм за асинхронно криптиране. Алгоритъма разчита на факторизацията на две големи прости числа. Той решава проблема как да изпратиш криптирана информация до някой, без предварително да споделиш ключа за криптиране и декриптиране с него. През 1977г. Роналд Ривест, Леонард Аделман и Ади Шамир започват разработването му, като всъщност името RSA е съкратено от първите букви на тримата учени (Rivest, Shamir, Adleman), но те не са пионерите в областта. За пръв път през 1973г. идеята за публичен ключ е използвал Клифорд Кокс, който е английски математик и алгоритъма му е бил засекретен от Главното Управление на Комуникациите(GCHQ). През 1983г. RSA алгоритъмът е патентован за срок от 17 години. Патентът му: US 4,405,829 е насрочен да изтича на 21.09.2000г., но от компанията, притежаваща патента RSA Security публикуват алгоритъма за публично ползване на 6.09.2000г. и така е освободен от лицензи. И до днес се използва като един от основните алгоритми за подобряване на сигурността в протоколите SSH, S/MIME, SSL/TLS и др. за криптирана интернет комуникация,VPN,банковата система SWIFT също така и за електронни подписи, софтуерни програми (например браузъри). [1, 2, 3, 15]

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

## 2 Начин на действие

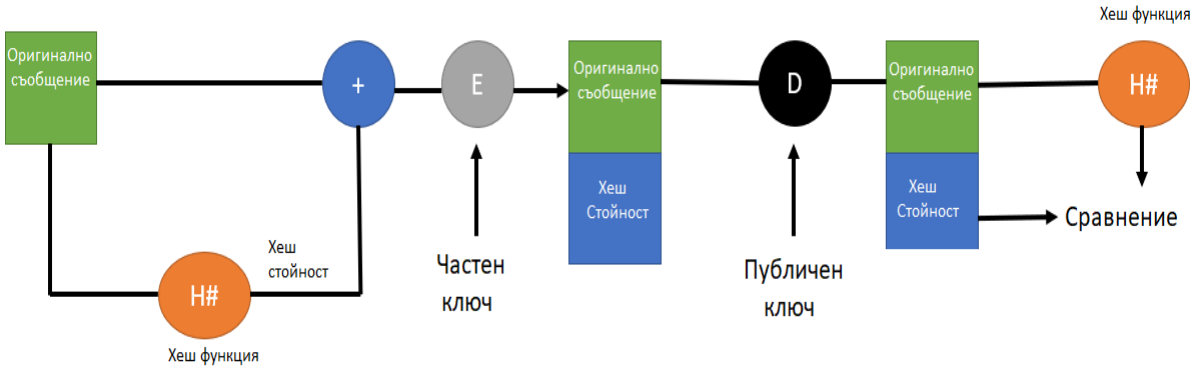
При RSA алгоритъмът се използват два ключа, като единия е публичен, а другия е т.н. частен ключ. И двата ключа се генерират от клиента, но частният ключ го знае само той, а публичния може да е достъпен на всеки в мрежата. Съобщенията могат да се криптират от всеки с публичния ключ, но могат да се декриптрат само от частния ключ. Двата ключа винаги са математически свързани. Механизма работи по следния начин (Фиг.1.) (Например с клиент и сървър) :




Фиг. 1.

- Клиентът праща заявка до сървъра заедно с публичния ключ;
- Сървърът криптира данните с помощта на ключа и праща данните на клиента;
- Клиента разчита данните, като използва частния ключ, който е наличен само в него.

При електронния подпис и верификация може да се каже, че процеса е обратен. Данните се криптират с частния ключ, след което се дешифрират с публичния ключ. Това само по себе си подсказва, че ако дешифрирането с частния ключ е успешно, значи е използван правилния частен ключ. Метода е (Фиг. 2.):




Фиг. 2.

- Данните се подават към хеш функция;
- Смесват се с хеш стойността и се криптират с частния ключ;
- Изпращат се на получателя и се декриптират;
- Данните преминават през същата хеш функция, както в началото;
- Сравнява се новата и старата стойност на хеша и ако съвпадат данните се верифицират.

Тези два метода са основните при работа с RSA алгоритъм. Те гарантират верифицирането, автентикацията, конфиденциалността и целостта на данните. [1, 4, 14]

# 3 Начин на криптиране

Първата задача е да се генерират публичния и частния ключ. Това е работа на получателя на съобщението, като до него предварително е изпратена заявка. Ключовете са с дължина между 1024 и 4096 бита като първите се считат за несигурни. Днешния стандарт за дължина е 2048 бита, а всички следващи по-големи се считат за по-сигурни и се използват за по рискови данни. За генерирането на публичния и частния ключ се използват две големи прости числа обозначени с p и q. След това се изчислява модулът на частния и публичния ключ чрез n:

$$n=p*q$$

Числото n се предава заедно с публичния ключ

Изчислява се Тотиентата за p и q:

$$\varphi=(p-1)*(q-1),$$

която остава при частния ключ и е „тайна“. Следващата стъпка е да се генерира случайно число e, за което важи:

$$1<e<\varphi$$

Също така необходимо условие е φ и e да са взаимно прости. Това число ще бъде степента на публичния ключ. Следва да се избере и степента на частния ключ d. Трябва да е такова число, че:

$$d\equiv 1*(\mathrm{mod}\ \varphi(n))$$

Това е всичко, което ни е нужно за създаването на двата ключа. Публичният ключ или по-точно числата n и e се изпращат на изпращача. Следващата стъпка е да се шифрира самото съобщение с помощта на ASCII, Unicode, Base64 или друга кодираща таблица. След като съобщението се кодира следва да се криптира по формулата:

$$C=M^e*\mathrm{mod}(n),$$

където M е кодираното съобщение, а C е готовото криптирано съобщение. Изпращачът е готов да изпрати данните получателя. За получателя остава да декриптира съобщението, като използва своя ключ n и d. Това се прави по формулата:

$$M=C^d*\mathrm{mod}(n)$$

И до тук комуникацията с криптиране между двамата е пълна. [1, 4, 13]

# 4 Ползи и недостатъци

Ползите на RSA алгоритъма са, че големите числа, използвани от него изискват много време за обратното изчисление за намиране на числата от частния ключ, но това освен полза

е и недостатък. Големите числа също така изискват и по-голяма изчислителна мощ при декриптирането при нормалната комуникация. Допълнителна сигурност идва и от факта, че частния ключ, без който не може да се декриптира съобщението, не се споделя с никой и остава невидим за трети страни (например т.н. снифери) или други атаки. С развитието на комуникационната техника се развиват и науките, което дава допълнителна сигурност на RSA алгоритъма, защото се откриват нови начини за предаване на все по-големи пакети от данни, което позволява предаването на по-дълги ключове. Най-голяма сигурност дава факта, че до сега не е известен достатъчно бърз алгоритъм за разделяне на число на прости множители. В днешно време с напредването на квантовите компютри различни учени твърдят, че е възможно да се „разбие“ RSA алгоритъма. До днес алгоритъмът остава най-сигурния за криптиране на различни типове данни. [5, 6, 12, 16]

## 5 Анализ на RSA и квантовите компютри

През 2020г. Global Risk Institute, който изследва рисковете финансовия сектор е публикувал доклад, за влиянието и бъдещото влияние на квантовите компютри върху RSA. От този доклад става ясно, че според изследванията на института до 30 години квантовите компютри ще могат да разшифроват RSA за по-малко от 24 часа. След две години излиза друг доклад на екип от китайски учени, които твърдят, че са провели изследвания и че е възможно да се „разбие“ 2048 битов RSA алгоритъм с помощта на 372 кубитов компютър (по това време най-мощният е 433 кубитов на IBM) и алгоритъма на Шор. През 2023г. успяват да факторизират 48 битово число с 10 кубитов компютър. През октомври 2024г. отново китайски учени публикуваха доклад, в който се твърди, че с помощта на 5760 кубитов компютър са подложили на изпитание RSA алгоритъм успешно. След това се оказа, че числото използвано за изпитанието е 50 битово, но това не може да се счита за повратен момент, защото при сложните ключове днес 50 бита са 9.67*10^16 вариации в сравнение с 1024 (1.797*10^308) или 2048 (3.231*10^616) бита, които се ползват днес. Китайските учени твърдят, че техния алгоритъм може да се използва и на по-големи числа, въпреки че все още не са проведени достатъчно изпитания. Това поставя въпроса за сигурността на банковите преводи и на всички комуникации използващи RSA. [7, 8, 9, 10, 11]

## 6 Заключение

Според авторите комбинация между алгоритъма на Шор, правилен алгоритъм за оптимизиране на квантовите изчисления и достатъчно мощен компютър ще може да изчисли над 1024 битви числа от RSA, за да го направи безполезен. Въпреки, че за сега разработките не са създали мощен квантов компютър за разбиране на RSA алгоритми достигането на това ниво е все по-близо. След факторизацията, което е „разбиване“ на 50 битово число от RSA алгоритъма логичната стъпка е да се пробва с по-големи числа до намиране на тяхното решение. Голяма част от комуникацията в интернет може в един момент да бъде застрашена, а сигурността сведена до минимум. RSA се ползва от дълги години и се е наложил като основен компонент от сигурността, което може да се окаже огромен недостатък на системите. От различните разработчици ще зависи как и колко бързо ще успеят да се ориентират към нови способи и алгоритми за криптиране, и защита на данните. В момента се работи над различни пост-квантови алгоритми, които да заместят сегашните, но успешната им инфилтрация в различните системи, приложения и протоколи е под въпрос, защото не се знае дали и те няма да се окажат прекалено слаба пречка за бъдещите квантови компютри с милиони кюбитове. В сферата на криптологията (криптографията) до сега сигурността в повечето случаи е изпреварвала развитието на техниката. Ако този баланс се наруши това може да застраши много отрасли по цял свят.

**ЛИТЕРАТУРА:**

[1] Ланджев И., Русева А. Аспекти на комбинаториката. Нов Български Университет, 2023г.

[2] Chao W., Qi Di W. Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage, Shanghai University, Shanghai, 2024.

[3] Denev D., Tsankov Ts. Development of a virtual private network in computer networks and communication environments. International scientific refereed online journal with impact factor SocioBrains, Issue 71, July 2020, ISSN 2367-5721, pp. 11-19.

[4] Denev D., Tsankov Ts. Synthesis and analysis of linear, discrete and time-invariant systems, used in the field of communications, using MATLAB and signal processing toolbox. Journal scientific and applied research, vol. 22, 2022, ISSN 1314-6289, pp. 72-80.

[5] Gheorghiu V., Mosca M. GRI quantum risk assessment report Feb. 2020, evolutionQ Inc.

[6] Konstantinova E., Tsankov Ts. Quantum prime factorization with Shor's algorithm. Annual of Konstantin Preslavski University of Shumen, Vol. IX E, Faculty of technical sciences, 2019, ISSN 1311-834X, pp. 10-14.

[7] Konstantinova E., Tsankov Ts. The use of packet sniffing tools in computer networks security. International Scientific Conference "Defense Technologies" DefTech 2020, ISSN 2367-7902, pp. 401-406.

[8] Mollin R. RSA and Public-Key Cryptography. CRC Press, 2002.

[9] Tsankov Ts., Konstantinova E. Analyzing security threats in smart homes technology. International Scientific Conference "Defense Technologies" DefTech 2020, ISSN 2367-7902, pp. 373-378.

[10] Yan B., Tan, Z. Factoring integers with sublinear resources on a superconducting quantum processor. 2022.

[11] www.rsasecurity.com

[12] https://www.rsa.com/

[13] https://www.gchq.gov.uk/

[14] https://www.ssl.com

[15] https://globalriskinstitute.org/

[16] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

# THE INTERNET OF THINGS (IOT) – COMMUNICATION PROTOCOLS, APPLICATIONS, AND FUTURE TRENDS IN SMART HOMES AND SUSTAINABLE DEVELOPMENT*

**MIHAIL S. SEYKOV, PETYA K. KOLEVA**

***ABSTRACT:*** *The Internet of Things (IoT) is revolutionizing how we interact with our living environments through seamless device communication protocols and advanced automation. This paper examines the evolution, application, and challenges of IoT communication frameworks like MQTT, CoAP, Zigbee, Z-Wave, and Matter. Furthermore, the paper explores IoT's transformative impact on smart homes, sustainability, and artificial intelligence integration, offering insights into future advancements and social implications. The paper also highlights the key security concerns, interoperability challenges, and the prospects of IoT integration in the context of emerging technologies like 5G and AI.*

***KEYWORDS:*** *IoT, smart homes, MQTT, CoAP, Zigbee, Z-Wave, Matter, automation, AI, social implications, 5G*

***DOI: https://doi.org/10.46687/ZBVC1878***

# ИНТЕРНЕТ НА НЕЩАТА (IoT) – ПРОТОКОЛИ ЗА КОМУНИКАЦИЯ, ПРИЛОЖЕНИЯ И БЪДЕЩИ ТЕНДЕНЦИИ В ИНТЕЛИГЕНТНИ ДОМОВЕ И УСТОЙЧИВО РАЗВИТИЕ

**МИХАИЛ С. СЕЙКОВ, ПЕТЯ К. КОЛЕВА**

***АБСТРАКТ:*** *Интернет на нещата (IoT) революционизира начина, по който взаимодействаме с нашата жизнена среда чрез безпроблемни комуникационни протоколи между устройства и напреднала автоматизация. Този доклад разглежда еволюцията, приложението и предизвикателствата на комуникационни рамки на IoT като MQTT, CoAP, Zigbee, Z-Wave и Matter. В допълнение, докладът разглежда трансформиращото въздействие на IoT върху интелигентните домове, устойчивостта и интеграцията на изкуствен интелект, като предоставя прозрения за бъдещи постижения и социални последици. Докладът също така подчертава основните проблеми със сигурността, предизвикателства за интероперативност и перспективите за интеграция на IoT в контекста на развиващите се технологии като 5G и AI.*

## 1 Въведение

Развитието на IoT е основен двигател за модернизацията на домовете и начина, по който те взаимодействат с обитателите си. Интелигентните домове притежават технологии като сензори, камери и автоматизирани уреди, обединени чрез мрежи и протоколи, създавайки среда на удобство, безопасност и енергийна ефективност.

IoT не е просто иновация, а вече основна част от ежедневието на много хора. Като тези технологии стават все по-достъпни за обществото ни.

Комуникационните протоколи като MQTT и Zigbee играят ключова роля в тази революция, позволявайки устройства от различни производители да комуникират заедно като една хармонична екосистема. Това създава нова реалност, в която всички елементи на

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

дома могат да бъдат автоматизирани и контролирани чрез приложения и сензори. Докладът разглежда техническите аспекти на тези протоколи и тяхното значение за интелигентните домове, допълвайки анализа с практически приложения и предизвикателства.

# 2 ИСТОРИЧЕСКО РАЗВИТИЕ НА IoT

Интернет на нещата (IoT) възниква като концепция в края на 90-те години, когато свързаните устройства са ограничени основно до индустриални приложения, включващи управление на производствени линии и логистика. Развитието на мобилните технологии и миниатюризацията на хардуера през следващите години допринася за навлизането на IoT в личното пространство, като се създава възможност за разширяване на интелигентните домове. С времето се появяват все по-усъвършенствани устройства като термостати, осветление, камери и системи за сигурност, които се интегрират в общи екосистеми.

Първоначалният етап на развитие (1999-2010) е фокусиран върху концепции като RFID и M2M комуникации. Тези технологии осигуряват основна свързаност между устройства и се прилагат в автоматизацията и индустриалните мрежи. В този период технологията ZigBee започва да се използва, предоставяйки ниска цена и висока надеждност, но същевременно се сблъсква с ограничения като малка изчислителна мощност и уязвимости в сигурността. През следващите години IoT започва да се утвърждава като част от ежедневието. Навлизането на устройства с интуитивни интерфейси, като гласови асистенти и мобилни приложения, позволява лесно управление на интелигентните домове. В този контекст обаче се идентифицират и предизвикателства, свързани с криптографската сигурност и разпределението на ключове в мрежите.

В настоящия етап развитието на 5G мрежи и нови стандарти като Matter предоставя нови възможности за взаимодействие и интеграция на устройства в IoT екосистемите. Технологиите за изкуствен интелект се използват за персонализиране на услугите, което допринася за повишаване на ефективността и удобството. В същото време подобрените механизми за сигурност минимизират рисковете от уязвимости, като се използват еднократни ключове и напреднали криптографски методи. Сигурността в IoT остава приоритет, тъй като мрежите стават все по-сложни. Протоколи като ZigBee се актуализират с нови защитни механизми, които предотвратяват атаки и ограничават рисковете от неоторизиран достъп. Въпреки това, се подчертава необходимостта от допълнителни изследвания и иновации за справяне с нововъзникващите заплахи.

Развитието на IoT подчертава значимостта на тези технологии в различни сфери, включително здравеопазването, транспорта и интелигентните градове. Това налага постоянен напредък в стандартизацията, сигурността и взаимодействието, за да се гарантира по-сигурна и ефективна среда за свързаните устройства. [1, 2, 6, 7, 8]

# 3 IoT АРХИТЕКТУРА И ПРОТОКОЛИ НА КОМУНИКАЦИЯ

IoT архитектурата се състои от четири основни слоя, които работят заедно за осигуряване на ефективна и сигурна комуникация между устройствата:

1. Сензори и устройства: Те събират данни като температура, влажност или движение.

2. Мрежов слой: Осигурява комуникацията чрез различни протоколи като Zigbee, MQTT и Wi-Fi.

3. Облачна инфраструктура**:** Тя съхранява и обработва данни за последваща употреба или бъдещ анализ.

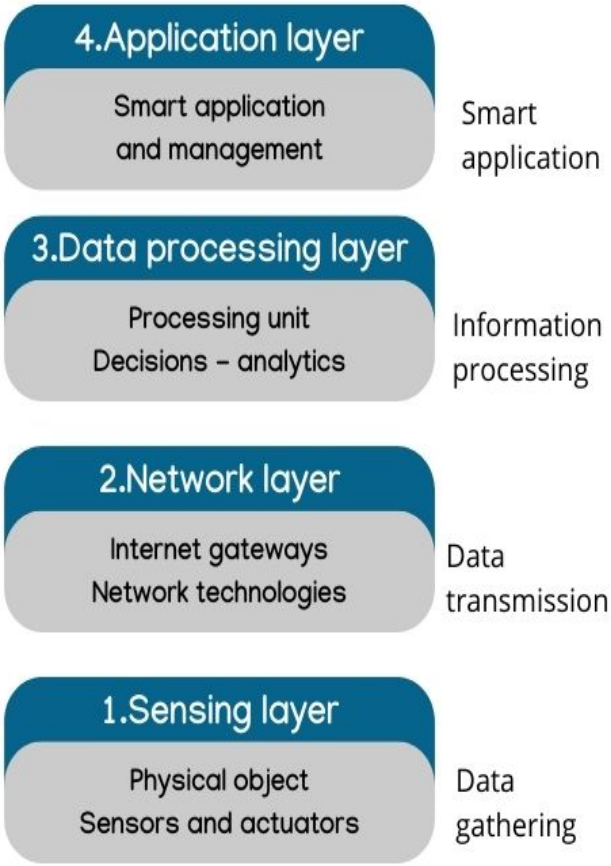
4. Приложен слой: Включва мобилни приложения и интерфейси за управление на устройствата.

Протоколите за комуникация играят основна роля в успешното функциониране на IoT. Те определят как устройствата обменят информация помежду си, също и как се съхраняват и анализират данни. [1, 2, 3, 9, 11]

**MQTT (Message Queuing Telemetry Transport)**

MQTT е протокол, който позволява надеждна комуникация между устройства, дори при слаби мрежи. Той е подходящ за приложения, които изискват чести и малки съобщения с ниска латентност.

- Основни приложения**:** Умни термостати, алармени системи, здравни монитори.
- Пример**:** В интелигентни домове с многобройни устройства MQTT намалява латентността чрез централизиран хъб, който осигурява бърза и ефективна комуникация между устройствата.**CoAP (Constrained Application Protocol)**




**Фиг. 1.** Основните слоеве на IoT архитектурата

CoAP е лек протокол, който използва минимални ресурси и е особено подходящ за сензори с ограничени капацитети. Неговата ефективност го прави популярен в среда на сензорни мрежи и приложения с ниска мощност.

- **Пример:** Автоматизация на осветлението и следене на околната температура. CoAP предлага бърза реакция при промени в околната среда.

**Zigbee и Z-Wave в интелигентните домове**

Zigbee и Z-Wave са два от най-популярните протоколи за безжична комуникация в интелигентните домове, благодарение на тяхната надеждност и ниска енергийна консумация.

- **Zigbee:** Използва mesh топология, при която всяко устройство може да препредава сигнали, което осигурява по-широк обхват на мрежата и висока мащабируемост. Основни приложения включват управление на осветление (Philips Hue), интелигентни контакти и сензори. Предимства: енергийна ефективност и възможност за свързване на до 65 000 устройства.

- **Z-Wave:** Този протокол използва специфична честотна лента, която избягва интерференция с Wi-Fi и Bluetooth. Основни приложения са свързани с управление на системи за сигурност, термостати и интелигентни брави. Лесната интеграция между различни марки устройства е значително предимство.

# 4 IoT и модерните интелигентни къщи

Интелигентните домове са сред най-ярките примери за приложението на IoT технологии, трансформиращи традиционните жилища в автоматизирани системи, които осигуряват комфорт, енергийна ефективност и безопасност. Тези технологии включват широк спектър от устройства и приложения, които взаимодействат помежду си чрез интернет връзки и комуникационни протоколи като ZigBee и Bluetooth. IoT осветителните тела позволяват динамично управление на осветлението в дома. Чрез мобилни приложения или гласови асистенти, потребителите могат да регулират яркостта, цветовата температура и времето за включване и изключване на осветлението. Технологии като LiFi (Light Fidelity) също се изследват за осигуряване на висококоростна комуникация в рамките на дома, използвайки светлинни вълни, които едновременно предоставят осветление и предават данни.

Сигурността на интелигентните домове е друг ключов аспект. Системите за видеонаблюдение, като умни камери, осигуряват постоянно наблюдение и уведомления за движение, като използват криптирани канали за предаване на видео данни. Интелигентни заключващи устройства позволяват дистанционно управление на достъпа до дома чрез мобилни приложения или биометрични идентификатори. Въпреки това, слабости в сигурността на протоколи като ZigBee могат да изложат системите на рискове от подслушване и манипулиране на данни.

Управлението на енергията също играе важна роля. IoT термостати като Nest анализират поведението на потребителите, за да оптимизират температурните настройки и да намалят консумацията на енергия. Интелигентните електромери и интегрираните системи за енергиен мониторинг предоставят подробна информация за консумацията на електроенергия и помагат за нейното ефективно управление. Гласовите асистенти като Amazon Alexa и Google Home действат като централни хъбове за управление на различните IoT устройства в дома. Те осигуряват интеграция между осветителни тела, системи за сигурност, домакински уреди и дори персонални развлекателни системи. С помощта на изкуствен интелект тези асистенти предлагат персонализирани решения за повишаване на удобството и ефективността.

Интелигентните домове не само осигуряват комфорт и удобство, но и представляват платформа за иновации, насочени към устойчивост и екологична ефективност. Продължаващото развитие на IoT технологии обещава още по-софистицирани решения и приложения, които ще направят домовете по-интелигентни и сигурни. [3, 4, 5, 7, 8, 10]

# 5 Влияние на изкуствения интелект върху IoT и бъдещето на интелигентните технологии

Изкуственият интелект (AI) променя значително функционирането и възможностите на IoT технологиите, като осигурява по-висока степен на автоматизация и персонализация. Чрез анализ на поведението на потребителите и използването на исторически данни, AI позволява на IoT устройствата да предлагат адаптивни решения, които оптимизират ежедневните дейности в интелигентните домове. Технологиите за гласово разпознаване, интегрирани в системи като Amazon Alexa и Google Assistant, се базират на AI, за да разбират и изпълняват по-точно командите на потребителите. Допълнително се осигурява навременно предупреждение за технически неизправности на устройствата, което предотвратява сериозни проблеми и намалява разходите за поддръжка.

Устойчивостта също е водещ приоритет при разработването на IoT решения. Интелигентните системи за управление на ресурси, като вода и електричество, намаляват екологичния отпечатък на домакинствата. Системите за напояване оптимизират използването на вода чрез анализ на метеорологичните условия и нуждите на растенията. IoT технологията играе роля и в процесите на рециклиране, като използва сензори за сортиране и управление на отпадъци. Тези иновации насърчават по-ефективното използване на ресурсите и минимизират вредното въздействие върху околната среда. Развитието на IoT среща редица предизвикателства, свързани с мащабируемостта, интероперативността и сигурността. Липсата на унифицирани стандарти между устройствата от различни производители затруднява тяхната интеграция. Освен това, с увеличаването на броя на свързаните устройства, се създават допълнителни изисквания за управление на мрежите и осигуряване на надеждна свързаност. Сигурността остава основен проблем, като уязвимости в протоколи и устройства често водят до риск от неоторизиран достъп или кражба на данни.

Бъдещето на IoT се свързва с внедряването на 5G технологии и нови стандарти като Matter, които ще подобрят съвместимостта и функционалността на устройствата. Благодарение на 5G се очаква значително ускоряване на свързаността и намаляване на латентността, което ще позволи интеграция на още по-сложни IoT системи. Matter предоставя стандартизирана платформа, която улеснява комуникацията между устройства от различни производители, правейки интелигентните домове по-достъпни и ефективни. В допълнение, напредъкът в областта на AI и сигурността ще допринесе за още по-голяма надеждност и безопасност, като същевременно IoT ще продължи да играе ключова роля в устойчивостта и енергийната ефективност на домовете и бизнеса. [5, 6]

# 6 Заключение

IoT е ключова част от бъдещето на интелигентните домове, предоставяща неограничени възможности за автоматизация, енергийна ефективност и персонализиране на обитаването. Въпреки техническите предизвикателства, бъдещите иновации като 5G и AI предлагат обещаващи възможности за още по-интегрирани и интелигентни решения в домовете на утрешния ден.

**ЛИТЕРАТУРА:**

[1] Denev, D., Tsankov, Ts. Development of a virtual private network in computer networks and communication environments. International scientific refereed online journal with impact factor SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71, July 2020, ISSN 2367-5721, pp. 11-19.

[2] Denev, D., Tsankov, Ts. Model of a terminal network device based on a single-chip microcontroller and Ethernet interface. Journal scientific and applied research, vol. 22, 2022, ISSN 1314-6289, pp. 66-71.

[3] 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, 2020, ISSN 2367-7902, pp. 373-378.

[4] Konstantinova, E., Tsankov, Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference "Ecology and environment", 2021, ISSN 2367-5209, pp. 109-121.

[5] 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, 2020, ISSN 2367-7902, pp. 379-385.

[6] Lilov, V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference "Defense Technologies" DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.

[7] https://www.deepseadev.com/en/blog/iot-architecture-explained/

[8] https://www.techradar.com/

[9] https://ieeexplore.ieee.org/

[10] https://www.iotforall.com/

[11] https://www.gartner.com/

# APPLICATION OF CONVOLUTIONAL NEURAL NETWORKS FOR OBJECT RECOGNITION IN AI VIDEO CAMERAS*

**SILVIA H. NIKOLOVA**

***ABSTRACT:*** *With the advancement of technology, especially in the field of artificial intelligence (AI), the capabilities of video cameras have expanded exponentially. One such capability is object recognition, where AI algorithms are used to identify and classify objects in a video feed. This technology has numerous applications in various industries, from surveillance and security to autonomous vehicles and augmented reality. AI object recognition in video cameras involves the use of deep learning algorithms, specifically convolutional neural networks (KHMs). These algorithms are trained on massive datasets of labeled images to learn patterns and features that distinguish one object from another. Once trained, a KHM can analyze video footage in real time and identify objects with a high degree of accuracy.*

***KEYWORDS:*** *artificial intelligence, convolutional neural networks, video surveillance, security systems*

***DOI: https://doi.org/10.46687/BZJI4555***

# ПРИЛОЖЕНИЕ НА КОНВОЛЮЦИОННИ НЕВРОННИ МРЕЖИ ЗА РАЗПОЗНАВАНЕ НА ОБЕКТИ ПРИ ВИДЕОКАМЕРИ С AI

**СИЛВИЯ Х. НИКОЛОВА**

***АБСТРАКТ:*** *С напредъка на технологиите, особено в областта на изкуствения интелект (AI), възможностите на видеокамерите се разшириха експоненциално. Една такава възможност е разпознаването на обекти, където AI алгоритми се използват за идентифициране и класифициране на обекти във видео емисия. Тази технология има множество приложения в различни индустрии, от наблюдение и сигурност до автономни превозни средства и добавена реалност. Разпознаването на обекти с AI във видеокамерите включва използването на алгоритми за дълбоко обучение, по-специално конволюционни невронни мрежи (КНМ). Тези алгоритми се обучават върху масивни набори от данни от етикетирани изображения, за да научат модели и характеристики, които отличават един обект от друг. Веднъж обучен, КНМ може да анализира видео кадри в реално време и да идентифицира обекти с висока степен на точност.*

## 1 Въведение

Конволюционните невронни мрежи (КНМ) представляват специализирана архитектура в областта на дълбокото обучение, проектирана специално за обработка на визуални данни. За разлика от традиционните невронни мрежи, КНМ използват уникална структура, която включва конволюционни слоеве, което им позволява автоматично да извличат йерархични характеристики от изображения. Тази способност позволява на КНМ да се обучават от необработени пикселни данни, ефективно елиминирайки необходимостта от ръчно извличане на функции. [1, 2, 10, 11]

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

Чрез прилагане на конволюционни операции тези мрежи могат да разпознават модели и структури в изображенията, което ги прави изключително подходящи за задачи като разпознаване на обекти и класификация на изображения [3].

Ключовите компоненти на КНМ играят решаваща роля за тяхната функционалност, по-специално конволюционните слоеве, слоевете за обединяване и напълно свързаните слоеве [4]. Конволюционните слоеве са отговорни за прилагането на филтри към входните изображения, което помага при откриването на ръбове, текстури и други важни характеристики. Следвайки конволюционните слоеве, обединяващите слоеве намаляват размерността на данните, позволявайки на мрежата да стане по-ефективна и по-малко склонна към пренастройване [3]. И накрая, напълно свързаните слоеве служат като класификатори, като вземат характеристиките на високо ниво, извлечени от предишните слоеве, и произвеждат крайния изход за задачи като разпознаване на обекти. Тази многослойна архитектура позволява на КНМ да улавят сложни модели и връзки в данните, подобрявайки цялостната им производителност в приложенията за обработка на изображения [5].

Предимствата от използването на КНМ при обработката на изображения са значителни, което ги прави предпочитан избор за различни приложения, изискващи разпознаване на обекти [4]. Едно от най-значимите предимства е способността им да постигнат висока точност с по-малко предварителна обработка в сравнение с традиционните методи, които често изискват обширно инженерство на функции. Освен това КНМ са силно мащабируеми, което им позволява да обработват големи набори от данни и сложни изображения без значителен спад в производителността [4]. Тяхната устойчивост на вариации в мащаба, въртенето и транслацията също допринася за тяхната ефективност в реални приложения, като например във видеокамери с изкуствен интелект и самоуправляващи се превозни средства, където точното разпознаване на обекти е от решаващо значение за безопасността и функционалността [2]. В резултат на това КНМ се превърнаха в неразделна част от напредъка в технологията за компютърно зрение, стимулирайки иновациите в множество сектори.

## 2 Техники за разпознаване на обекти с помощта на КНМ

Предварителната обработка и увеличаването на данните са ключови стъпки в приложението на конволюционните невронни мрежи (КНМ) за разпознаване на обекти, тъй като те значително подобряват качеството и количеството на входните данни [3]. Предварителната обработка включва техники като нормализиране, преоразмеряване и конвертиране на изображения в подходящ формат, което може да помогне за подобряване на работата на КНМ, като гарантира, че входните данни са последователни и стандартизирани [2]. Освен това техниките за увеличаване на данни, като завъртане, обръщане, мащабиране и корекции на цвета, могат изкуствено да разширят набора от данни за обучение, позволявайки на модела да се учи от по-разнообразен набор от примери. Този подход не само смекчава пренастройването, но също така повишава способността на модела да обобщава нови, невиждани данни, което в крайна сметка води до по-стабилни възможности за разпознаване на обекти.

Обучението на КНМ за откриване на обекти включва няколко ключови стъпки, за да се гарантира, че моделът се научава да идентифицира точно и класифицира обекти в изображения [6]. Този процес обикновено започва с избора на подходяща КНМ архитектура, която може да включва добре познати модели като VGGNet, ResNet или YOLO. Тези архитектури използват конволюционни слоеве, които прилагат обучени

филтри към входните изображения, като ефективно улавят локални характеристики, които са от съществено значение за разпознаването на обект [4]. Фазата на обучение изисква етикетиран набор от данни, където изображенията са анотирани с ограничителни полета и етикети на класове, което позволява на КНМ да научи моделите, свързани с всеки обект. Чрез итеративно обучение моделът настройва своите параметри, за да минимизира класификационната грешка, като в крайна сметка постига високо ниво на точност при откриване и разпознаване на обекти в различни среди.

Оценяването на производителността на моделите за разпознаване на обекти е важна стъпка за гарантиране на тяхната ефективност в реални приложения[7]. Общите показатели за оценка включват прецизност, припомняне и F1 резултат, които заедно дават представа за точността и надеждността на модела. Освен това използването на матрици на объркване може да помогне за визуализиране на представянето на модела в различни класове, позволявайки по-добро разбиране на това къде моделът превъзхожда или се бори. Също така е важно да се извършват оценки както на набори от данни за обучение, така и на валидиране, за да се идентифицира всяко потенциално пренастройване. Чрез непрекъснато усъвършенстване на модела въз основа на оценки на производителността, разработчиците могат да подобрят възможностите за разпознаване на обекти на КНМ, което води до по-надеждни системи за AI видеокамери, способни да функционират ефективно в различни сценарии.

## 3 Приложения на КНМ във видеокамери с изкуствен интелект

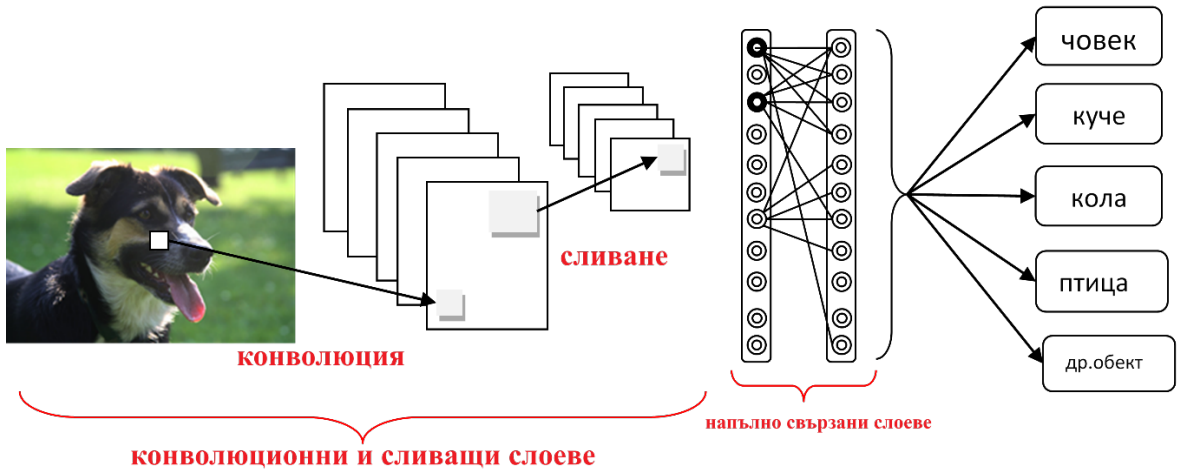
КНМ също напредват в интелигентните домашни устройства, особено в подобряването на сигурността и автоматизацията [9]. Чрез включването на способности за разпознаване на обекти, тези устройства могат да идентифицират познати лица, да наблюдават необичайни дейности и да правят разлика между доброкачествени и заплашителни ситуации [7]. Например интелигентните охранителни камери, оборудвани с КНМ, могат да изпращат предупреждения до собствениците на жилища, когато открият непознати лица, като по този начин подобряват мерките за сигурност на дома. Освен това тези устройства могат да се интегрират с други интелигентни системи за автоматизиране на реакциите, като например заключване на врати или включване на светлини, когато бъдат открити определени обекти. Тази синергия между КНМ и технологията за интелигентен дом не само повишава сигурността, но също така допринася за по-удобна и ефективна жизнена среда.

Едно от най-въздействащите приложения обаче на конволюционните невронни мрежи (КНМ) е във видеокамерите с изкуствен интелект за откриването на обекти в реално време в системите за наблюдение [1]. Тези системи използват КНМ за анализиране на видео емисии и идентифициране на различни обекти, като хора, превозни средства и други съответни обекти, със забележителна точност и скорост (фиг. 1).

Архитектурата на КНМ е особено подходяща за обработка на визуални данни, позволявайки ефективно извличане и класифициране на характеристики [3]. Например захранваните с изкуствен интелект VIGI камери използват КНМ за филтриране на фалшиви аларми, причинени от нецелеви обекти като животни, листа и променливи светлинни условия [8] (фиг. 2). Тази възможност не само повишава надеждността на системите за наблюдение, но също така минимизира ненужните сигнали, рационализирайки операциите по сигурността.

Такива архитектури са особено ефективни за интегриране в роботизирани системи за охрана на големи по площ обекти със специфични географски и архитектурни особености

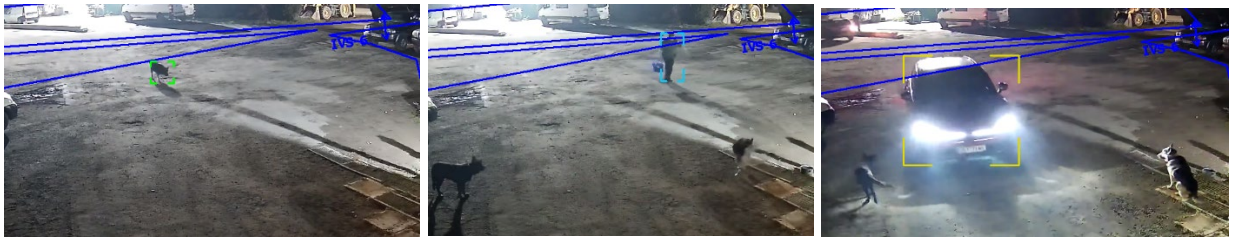
[12]. Обработката на огромни по обем данни и необходимостта от точна и бърза диагностика на евентуалните заплахи, прави почти задължително използването на камери за видеонаблюдение с внедрени конволюционни нервни мрежи. Традиционните техники за компютърно зрение разчитат на ръчно изработени функции и са ограничени в способността си да обобщават нови обекти или среди. Алгоритмите на КНМ, от друга страна, се учат от примери и подобряват своята точност с течение на времето. Друго предимство от използването на КНМ за разпознаване на обекти във видеокамери е способността им да се адаптират към променящите се условия. Тази гъвкавост е от решаващо значение там, където обектите могат да се появят по непредвидими начини. Разчитайки на богатата база данни, зададена при проектирането, видеокамерата се „научава“ да различава животни например и да не регистрира тяхното движение в зоната за охрана. На фиг. 3 е проследено развитието на една КНМ във видеокамера с AI в разпознаването на кучета. В началото мрежата регистрира кучето и го маркира в зелено, като в течение на самообучението игнорира кучетата и подава сигнали за автомобили ( в жълто ) и хора ( в синьо ), според зададените сценарии за охрана.




**Фиг. 1.** Архитектура на конволюционни невронни мрежи




**Фиг. 2.** Системи за видеоанализ



**Фиг. 3.** Развитие на КНМ при разпознаване на куче

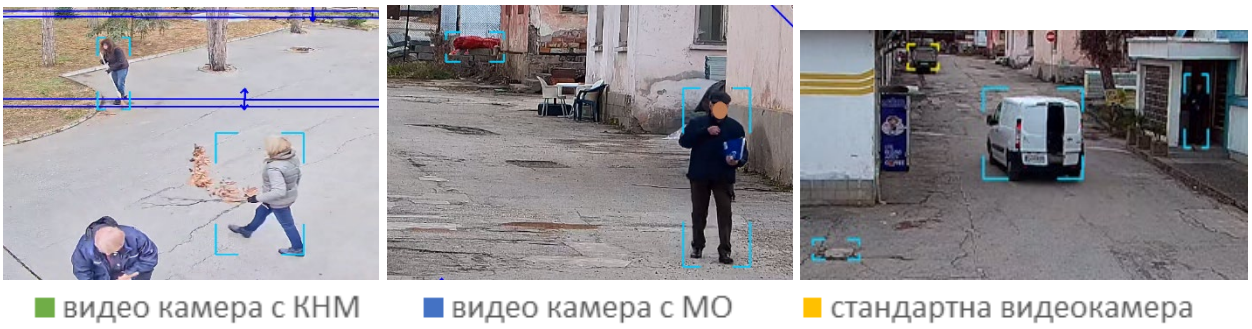
# 4 Резултати

Емпиричното изследване за целите на доклада е извършено чрез изследване и анализ на данни от роботизирана система за охрана с видеонаблюдение ТЕДИ [10]. Анализът се разпростира върху три вида видеокамери, които са поставени в еднакви условия на работа, като разликите на външните параметри като температура, осветеност и натовареност на движение са пренебрежимо малки и не оказват влияние на крайните резултати (Таблица 1).

**Таблица 1.** Данни от камерите за регистрирани аларми от хора

| 56 среден брой преминавания на хора на ден | Стандартни камери | | Камери с МО | | Камери с КНМ | |
|---|---|---|---|---|---|---|
| | бр.коректни сработвания | % ефективност | бр.коректни сработвания | % ефективност | бр.коректни сработвания | % ефективност |
| ден 1 | 28 | 50 | 22 | 40 | 28 | 50 |
| ден 2 | 28 | 50 | 25 | 45 | 31 | 55 |
| ден 3 | 29 | 52 | 24 | 42 | 36 | 65 |
| ден 4 | 31 | 55 | 25 | 45 | 37 | 66 |
| ден 5 | 34 | 60 | 28 | 50 | 45 | 81 |
| ден 6 | 35 | 63 | 29 | 51 | 48 | 85 |
| ден 7 | 37 | 66 | 31 | 55 | 48 | 86 |
| ден 8 | 38 | 67 | 31 | 56 | 50 | 90 |
| ден 9 | 38 | 68 | 31 | 55 | 52 | 92 |
| ден 10 | 40 | 72 | 34 | 60 | 53 | 95 |
| ден 11 | 39 | 70 | 34 | 61 | 55 | 98 |
| ден 12 | 39 | 70 | 33 | 59 | 54 | 96 |
| ден 13 | 41 | 74 | 34 | 60 | 53 | 95 |
| ден 14 | 42 | 75 | 32 | 58 | 55 | 98 |

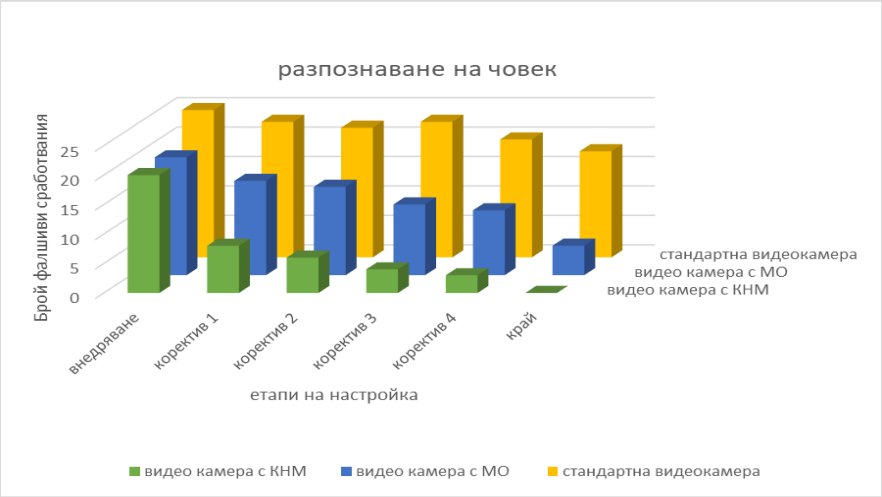
При стандартните видеокамери засичането на движение се извършва от алгоритми на базата на измененията в картината. Този метод използва алгоритъм, който засича движение, като сравнява текущата картина с предишната. Така, когато има значителни разлики в картината, камерата подава сигнал, че има движение. Въпреки, че този метод е ефективен за засичане на движение е видно, че води до лъжливи аларми при промени в осветлението (фиг. 4). Всеки различен обект в кадъра се анализира като човек (в синьо). Част от фалшивите сигнали могат да се избегнат чрез механична настройка на чувствителността на камерата.



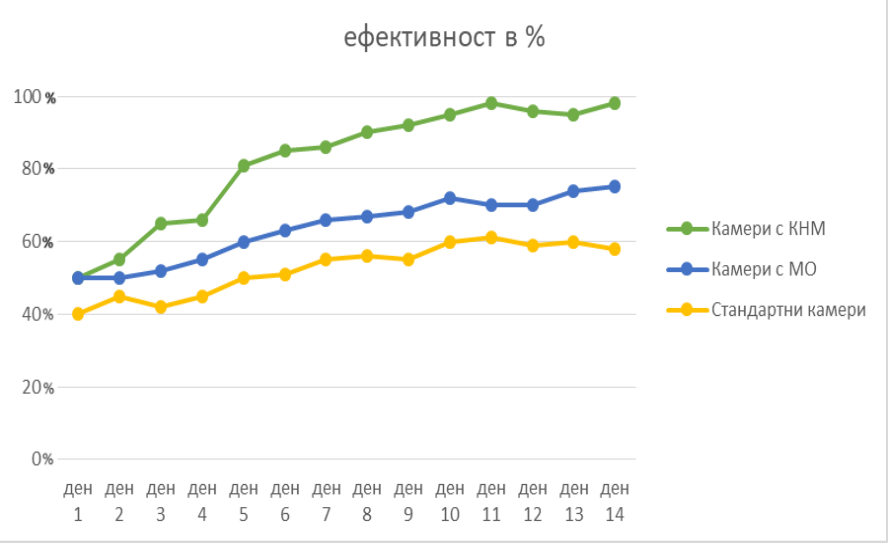

**Фиг. 4.** Действие на алгоритъм за разпознаване на хора

Значително по-добри резултати при реални условия се наблюдават при камерите с машинно обучение (МО). Алгоритмите за машинно обучение могат да бъдат обучени с помощта на големи набори от данни с етикетирани видео данни, което им позволява да се научат да разпознават модели и аномалии във видеозаписа. Чрез непрекъснато подобряване на тяхната производителност чрез обратна връзка от персонала по сигурността, тези алгоритми могат да станат много точни при идентифицирането(фиг. 5).

При най-модерните технологии за изкуствен интелект включително Deep Learning алгоритъм за задълбочен анализ, се осигурява по-голяма гъвкавост и точност при изпълнение на вградените в камерата интелигентни функции. Това дава възможност камерите да се използват за класификация на обекти при периметрова охрана, детекция на лица, метаданни, броене на хора, статистика на данните за трафика и др. Използваните конволюционни невронни мрежи в алгоритмите за изкуствен интелект подобряват значително точността и значително намаляват фалшивите аларми при периметровата охрана и увеличават ефективността на системата за наблюдение. Точността при засичане на хора достига 98% (фиг. 6).




**Фиг. 5.** Брой фалшиви сработвания при разпознаване на човек




**Фиг. 6.** Ефективност на видовете камери в %

# 5 Заключение

Приложението на конволюционните невронни мрежи (КНМ) в разпознаването на обекти представлява значителен напредък във възможностите на AI видеокамерите. Със своята структурирана архитектура, включваща конволюционни, обединяващи и напълно свързани слоеве, КНМ превъзхождат обработката на сложни данни за изображения, което ги прави безценни за различни задачи за разпознаване на обекти. Ефективни техники като предварителна обработка и увеличаване на данни, заедно със строго обучение и оценка, гарантират висока производителност и точност при откриване и класифициране на обекти. Практическите приложения на КНМ във видеокамерите с изкуствен интелект са неизброими, като подобряват системите за наблюдение в реално време, повишават безопасността на автомобилите и подобряват сигурността и автоматизацията в интелигентните домашни устройства. Тъй като технологията продължава да се развива, интегрирането на КНМ в решения за видеонаблюдение и сигурност вероятно ще нарасне, проправяйки пътя за по-интелигентни и по-безопасни среди.

**ЛИТЕРАТУРА:**


[1] Кърдев, В., Пасарелски, Р., Приложение на подходи на изкуствен интелект и машинно обучение в киберсигурността. Годишник Телекомуникации (2021), том 8, с. 53 – 64.

[2] Ламбова, Й., Ламбов, В., Изкуствените невронни мрежи–определение и приложение, Сборник с доклади от международна научна конференция „Отбранителни технологии“ DefTech (2021) Факултет по артилерия противовъздушна отбрана и комуникационни и информационни системи, ISSN 2367-7902.

[3] Христов, А., Нишева, М., Димов Д., Въведение в конволюционните невронни мрежи, София (2018).

[4] Драгиев, Б., Невронни мрежи – история, развитие и функционалност, (2018), Извлечено на 10.10.2024 от https://www.iphos.bg.

[5] WWW Интелигентни технологии за видеонаблюдение (2021), Извлечено на 10.10.2024г. от https://www.tech-dom.com/bg/inteligentni-tehnologii-za-videonablyudenie/2/2315/.

[6] Татарианц, М., AI Оценка на позата във фитнес приложението (2020), Извлечено на 10.10.2024г. от www.unite.ai/bg/ai-pose-estimation-in-fitness-application/.

[7] Biswal, A., Convolutional Neural Network Tutorial (2024), Извлечено на 20.10.2024 от https://www.simplilearn.com/tutorials/deep-learning-tutorial/convolutional-neural-network.

[8] VIGI AI Разпознаване.www.tp-link.com/bg/technology/vigi-ai/, Извлечено на 20.10.2024.

[9] Цанов, И., Изкуственият интелект в контекста на управлението и сигурността, София е-книга (2022).

[10] Denev, D., Tsankov, Ts. Progress and trends in machine vision smart cameras. Scientific Conference with international participation MATTEH 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 116-124.

[11] Konstantinova, E., Tsankov, Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference “Ecology and environment”, 2021, ISSN 2367-5209, pp. 109-121.

[12] Nikolova S. Design, development and research of process efficiency in a robotic intelligent security system “TEDI”. KNOWLEDGE – International Journal Scientific Papers, Vol. 63.3, Institute of Knowledge Management, Skopje, (2024), ISSN 2545-4439, pp. 289-295.

# ADVANTAGES AND DISADVANTAGES OF THE ALGORITHM BERNOULLI NAIVE BAYES CLASSIFIER*

**NELI A. ARABADZHIEVA-KALCHEVA, GINKA K. MARINOVA, MAYA P. TODOROVA**

***ABSTRACT:*** *The report examines the widely used Bernoulli Naive Bayes classifier, focusing on its characteristics, strengths, and weaknesses. Studies indicate that this classifier is not a universal classification method capable of guaranteeing 100% accuracy across all application tasks.*

***KEYWORDS:*** *Bernoulli Naive Bayes Classifier, text classification, machine learning*

***DOI: https://doi.org/10.46687/NFKV8841***

# ПРЕДИМСТВА И НЕДОСТАТЪЦИ НА АЛГОРИТЪМА БЕРНУЛИЕВ НАИВЕН БЕЙСОВ КЛАСИФИКАТОР

**НЕЛИ А. АРАБАДЖИЕВА-КАЛЧЕВА, ГИНКА К. МАРИНОВА, МАЯ П. ТОДОРОВА**

***АБСТРАКТ:*** *В доклада е разгледан широко използваният алгоритъм Бернулиев Наивен Бейсов класификатор, като се акцентира върху неговите характеристики, силни и слаби страни. Проучванията сочат, че този класификатор не представлява универсален метод за класификация, който да гарантира 100% точност във всички приложни задачи.*

## 1 Въведение

Класификацията е процес, при който обекти, явления или процеси се разпределят в групи въз основа на определени съществени характеристики, като се подреждат в определен ред, отразяващ степента на тяхното сходство.

Основната цел на класификацията е да се определи принадлежността на даден обект към предварително зададен клас, използвайки набор от характеристики като цена, тегло, качество, размери, количество и други. Тези характеристики, които играят ключова роля в класификацията, се наричат предиктори. За решаването на класификационна задача е необходимо да се създаде алгоритъм, който изгражда обобщен модел, способен еднозначно да свързва стойностите на предикторите с класа, към който принадлежи обектът..

## 2 Алгоритъм Наивен Бейсов класификатор

Един от утвърдените алгоритми в машинното обучение е Наивният Бейсов класификатор, който използва теоремата на Бейс за изчисляване на апостериорната вероятност за настъпване на определено събитие. Благодарение на „наивното“ предположение за условна независимост между всички двойки атрибути, този класификатор успешно се справя с големия брой атрибути, описващи един пример, което го прави подходящ за преодоляване на така нареченото „проклятие на размерността“.

Теорема на Бейс (1) [1, 2, 3, 4, 5, 6 ]

$$P(y = c|x) = \frac{P(x|y=c)P(y=c)}{P(x)} \quad (1)$$

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

където: P(y=c|x) е вероятността обект да принадлежи на клас c (апостериорна вероятност на класа)
P(x|y=c) – вероятността обекта x да среща в средата на обекта на класа *c*
P(y=c) – безусловна вероятност да се среща обект y в клас *c* (априорна вероятност на класа)
P(x) – безусловна вероятност на обекта x
Целта на класификацията се състои в това, да се определи към какъв клас принадлежи обекта x. Следователно е необходимо да се намери вероятностен клас на обекта x, т.е. необходимо е от всички класове да се избере този, който дава максимална вероятност P(y=c|x).

$$c_{opt} = \arg\max_{c \in C} P(x|y=c)P(y=c) \quad (2)$$

Известни алгоритми от типа Наивен Бейсов класификатор са: Гаусов, Бернулиев и Мултиномиален, свързани с различни предположения за разпределението на признаците.

# 3 Алгоритъм Бернулиев Наивен Бейсов класификатор

Бернулиевият Наивен Бейсов класификатор [1, 2, 3, 4, 5, 6] представя документа като бинарен вектор на пространството, който може да се разгледа като точка в пространството от думи. Стойност единица показва дали думата се появява поне веднъж в документа, а стойност нула кореспондира липса на същата дума. По такъв начин се разглеждат случаите на присъствие или отсъствие на дума в текста, без да се отчита колко пъти се повтаря дадена дума. С такова представяне, се прави наивното предположение на Бейс, че вероятността всяка дума да се среща в текста е независима от появата на други думи.

При създаден речник $V = \{w_t\}_{t=1}^{|V|}$ съдържащ множество от думи с размер $|V|$, $t$–тото измерение на бинарния вектор на пространството, представляващ документ, където $t \in \{1,2,...,|V|\}$ съответства на думата $w_t$ в речника [2, 6].

Ако $b_i$ е вектор от характеристики за $i$-я документ $D_i$, тогава $t$–я елемент записан като $b_{it}$ е 0 или 1, представляващ отсъствие или присъствие на думата в документа.

Нека условната вероятност $P(w_t|C)$ е вероятността да се среща в документа, при условие, че е дефиниран клас C. Тогава вероятността думата $w_t$ да не се среща в документа се представя като: $1 - P(w_t|C)$. Ако се направи наивното Бейсово предположение, че вероятността за поява на всяка дума е независима от появата на коя да е друга дума, условната вероятност на документа $P(D_i|C)$ може да се представи в зависимост от условната вероятност на думата $P(w_t|C)$.

$$P(D_i|C) \sim P(b_i|C) = \prod_{t=1}^{|V|}[b_{it}\,P(w_t|C) + (1 - b_{it})(1 - P(w_t|C))] \quad (3)$$

Тази формула се прилага за всички думи в речника. Ако думата $w_t$ е налична в документ, тогава $b_{it}=1$ и вероятността е $P(w_t|C)$. Ако думата липсва, тогава $b_{it}=0$ и вероятността е $1 - P(w_t|C)$.

На практика някои думи могат да не присъстват в даден клас обучаващи данни. Тогава стойностите на вероятностите ще имат нулеви значения. Сложността възниква когато се умножават нулевите стойности във формула (3). В този случай целият израз се нулира и се изгубва информация. За да се избегне получаването на нулеви вероятности се използва Лапласово изглаждане, което се заключава в добавяне на единица в числителя [7] (4).

$$P(w_t|C_k) = \frac{1+\sum_{t=1}^{|V|} b_{it}P(C_k|d_i)}{2+\sum_{t=1}^{|V|} b_{it}P(C_k|d_i)} \quad (4)$$

Параметрите на вероятностите са вероятностите на всяка дума, която се среща в документа, в случай, че е дефиниран клас *C*.

**Предимства:**

- подходящ за йерархична класификация, когато данните за обучението са подредени в таксономия по теми [8];
- работи ефективно с много малък брой функции [8];
- подходящ е при кратки текстове и при малки размери на речника [8, 2, 6];
- особената му сила е неговата ефективност, като при едно обхождане на данните връща приемлив резултат [9];
- надежден, дори при наличие на шум [9];
- изисква малко количество данни за обучение, за да се изчислят необходимите параметри за класифициране [10];
- алгоритъма е изчистен, защитен от напасване [3].

**Недостатъци:**

- не е подходящ за големи размери на речника [6, 8, 9];
- представя се много слабо, когато функциите са силно корелирани [10];
- допускането за независимост на признаците едни от други [9, 10].

# 4 Заключение

Бернулиевият Наивен Бейсов класификатор е ефективен инструмент за текстова класификация, особено в случаи на кратки текстове и малки размери на речника. Неговата сила се крие в способността му да работи с малко количество обучаващи данни и в простотата на алгоритъма, което го прави лесен за внедряване и устойчив на пренапасване. Въпреки това, класификаторът има някои ограничения, като основното е, че не отчита смисловите взаимоотношения между думите и прави предположението за независимост на признаците, което може да не отразява реалността в случаите на силно корелирани атрибути.

Изследванията показват, че макар и полезен за определени задачи, Бернулиевият Наивен Бейсов класификатор не представлява универсален метод, който да гарантира 100% точност във всяка приложна ситуация. Въпреки това, неговата ефективност при обработка на специфични видове данни, като йерархично подредени или кратки текстове, го прави ценен инструмент за класификация в конкретни приложения.

**ЛИТЕРАТУРА:**

[1] Kalcheva N., M. Todorova, G. Marinova, Naive Bayes Classifier, Decision Tree and AdaBoost Ensemble Algorithm. Advantages and disadvantages, 6th International Conference – ERAZ 2020 – Knowledge based sustainable development, Online/virtual, May 21, 2020, Published by: Association of Economists and Managers of the Balkans – Belgrade, Serbia https://doi.org/10.31410/ERAZ.2020.153 (doi: 10.31410/ERAZ.2020.153)

[2] McCallum, A., K. Nigam. A comparison of event models for Naive Bayes text classification. Papers from the 1998 AAAI Workshop, 1998, pp. 41-48Atanassov, K. Theory of Generalized nets (a topological aspect), Methods of Operation Research, 51, 1984, 217-226

[3] Murphy, K. Machine learning a probabilistic perspective. The MIT Press Cambridgr, 2012.

[4] Raschka, S. Naive Bayes and text classification I - Introduction and theory. Cornell University library, Ithaca, 2014.

[5] Sayfullin, L., E. Eirolay, D. Komashinskyz, P. Palumboz, Y. Miche, A. Lendassex, J. Karhunen. Improved Naive Bayes classifier for android malware classification. The Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2015.

[6] Shimodaira, H. Text classification using Naive Bayes. Learning and Data Note 7, 2014, pp. 1-9.

[7] Юсупова, Н., Д. Богданова, М. Бойко. Алгоритмическое и программное обеспечение для анализа тональности текстовых сообщений с использованием машинного обучения. Вестник Уфимского государственного авиационного технического университета 16, no. 6, 2012.

[8] Aggarwal, C., Z. ChengXiang. Mining Text Data, Springer, 2012.

[9] Manning, C., P. Raghavan, H. Schütze. Introduction to Information Retrieval. Cambridge University Press, 2008.

[10] Khan, A., B. Baharudin, L. Lee, K. Khan. A review of machine learning algorithms for text-documents classification. Journal of Advances Information Technology, vol. 1, 2010, pp. 4-20.

# APPLICATION OF FAILURE MODE AND EFFECTS ANALYSIS FOR EVALUATING HUMAN RELIABILITY*

**NELI A. ARABADZHIEVA-KALCHEVA, TSVETOSLAV S. TSANKOV, MAYA P. TODOROVA, GINKA K. MARINOVA**

***ABSTRACT:*** *The Human Reliability Assessment (HRA) and Failure Mode and Effects Analysis (FMEA) examine the impact of human errors and technical failures on the operation of complex systems. These approaches utilize qualitative and quantitative methods to identify potential risks, assess their impact, and develop strategies to minimize them. The application of HRA and FMEA is particularly valuable in the fields of computer science and cybersecurity, where the reliability and protection of systems depend on the interaction between humans and technologies.*

***KEYWORDS:*** *Human Reliability Assessment, HRA, Failure Mode and Effects Analysis, FMEA, risk management, risk assessment, risk analysis, risk assessment methods*

***DOI: https://doi.org/10.46687/BOIK9859***

# ПРИЛОЖЕНИЕ НА АНАЛИЗА НА ВИДОВЕТЕ ОТКАЗИ И ПОСЛЕДСТВИЯТА ОТ ТЯХ ЗА ОЦЕНКА НА НАДЕЖДНОСТТА НА ЧОВЕШКИЯ ФАКТОР

**НЕЛИ А. АРАБАДЖИЕВА-КАЛЧЕВА, ЦВЕТОСЛАВ С. ЦАНКОВ, МАЯ П. ТОДОРОВА, ГИНКА К. МАРИНОВА**

***АБСТРАКТ:*** *Анализът на надеждността на човешкия фактор (HRA - Human Reliability Assessment) и Анализът на видовете откази и последствията от тях (FMEA - Failure Mode and Effects Analysis) изследват влиянието на човешките грешки и техническите откази върху функционирането на сложни системи. Тези подходи използват качествени и количествени методи за идентифициране на потенциални рискове, оценка на тяхното въздействие и разработване на стратегии за минимизиране на риска. Прилагането на HRA и FMEA е особено полезно в областта на компютърните науки и киберсигурността, където надеждността и защитата на системите зависят от взаимодействието между човека и технологиите.*

## 1 Въведение

Процесът на управление на риска представлява комплекс от взаимосвързани дейности, включващи обмен на информация, консултиране, дефиниране на контекста, оценка, въздействие, наблюдение и преглед на риска. Той осигурява структура за ефективно управление на несигурностите, които могат да повлияят на постигането на целите.

Оценката на риска е основен компонент на управлението на сигурността и се разглежда като поредица от стъпки за идентифициране, анализ и оценяване на риска, свързан с даден проект или дейност.

Стандарт 31010 [1] представя набор от методи за управление на риска, с подробни препратки към други международни стандарти, които описват концепциите и приложението на тези методи в по-голяма дълбочина. Един от включените методи е Анализ

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

на надеждността на човешкия фактор, който играе важна роля при оценката и управлението на риска, свързан с човешките действия, както и методът Анализ на видовете откази и последствията от тях, който предоставя структурирана рамка за идентифициране и оценка на технически и човешки откази.

## 2 Анализ на надеждността на човешкия фактор

Анализът на надеждността на човешкия фактор [1] (Human Reliability Assessment – HRA) е основен инструмент за разбиране и управление на човешките грешки в различни системи. Човешкият фактор играе съществена роля в безопасността и ефективността на сложни технически и организационни системи, като например енергетиката, авиацията, медицината и производството. Изследванията показват, че HRA не само идентифицира грешките, но и осигурява основа за приоритизиране на обучения и разработване на стратегии за намаляване на риска чрез анализ на критични събития [2]. Проучването на надеждността на човешкия фактор изследва взаимодействията между хората и технологиите, за да идентифицира рисковете, свързани с човешките грешки, и да предложи стратегии за тяхното намаляване.

Човешките грешки могат да бъдат резултат от недостатъчно време за вземане на решения, прекомерна умора, липса на обучение или други психологически и организационни фактори. Например, в ситуации с високо ниво на стрес, когато операторът има ограничено време за реакция, вероятността за грешки значително нараства. В контекста на сложни технологични системи като енергийните, анализът на потенциалните човешки грешки се комбинира с подходи като FMEA, които позволяват количествено определяне на рисковете и оптимизиране на реакциите към грешки [3]. От друга страна, в определени случаи човешките действия могат да бъдат единственият механизъм за предотвратяване на по-сериозни аварии. Това подчертава значимостта на комбинирания подход, който интегрира HRA и FMEA за по-добро управление на рисковете в технологично сложни среди [4]. Анализът на надеждността на човешкия фактор предоставя рамка за анализ както на качествено, така и на количествено ниво. Качественият анализ се фокусира върху идентифициране на възможностите за човешки грешки и техните причини. Той включва изследване на задачите, които трябва да се изпълнят, видовете грешки, които могат да възникнат, и начините за тяхното предотвратяване. Количественият анализ, от друга страна, изчислява вероятностите за възникване на грешки и предоставя данни за по-задълбочен анализ на риска или интеграция в модели за откази. И двата подхода са взаимно допълващи се и осигуряват по-цялостен поглед върху рисковете, свързани с човешките действия.

Анализът на надеждността на човешкия фактор разчита на специфични входни данни, които включват описание на задачите, които трябва да бъдат изпълнявани от хората, историческа информация за видовете грешки, наблюдавани в практиката, както и знания и опит в областта на човешките грешки и тяхната количествена оценка. Изходните данни от анализа обикновено включват списък с потенциални грешки и методи за тяхното предотвратяване, както и оценка на риска, свързан с тези грешки. Тези резултати често се използват за оптимизиране на системния дизайн с цел минимизиране на вероятността за грешки.

Въпреки своите предимства, Анализът на надеждността на човешкия фактор има и някои ограничения. Сложността и разнообразието на човешкото поведение затрудняват моделирането на всички възможни сценарии. Много дейности не могат да бъдат сведени до прости бинарни състояния „успех/провал“, което усложнява анализа на частични грешки

или некачествени решения. Освен това количествената оценка на риска често изисква значителни ресурси и време. Въпреки тези предизвикателства, Анализът на надеждността на човешкия фактор осигурява ценен принос за управлението на сложни системи, като предлага структурирани механизми за анализ и минимизиране на човешките грешки.

Анализът на надеждността на човешкия фактор (Human Reliability Assessment – HRA) е основен инструмент за разбиране и управление на човешките грешки в различни системи. Човешкият фактор играе съществена роля в безопасността и ефективността на сложни технически и организационни системи, като например енергетиката, авиацията, медицината и производството. Проучването на надеждността на човешкия фактор изследва взаимодействията между хората и технологиите, за да идентифицира рисковете, свързани с човешките грешки, и да предложи стратегии за тяхното намаляване.

Човешките грешки могат да бъдат резултат от недостатъчно време за вземане на решения, прекомерна умора, липса на обучение или други психологически и организационни фактори. Например, в ситуации с високо ниво на стрес, когато операторът има ограничено време за реакция, вероятността за грешки значително нараства. От друга страна, в определени случаи човешките действия могат да бъдат единственият механизъм за предотвратяване на по-сериозни аварии. Значимостта на оценката на надеждността на човешкия фактор често се подчертава от исторически примери, при които грешките на операторите са довели до катастрофални събития. Тези примери демонстрират опасността от съсредоточаване единствено върху техническите аспекти на риска и необходимостта от интегриране на човешкия фактор в процесите на управление на риска.

Анализът на надеждността на човешкия фактор предоставя рамка за анализ както на качествено, така и на количествено ниво. Качественият анализ се фокусира върху идентифициране на възможностите за човешки грешки и техните причини. Той включва изследване на задачите, които трябва да се изпълнят, видовете грешки, които могат да възникнат, и начините за тяхното предотвратяване. Количественият анализ, от друга страна, изчислява вероятностите за възникване на грешки и предоставя данни за по-задълбочен анализ на риска или интеграция в модели за откази. И двата подхода са взаимно допълващи се и осигуряват по-цялостен поглед върху рисковете, свързани с човешките действия.

За да бъде анализът ефективен, процесът на оценка на надеждността на човешкия фактор следва структурирана последователност от стъпки. Първата стъпка е идентифицирането на проблема, което включва определяне на аспектите на човешкото поведение, които трябва да бъдат оценени. Това означава дефиниране на специфични задачи или дейности, където човешките грешки могат да окажат влияние върху надеждността на системата, както и установяване на контекста и условията на работа (например, стрес, време за реакция, обучение).

След това се извършва анализ на задачите, който разглежда конкретните действия, които трябва да се изпълнят, и техните взаимодействия със системата. Чрез техники като Task Analysis се изучават последователността от действия и необходимите ресурси и инструменти за тяхното изпълнение. На този етап се изяснява какви помощни средства са необходими за подпомагане на процеса.

Следващата важна стъпка е анализът на грешките, при който се идентифицират възможните грешки и техните последствия. Тези грешки могат да включват пропуски в изпълнението на задачите, неправилно изпълнение или липса на действия. За категоризация

на грешките често се използват методологии като Human Error Identification (HEI) или Human Error Analysis (HEA).

Количествената оценка е следващият етап, където грешките се анализират с помощта на количествени подходи. Това включва методологии като FMEA (Failure Mode and Effects Analysis), HEART (Human Error Assessment and Reduction Technique) и THERP (Technique for Human Error Rate Prediction). Например, FMEA позволява оценка на грешките въз основа на тежест (S), вероятност за поява (O) и вероятност за разкриване (D), като рискът се изчислява чрез индекса RPN (Risk Priority Number).

На етапа на скрининг се определя кои задачи или грешки изискват детайлен количествен анализ и кои могат да бъдат разгледани на по-високо ниво. Това позволява ефективно разпределение на ресурсите.

Ключов етап в процеса е намаляването на грешките, което включва разработване на стратегии за минимизиране на риска. Това може да бъде осъществено чрез обучение на персонала, подобряване на интерфейсите или внедряване на защитни механизми като автоматични системи за предупреждение.

Накрая, всички стъпки се документират в детайли, за да се осигури база за бъдещи анализи и актуализации. Документацията включва идентифицираните рискове, използваните методологии и предложените мерки за намаляване на грешките. Този структуриран подход гарантира прозрачност и проследимост на анализа.

Анализът на надеждността на човешкия фактор разчита на специфични входни данни, които включват описание на задачите, историческа информация за грешките и експертни знания. Изходните данни от анализа предоставят списък с потенциални грешки и методи за тяхното предотвратяване, което често се използва за оптимизиране на системния дизайн. Въпреки своите предимства, анализът има и някои ограничения, свързани със сложността и разнообразието на човешкото поведение, както и с необходимостта от значителни ресурси за количествена оценка. Независимо от тези предизвикателства, HRA остава ценен инструмент за управление на човешките грешки в сложни системи.

## 3 Приложение на FMEA за оценка на надеждността на човешкия фактор

Процесът на анализ на надеждността на човешкия фактор може да бъде разширен чрез приложението на Анализ на видовете откази и последствията от тях (FMEA (Failure Mode and Effects Analysis)), което предоставя структурирана методология за идентифициране, оценка и минимизиране на рисковете, свързани с човешките грешки. FMEA е един от първите методи за изследване на риска, разработен през петдесетте години на миналия век с цел разрешаване на проблеми, възникнали във военни съоръжения [5]. Първоначално създаден за системни инженери, този метод изследва потенциални повреди в продукти или процеси и служи за оценка на приоритетите при управление на риска, за да се смекчат известни уязвимости. Прилагането на FMEA позволява ранно идентифициране на потенциални източници на грешки и техните последствия върху качествените характеристики на системата, с цел минимизиране на рисковете и подобряване на надеждността [6].

За да се приложи ефективно този подход, е необходимо първо да се дефинират ключовите процеси и задачи, които ще бъдат анализирани. В тази стъпка се идентифицират критичните взаимодействия на човека със системата, като например контролни действия,

вземане на решения или въвеждане на данни. Това включва конкретни примери, като работа на оператор с контролен интерфейс или реакции при вземане на решения в критични ситуации. За да се приложи ефективно този подход, е необходимо първо да се дефинират ключовите процеси и задачи, които ще бъдат анализирани. В тази стъпка се идентифицират критичните взаимодействия на човека със системата, като например контролни действия, вземане на решения или въвеждане на данни. Това включва конкретни примери, като работа на оператор с контролен интерфейс или реакции при вземане на решения в критични ситуации.

Следващата стъпка включва идентификация на потенциалните грешки, като се описват възможните сценарии, при които грешките могат да възникнат. Това може да включва неправилно въвеждане на данни, забавена реакция или пропускане на важна информация. Тези идентифицирани грешки са основата за последващата оценка на риска, която изисква количествено измерване на три ключови параметъра: тежест (S), вероятност за поява (O) и вероятност за разкриване (D). Тежестта оценява степента на въздействие на грешката върху системата, вероятността за поява измерва шанса грешката да се случи, а вероятността за разкриване определя колко вероятно е грешката да бъде засечена преди да доведе до отказ. Всички тези параметри се комбинират чрез формулата RPN=S×O×D, която изчислява приоритетния индекс на риска (Risk Priority Number). На база на получените стойности рисковете могат да бъдат класифицирани като ниски, средни или високи, което позволява тяхното приоритизиране.

Въз основа на анализа се разработват действия за намаляване на риска, които могат да включват подобрения в интерфейса, провеждане на допълнителни обучения за персонала или добавяне на предупредителни сигнали и автоматизирани проверки. Например, ако вероятността за грешка е висока поради липса на обучение, може да бъде предложено организиране на специализирани тренировки за служителите. Важна част от процеса е документацията на анализа, която изисква подробно записване на всички идентифицирани грешки, техните параметри и предложените мерки. Тази структурирана документация е ценен ресурс за бъдещи анализи и актуализации, осигуряващи прозрачност и последователност в управлението на рисковете, свързани с човешкия фактор.

Интеграцията на FMEA в анализа на надеждността на човешкия фактор позволява по-цялостен и систематичен подход към управлението на човешките грешки, като осигурява ясна рамка за идентифициране, оценка и минимизиране на рисковете. Това прави методологията изключително подходяща за сложни системи, в които взаимодействието между човека и технологията играе ключова роля за ефективността и безопасността.

FMEA (Failure Mode and Effects Analysis) е методология, която може ефективно да се прилага за оценка на надеждността на човешкия фактор в различни контексти и ситуации. Методът позволява систематично идентифициране на потенциални човешки грешки, анализ на техните причини и последствия, както и разработване на подходящи мерки за намаляване на риска. FMEA осигурява рамка за структурирано анализиране, като комбинира количествени и качествени подходи за оценка на риска.

Тази методология може да бъде използвана за различни примери, като проектирането на нови системи, оптимизация на работни процеси или въвеждането на нови технологии. В такива случаи е полезно да се използва стандартна таблица за документиране и анализ на идентифицираните рискове. Пример за такава таблица е следният формат:

| **Задача**: Анализ на рисковете, свързани с надеждността на човешкия фактор | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Изготвил: …** | | | | | | | |
| **№** | **Описание на риска** | **Тежест (S)** | **Вероятност за поява (O)** | **Вероятност за разкриване (D)** | **RPN = S * O * D** | **Ниво на риска** | **Възможни действия** |
| **1.** | | | | | | | |
| **…** | … | … | … | … | … | … | … |

# 4 Заключение

Анализът на надеждността на човешкия фактор (HRA) и Анализът на видовете откази и последствията от тях (FMEA) са два допълващи се методи за управление на риска в сложни системи. HRA позволява задълбочено разбиране на човешките грешки и тяхното въздействие върху системата, докато FMEA осигурява структурирана рамка за идентифициране и оценка на техническите и човешките откази. Комбинираното им приложение предоставя цялостен подход за повишаване на надеждността и сигурността, като подпомага оптимизирането на процесите и минимизирането на рисковете. Тези методи са особено ценни в области, където взаимодействието между човека и технологиите е критично за успеха на системата.

**ЛИТЕРАТУРА:**

[1] БДС EN ISO 31010, Управление на риска. Методи на оценяване на риска, https://www.bds-bg.org/.

[2] Aalipour, M., Human reliability assessment in the process industry, Journal of Loss Prevention in the Process Industries, Elsevier, vol. 41, pp. 76–84, 2016.

[3] Dhillon, B. S., Human reliability and error in transportation systems, Springer, 2006.

[4] Boring, R. L., Gertman, D. I., Integrating human reliability analysis with probabilistic safety assessment, Reliability Engineering & System Safety, Elsevier, vol. 92, no. 12, pp. 1764–1772, 2007.

[5] Reddy, V., Gangadharappa, H. V. Vijayakumar, Shashikanth, D., Risk assessment by using failure mode effective analysis (FMEA) tool: an overview, World Journal of Pharmaceutical Research, vol. 4, no. 3, pp. 567–574, 2015.

[6] Carlson, C., Understanding and Applying the Fundamentals of FMEAs, Tucson, Arizona: Annual RELIABILITY and MAINTAINABILITY Symposium, 2014.

# THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND ITS APPLICATIONS IN THE MODERN WORLD*

**EMILI K. DIMITROVA, DANIEL R. DENEV**

***ABSTRACT:*** *This article discusses artificial intelligence, one of the most rapidly developing technologies, which has a significant impact on the transformation of various industries. The development of artificial intelligence will be explored – from its initial concepts to its current advancements. The ways in which artificial intelligence is transforming key sectors such as healthcare, transportation, finance, and education, as well as its impact on people's daily lives, will be examined. In addition to its benefits, ethical issues and data privacy concerns will also be discussed. The article presents the main advantages and potential risks of using artificial intelligence, as well as its future development in this field.*

***KEYWORDS:*** *artificial intelligence, ethical issues, data privacy*

***DOI: https://doi.org/10.46687/ZPLN4390***

# РАЗВИТИЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ И ПРИЛОЖЕНИЯТА МУ В СЪВРЕМЕННИЯ СВЯТ

**ЕМИЛИ К. ДИМИТРОВА, ДАНИЕЛ Р. ДЕНЕВ**

***АБСТРАКТ:*** *В настоящия доклад се разглежда изкуственият интелект, който е един от най-динамично развиващата се технология и има значителен принос за трансформацията на различни индустрии. Ще се разгледа развитието на изкуствения интелект – от първоначалните му концепции до съвременното му развитие. Начина по, който изкуствения интелект преобразува ключови сектори като: здравеопазване, транспорт, финанси, образование и неговото въздействие върху ежедневието на хората. Освен ползи се разглеждат и етичните въпроси и защита на личните да данни. Представят се основните предимства и възможни рискове от ползването на изкуствен интелект и бъдещето развитие в тази сфера.*

## 1 Въведение

Изкуственият интелект се определя като способността на машините да изпълняват задачи, които традиционно изискват човешка интелигентност, като разпознаване на модели, решаване на проблеми, учене и разбиране на езика. Първоначално смятан за слаба академична дисциплина изкуствения интелект се превърна в двигател на икономическото развитие и иновации. Основните въпроси, които се разглеждат, са как технологиите на изкуствения интелект се развиват, как се прилагат в реалния свят и какви са етичните и социалните аспекти на тяхното използване. Концепцията за създаване на „мислещи машини“ е дълбоко вкоренена в човешката история, започвайки още от античните митове за автоматони и преминавайки през визиите на мислители като Лайбниц, Декарт и Тюринг.

Терминът "изкуствен интелект" е въведен през 1956 г. на конференцията в Дартмут, където изследователи като Джон Маккарти, Марвин Мински и Алън Нюел формулират амбицията за създаване на машини, които могат да мислят и учат като хората. Макар началните опити да са били ограничени от липсата на изчислителни ресурси и данни, ИИ

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“

успя да премине през няколко значими етапа на развитие, водени от нововъведения в алгоритмите и хардуера. [3, 4]




**Фиг. 1.** *Технологията изкуствен интелект* [4]

## 2 Етапи на развитие на изкуствения интелект

- Ранни изследвания (1950–1970 г.)

Ранната история на ИИ започва с визионерски идеи на мислители като Алън Тюринг, който въвежда концепцията за машинно мислене чрез своя знаменит тест за изкуствен интелект. През този период се създават първите компютърни програми, които могат да решават прости математически и логически задачи. Един от най-забележителните примери е програмата Logic Theorist, разработена през 1956 г., която е способна да доказва математически теореми. През този етап ограниченията в изчислителната мощ и липсата на достатъчно данни възпрепятстват значителния напредък, но полагат основите на бъдещото развитие.

- Ерата на експертните системи (1970–1990 г.)

Експертните системи представляват първия мащабен опит за практическо приложение на ИИ. Те използват набор от правила, базирани на знанията на човешки експерти, за решаване на специфични задачи. Примери включват системите MYCIN за диагностика в медицината и DENDRAL за анализ на химически съединения. Въпреки успехите, тези системи страдат от редица ограничения, включително липса на гъвкавост и невъзможност за самообучение, което ограничава тяхната универсалност.

- Машинно обучение и големи данни (1990–2010 г.)

С нарастването на мощността на компютрите и наличието на големи обеми от данни, подходите за машинно обучение заменят традиционните експертни системи. Алгоритмите започват да използват статистически модели за идентифициране на закономерности в данните. През този период се развиват методи като поддръжка на векторни машини и решаващи дървета, които намират приложение в области като финансови прогнози и обработка на изображения.

- Дълбоко обучение и съвременен ИИ (2010 г. – до днес)

Дълбокото обучение, базирано на многослойни невронни мрежи, доведе до значителни пробиви. Системи като AlphaGo на Google DeepMind показаха, че машините могат да надминат човека в сложни игри като Го. Невронните мрежи също така направиха възможни приложения като разпознаване на лица, автоматизирано превеждане и автономни автомобили. [3]




**Фиг. 2.** *Развитието на изкуствения интелект по години*

## 3 Основни технологии на изкуствения интелект

Основни технологии на изкуствения интелект са:

***Машинно обучение***

Машинното обучение включва алгоритми, които позволяват на системите да учат и подобряват своето представяне, без да бъдат програмирани изрично за всяка задача. Съществуват три основни вида машинно обучение:

- Надзиравано обучение: Алгоритъмът се обучава върху предварително етикетирани данни.
- Ненадзиравано обучение: Системата анализира неизследвани данни, за да открие скрити модели.
- Подсилващо обучение: Машината се обучава чрез опит и грешка, като получава награди за правилни действия.

***Дълбоко обучение***

Дълбокото обучение използва сложни невронни мрежи с множество слоеве за откриване на високоструктурни закономерности в данните. Това е основната технология зад модерните системи за разпознаване на глас и изображения.

***Обработка на естествен език (NLP)***

NLP позволява на машините да разбират и генерират човешки език. Приложенията включват чатботове, преводачи и системи за автоматизиран анализ на текстове. Популярни модели като GPT (Generative Pre-trained Transformer) значително подобриха качеството на тези системи.

***Компютърно зрение***

Компютърното зрение се фокусира върху анализ и интерпретация на визуални данни. То намира приложение в медицинската диагностика (например разпознаване на заболявания), системи за сигурност и автономни превозни средства.

***Роботика***

Роботиката комбинира изкуствения интелект с механични системи, за да създаде машини, които могат да изпълняват сложни физически задачи. Примери включват индустриални роботи, дронове и хуманоидни роботи като ASIMO.

# 4 Приложения на изкуствения интелект в съвременния свят

***Здравеопазване***

Изкуствения интелект революционизира медицината чрез:

- Диагностика: Системи като IBM Watson анализират медицински изображения и история на пациенти, за да предложат точни диагнози.
- Роботизирана хирургия: Роботите, като da Vinci, извършват сложни операции с висока прецизност.
- Персонализирана медицина: Изкуствения интелект анализира генетична информация за индивидуално лечение.

***Транспорт***

Автономните превозни средства използват ИИ за разпознаване на околната среда и вземане на решения в реално време. Системи за управление на трафика оптимизират маршрути и намаляват задръстванията.

***Финанси***

Изкуствения интелект се използва за:

- Откриване на измами: Анализиране на транзакции за идентифициране на подозрителна активност.
- Автоматизирана търговия: Предсказване на пазара и изпълнение на сделки със светкавична скорост.

***Образование***

Адаптивни платформи като Khan Academy използват изкуствения интелект, за да персонализират обучението спрямо индивидуалните нужди на учениците и студентите.

***Развлекателна индустрия***

Изкуствения интелект създава музика, филми и видеоигри. Алгоритмите за препоръки подобряват потребителското преживяване, предлагайки персонализирано съдържание.

# 5 Предизвикателства към изкуствения интелект и етични въпроси

Въпреки че изкуственият интелект предлага огромни възможности за трансформиране на обществото, неговото развитие и внедряване повдигат множество предизвикателства и етични дилеми. Тези въпроси обхващат аспекти като прозрачност, справедливост, социално въздействие, загуба на работни места и рискове за сигурността. В тази точка разглеждаме в дълбочина ключовите области, където се проявяват тези проблеми.

***Прозрачност и обяснимост***

Една от основните критики към съвременните системи за изкуствен интелект, особено тези, базирани на дълбоки невронни мрежи е липсата на прозрачност. Алгоритмите често действат като „черни кутии“, при които е трудно да се разбере как точно са стигнали до дадено решение. Това представлява проблем в критични области като:

- Медицина, където изкуствения интелект предлага диагнози или терапевтични препоръки, но лекарите и пациентите не могат да разберат напълно причините за тези препоръки.
- Правосъдие, където системи за предсказателно правосъдие вземат решения за съдбата на хора, без да има яснота относно използваните критерии.

Тази липса на обяснимост затруднява доверието в изкуствения интелект, ограничава неговото приемане и повдига въпроси за отговорността при грешки.

***Етика и предразсъдъци***

Изкуственият интелект е толкова добър, колкото са добри данните, с които е обучен. Проблеми възникват, когато алгоритмите наследяват предразсъдъци или неравенства от исторически данни. Например:

- В системи за наемане на персонал са открити предразсъдъци към жени и малцинства, защото историческите данни отразяват съществуващи дискриминационни практики.
- Програмите за разпознаване на лица често показват по-ниска точност при идентифициране на хора с различен етнически произход, което може да доведе до дискриминационни резултати в системи за сигурност.
- Необходимостта от създаване на етично „осъзнат“ изкуствен интелект, който да минимизира тези рискове, става критична задача за разработчиците и регулаторите.

***Загуба на работни места и социално въздействие***

Една от най-дискутираните теми е въздействието на изкуствения интелект върху пазара на труда. Автоматизацията може да замени милиони работни места, особено в сектори като производство, транспорт и административни услуги. Според прогнози, професии, които включват рутинни задачи, са най-застрашени, например:

- Шофьори и оператори, поради възхода на автономните превозни средства.
- Касиери и обслужващ персонал, с навлизането на автоматизирани системи за самообслужване.

В същото време, изкуствения интелект създава нови работни места в области като разработка на алгоритми, управление на данни и етична регулация. Предизвикателството е да се подготвят служители за тези нови роли чрез програми за преквалификация и образование.[5]

***Киберсигурност и поверителност***

Изкуствения интелект играе двойствена роля в сферата на киберсигурността:

- Като защитник: Алгоритмите за изкуствен интелект могат да анализират големи обеми от данни за откриване на необичайна активност, която сигнализира за кибератака.
- Като заплаха: Злонамерени актьори използват изкуствения интелект за създаване на усъвършенствани кибератаки, като например фалшиви идентичности (deepfakes) и автоматизирано генериране на зловреден софтуер.

Пример за това са deepfakes, които се използват за разпространение на дезинформация или измами, като фалшиви видеа, показващи политици или публични личности.

***Право на личен живот***

Изкуственият интелект зависи от огромни обеми данни, за да бъде ефективен, което поставя въпроси за защитата на личната информация. Технологии като проследяване на поведението в интернет, разпознаване на лица и анализ на социални мрежи често се използват без изричното съгласие на потребителите. Примерите включват:

***Анализ на потребителски данни от компании за рекламни цели***

Масово наблюдение от правителства, което нарушава правото на личен живот. Регулирането на тези аспекти е критично за баланса между иновации и защита на индивидуалните права.

***Автономност и отговорност***

Разработването на автономни системи, като например дронове и автономни автомобили, поставя въпроса за отговорността. При инциденти, причинени от изкуственият

интелект, трудно е да се определи кой носи отговорност – разработчиците, операторите или самите машини.

***Социално неравенство***

Широкото прилагане на изкуственият интелект рискува да задълбочи социалните неравенства. Достъпът до технологии и ползите от тях често са съсредоточени в по-развитите икономики и компании с високи ресурси, което оставя малки и развиващи се държави извън тези процеси.

# 6 Стратегии за преодоляване на предизвикателствата

- ***Разработка на обясними модели***: Инвестиране в изследвания за създаване на „интерпретируем“ изкуствен интелект, който да предоставя ясни и разбираеми обяснения за взетите решения.
- ***Етични кодекси и регулации:*** Разработване на международни стандарти и правна рамка за използване на изкуствения интелект.
- ***Инвестиране в преквалификация:*** Подкрепа за работниците, които могат да бъдат засегнати от автоматизацията, чрез осигуряване на достъп до обучение и нови възможности.
- ***Защита на личните данни:*** Въвеждане на стриктни регулации за събиране, съхранение и използване на лична информация.

Тези подходи са ключови за справяне с предизвикателствата и насърчаване на отговорното развитие и използване на изкуственият интелект.

**Таблица 1:** *Прогнозна ефективност за преодоляване на предизвикателства*

| Мярка | Очаквано намаление на риска (% до 2030 г.) | Разходи за прилагане (млрд. USD) |
|---|---|---|
| Разработка на обясними модели | 50 | 15 |
| Етични кодекси и регулации | 30 | 5 |
| Инвестиране в преквалификация | 40 | 20 |
| Защита на личните данни | 60 | 10 |

**Таблица 2:** *Прогнози за внедряване на изкуствения интелект*

| Година | Процент от компаниите използващи обясними изкуствени интелектуални модели (%) | Процент от данните със стриктна защита (%) |
|---|---|---|
| *2025* | *40* | *70* |
| *2030* | *70* | *85* |
| *2040* | *90* | *95* |

# 7 Разработка и оценка на обясними модели на изкуствен интелект

***Разработка на обясними модели***

Този тип модели се използват за групиране на предмети, процеси, обекти или категории въз основа на определени съществени характеристики, като същевременно ги

подреждат според степента на тяхното сходство. Основната цел при създаването на обясним модел е да се определи принадлежността на даден обект към предварително дефиниран клас, съобразявайки се с набор от негови характеристики – например цена, тегло, качество, размери, количество и други свойства. Характеристиките, които играят ключова роля за класификацията в тези модели, се наричат предиктори. За решаването на задачата за класификация е необходимо създаването на алгоритъм, който изгражда обобщен модел, способен еднозначно да свързва стойностите на предикторите с класа, към който принадлежи обектът. [2, 6]

***Оценяване на обясними модели***

Оценката на обясним модел се извършва чрез сравнение между предсказания клас на модела за всеки обект в тестовия набор и неговата действителна стойност. Ако двете стойности съвпадат, класификацията се счита за правилна, а ако не – се отчита класификационна грешка [1, 5]. Обяснимият модел отнася даден обект към един от възможните класове: правилно класифициран (True) или неправилно класифициран (False). При този подход са възможни четири вида класификация:

- True Positive (TP) – действителен е клас Positive и вярно класифициран като клас

Positive;

$$TP\ Rate = \frac{TP}{TP+FN} \quad \textbf{(1)}$$

- True Negative (TN) – действителен е клас Negative и вярно класифициран като клас Negative;

$$TN\ Rate = \frac{TN}{TN+FP} \quad \textbf{(2)}$$

- False Positive (FP) – действителен е клас Negative, а невярно класифициран като клас Positive;

$$FP\ Rate = \frac{FP}{FP+TN} \quad \textbf{(3)}$$

- False Negative (FN) – действителен е клас Positive, а невярно класифициран като клас

$$FN\ Rate = \frac{FN}{FN+TP} \quad \textbf{(4)}$$

Точност (Accuracy) се определя като съотношението между правилно класифицираните обекти и общия брой обекти в тестовия набор. Резултатът обикновено се изразява в проценти.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \quad \textbf{(5)}$$

Класификационна грешка (Error Rate) се изчислява като дял на неправилно класифицираните обекти спрямо общия брой обекти в тестовия набор. Тази стойност също се представя в проценти.

$$\text{Error Rate} = \frac{FP+FN}{TP+FP+TN+FN} \quad \textbf{(6)}$$

Прецизност (Precision) измерва точността на класификатора, като показва какъв процент от предсказаните обекти за даден клас са правилно класифицирани.

$$\text{Precision} = \frac{TP}{TP+FP} \quad \textbf{(7)}$$

Чувствителност (Recall) оценява пълнотата на класификатора, тоест каква част от обектите, които реално принадлежат на даден клас, са правилно идентифицирани. Резултатите обикновено се представят в проценти.

$$\text{Recall} = \frac{TP}{TP+FN} \quad \textbf{(8)}$$

F-мерка (F-measure) комбинира прецизността и чувствителността чрез тяхната претеглена хармонична средна стойност, като и тя се изразява в проценти

$$\text{F measure} = \frac{2}{{}^{1}/_{Recall} + {}^{1}/_{Precision}} \quad \textbf{(9)}$$

# 8 Заключение

Докладът разглежда развитието на изкуствения интелект, неговите приложения, предизвикателства и етични въпроси, както и стратегиите за преодоляване на потенциалните рискове. Изкуственият интелект (ИИ) е една от най-значимите технологични революции на 21-ви век, която оказва дълбоко влияние върху обществото, икономиката и ежедневието на хората. Неговото развитие, започнало с теоретични изследвания и експериментални приложения, днес е основен двигател на иновациите в множество индустрии. Чрез своите разнообразни технологии, като машинно обучение, дълбоко обучение, обработка на естествен език и компютърно зрение, изкуствения интелект предоставя безпрецедентни възможности за подобряване на човешкия живот и решаване на сложни глобални проблеми.

Приложенията на изкуствения интелект вече трансформират ключови сектори – от здравеопазването и транспорта до образованието и финансите. Например, в медицината той подпомага ранната диагностика и персонализираните терапии, докато в транспорта се използва за разработване на автономни превозни средства, които обещават по-безопасни пътища. Финансовият сектор използва изкуствения интелект за борба с измамите и оптимизация на инвестиционните стратегии, а образователните платформи се адаптират към индивидуалните нужди на учащите, предоставяйки им персонализирано обучение.

**ЛИТЕРАТУРА:**

[1] Калчева Н., Обзор на публикации със сравнителен анализ на методи и алгоритми за класификация на текст в машинното обучение, Списание Компютърни науки и технологии, ISSN 1312 -3335, 2020, ТУ – Варна, България, том 1, стр. 118-125.

[2] Калчева Н., М. Тодорова, Системи за управление на съдържание, 2016, Fourth Scientific International Conference Computer Sciences and Engineering, Varna, Bulgaria, ISSN 1312-3335, стр. 129-135

[3] Konstantinova E., Tsankov Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference “Ecology and environment”, 2021, ISSN 2367-5209

[4] Schmidhuber, J., Deep Learning in Neural Networks: An Overview of Neural Networks, 2015, Journal of Neural Networks Volume 61, ISSN: 0893-6080 DOI: 10.1016/j.neunet.2014.09.003, pp. 85-117

[5] Sutton, S., Barto G., Reinforcement Learning: An Introduction, 2018, The MIT Press, ISBN: 9780262039246, pp. 414-418

[6] Tegmark, M., Life 3.0: Being Human in the Age of Artificial Intelligence, 2017, Knopf Publishing Group, ISBN:978-1-101-94659-6, pp. 301-308

# COMPUTER SECURITY AND TRAFFIC MANAGEMENT IN COMMUNICATION NETWORKS*

**DIMITAR R. ILIEV, DANIEL R. DENEV**

***ABSTRACT:*** *This report examines the key aspects of computer security and network traffic management, which are essential for modern communication systems. The computer security section analyzes the principles of confidentiality, integrity, and availability, as well as the main threats, such as malware, phishing attacks, and zero-day vulnerabilities. Multi-layered security approaches, including encryption, firewalls, and multi-factor authentication, are also presented. Network traffic management focuses on the challenges associated with variable loads, network anomalies, and latency. Innovative technologies such as QoS, SDN, and real-time monitoring are presented, which improve the efficiency and reliability of networks.*

***KEYWORDS:*** *traffic management, phishing attacks, firewalls*

***DOI: https://doi.org/10.46687/XZLS4002***

# КОМПЮТЪРНА СИГУРНОСТ И УПРАВЛЕНИЕ НА ТРАФИК В КОМУНИКАЦИОННИТЕ МРЕЖИ

**ДИМИТЪР Р. ИЛИЕВ, ДАНИЕЛ Р. ДЕНЕВ**

***АБСТРАКТ:*** *Настоящият доклад разглежда ключовите аспекти на компютърната сигурност и управлението на мрежовия трафик, които са от съществено значение за модерните комуникационни системи. В частта за компютърната сигурност се анализират принципите на конфиденциалност, цялостност и достъпност, както и основните заплахи, като зловреден софтуер, фишинг атаки и zero-day уязвимости. Представени са също така многопластови подходи за защита, включващи криптиране, файъруоли и многофакторна автентикация. В управлението на мрежовия трафик се акцентира върху предизвикателствата, свързани с променливите натоварвания, мрежовите аномалии и забавянето. Представени са иновативни технологии като QoS, SDN и мониторинг в реално време, които подобряват ефективността и надеждността на мрежите.*

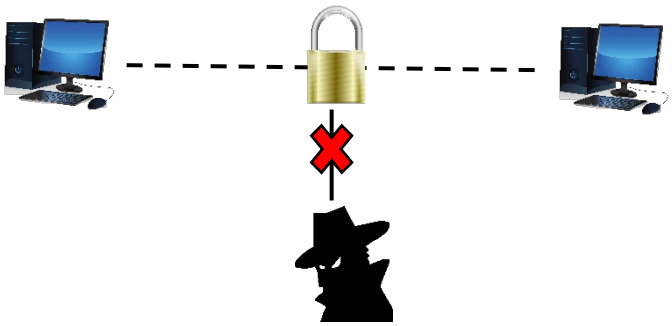
## 1 Въведение

С развитието на информационните технологии и цифровите комуникации, управлението на трафика в мрежите и компютърната сигурност играят критична роля за защита на информацията и поддържане на качествена свързаност. Този доклад разглежда основните аспекти на компютърната сигурност, предизвикателствата при управление на мрежовия трафик и решенията за осигуряване на стабилна и защитена комуникационна инфраструктура. [4, 5, 7, 8]

## 2 Основни принципи на компютърната сигурност

Компютърната сигурност, или киберсигурността, включва защитата на цифрови системи и мрежи срещу злонамерени атаки и неоторизиран достъп. Това е основополагаща дисциплина в съвременния свят, където данните и мрежите играят критична роля за функционирането на организации, държави и отделни лица.

* Докладът е финансиран по проект № РД-08-133/02.02.2024 „Подобряване на изследователската среда в областта, свързана с автоматизация на процеси“



**Фиг. 1.** Компютърна сигурност в комуникационните мрежи

### 2.1. Принципи на сигурността

Компютърната сигурност се основава на следните ключови принципи:

- ***Конфиденциалност:*** *Конфиденциалността гарантира, че информацията е достъпна само за оторизирани лица. Тя се осигурява чрез механизми за контрол на достъпа, като пароли, биометрия и криптиране на данните. Пример за нарушение на конфиденциалността е кражбата на лични данни от хакери, което може да доведе до финансови загуби или компрометиране на идентичността.*
- ***Цялостност:*** *Цялостността защитава данните от неоторизирана промяна. Всяка промяна в данните трябва да бъде проследима и одобрена. Примери за мерки за защита на цялостността включват използването на хеширащи алгоритми, които гарантират, че данните не са били променени по време на трансфер.*
- ***Достъпност:*** *Достъпността е свързана със способността на оторизираните потребители да имат достъп до данни или системи, когато им е необходимо. Атаки като DDoS (разпределен отказ на услуга) могат да компрометират достъпността и да причинят значителни загуби за бизнеса.*

### 2.2. Основни заплахи за компютърната сигурност

Модерните технологии създават множество уязвимости. Ето някои от най-често срещаните заплахи:

- ***Зловреден софтуер (Malware):*** *Зловредният софтуер включва вируси, червеи, троянски коне и рансъмуер. Той може да бъде използван за кражба на данни, повреда на файлове или извличане на откуп от жертвата.*
- ***Фишинг атаки:*** *Това са опити за измама, при които жертвите биват подведени да разкрият лична информация, като потребителски имена, пароли и кредитни карти. Фишингът често използва фалшиви уебсайтове или имейли, които изглеждат автентични.*
- ***Социално инженерство:*** *Атакуващите манипулират хора, за да получат достъп до защитени системи. Тези атаки се базират на доверие и липса на подозрение.*
- ***Zero-day уязвимости:*** *Уязвимости в софтуера, които все още не са известни на разработчиците и са открити от хакери, преди да бъдат коригирани.*

### 2.3. Методи за защита

Сигурността изисква многопластов подход, който включва следните мерки:

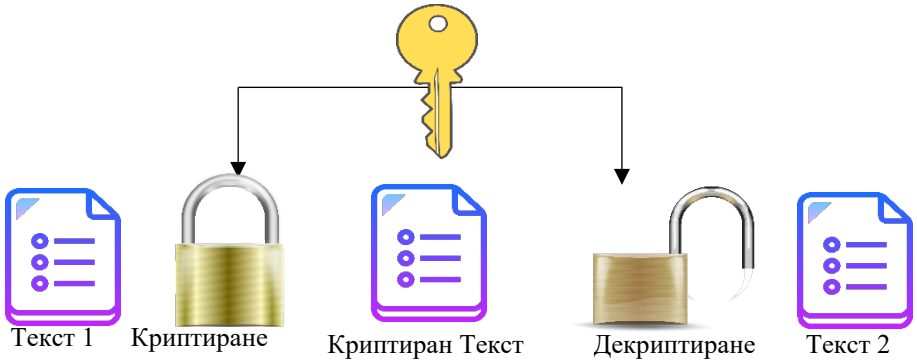
- ***Защитна стена:*** *Защитните стени филтрират мрежовия трафик, позволявайки само легитимни връзки. Те могат да блокират неоторизирани опити за достъп.*

➢ ***Криптиране:*** *Криптирането защитава данните чрез превръщането им в нечетлив формат за неоторизирани потребители. SSL и TLS са примери за криптиращи протоколи.*

➢ ***Многофакторна автентикация (MFA):*** *MFA добавя допълнителен слой на сигурност чрез изискване на повече от един начин за идентификация (напр. парола + код от SMS).*



**Фиг. 2.** Основни заплахи в компютърната сигурност




**Фиг. 3.** Действие на криптиране

## 3 Управление на трафика в комуникационните мрежи

С нарастването на обема на данните и сложността на мрежите, управлението на трафика става ключово за осигуряване на качествена комуникация. То включва различни методи и технологии за оптимизация на преноса на данни. [1, 2, 3]

### 3.1. Основни предизвикателства при управление на трафика

Мрежовият трафик е непредсказуем и подлежи на множество влияния:

➢ ***Променливи натоварвания:*** *Времето на деня, сезоните и специални събития могат да причинят внезапни увеличения в трафика, което води до претоварване.*

➢ ***Забавяне на данни (Latency):*** *Високото забавяне е особено проблематично за приложения като видеоконференции и игри в реално време.*

- ***Мрежови аномалии:*** *Атаки като DDoS или грешки в конфигурацията могат да доведат до сривове в мрежата.*

**3.2. Технологии за управление**

За справяне с тези предизвикателства се използват съвременни технологии:

- ***Quality of Service (QoS):*** *QoS е набор от технологии, които приоритизират трафика въз основа на неговата критичност. Например, трафикът за видеоконференции може да бъде приоритизиран пред имейли.*
- ***SDN (Software-Defined Networking):*** *SDN разделя управлението на мрежата от хардуера, позволявайки по-гъвкава и динамична конфигурация. Централизираното управление прави мрежите по-лесни за мониторинг и оптимизация.*
- ***Мрежови буфери:*** *Буферирането временно съхранява данни, за да компенсира забавянията при преноса.*

**3.3. Практически подходи**

Динамично маршрутизиране: Данните могат да бъдат насочвани през алтернативни маршрути, за да се избегнат претоварени зони.

- ***Мониторинг в реално време:*** *Използването на инструменти като NetFlow и Wireshark позволява бърза диагностика и разрешаване на проблеми.*

**Таблица 1:** Сравнение на подходи за управление на трафика в мрежите

| Критерий | Традиционни подходи | Съвременни подходи |
|---|---|---|
| *Управление на трафика* | *Статично и ръчно конфигуриране* | *Динамично, автоматизирано чрез QoS, SDN и мониторинг в реално време.* |
| *Преодоляване на забавяне* | *Ограничени решения, основно кеширане* | *Използване на мрежови буфери и динамично маршрутизиране.* |
| *Откриване на проблеми* | *Ръчно наблюдение и диагностика* | *Проактивно откритие на аномалии чрез мониторинг и анализ с NetFlow и Wireshark.* |

# 4 Съвременни технологии за сигурност и управление

С развитието на технологиите и все по-нарастващата зависимост от цифрови платформи и услуги, се налага прилагането на иновативни подходи за защита и управление на мрежите. Традиционните методи често са недостатъчни за справяне със сложните заплахи и динамичните натоварвания, които характеризират съвременните комуникационни системи. Съвременните технологии като изкуствения интелект (AI), машинното обучение (ML) и облачните решения трансформират начините за управление на трафика и осигуряване на сигурността. Те позволяват проактивно откриване на заплахи, автоматизация на задачите и оптимизация на ресурсите. Нови концепции като Zero Trust архитектурата и киберсигурността в облачни среди предлагат допълнителни слоеве на защита и адаптивност, което е от съществено значение в постоянно променящата се дигитална среда. В тази част се разглеждат тези иновации и тяхното влияние върху бъдещето на компютърната сигурност и управление на мрежовия трафик.

**4.1. Изкуствен интелект и машинно обучение**

С развитието на изкуствения интелект (AI), мрежите стават по-интелигентни и по-способни да откриват и реагират на заплахи:

- ***Откриване на заплахи:*** *AI анализира логове и аномалии в мрежата, за да идентифицира подозрителни модели. Например, той може автоматично да засече опити за неоторизиран достъп.*

- ***Автоматизация на задачите:*** *Много мрежови задачи, като настройване на защитни стени или управление на трафик, могат да бъдат автоматизирани чрез AI.*

**4.2. Киберсигурност в облачни среди**

С нарастващата употреба на облачни технологии възникват специфични предизвикателства:

- ***Шифроване на данни:*** *Всички данни в облака трябва да бъдат шифровани, за да се защитят от потенциални заплахи.*
- ***Защитни стени за приложения (WAF):*** *WAF предпазва уеб приложенията от атаки като SQL инжекции и скриптове между сайтове (XSS).*

**4.3. Zero Trust подход**

Zero Trust моделът изисква от всяка заявка да бъде валидирана, независимо дали идва от вътрешен или външен източник:

- ***Минимален достъп:*** *Потребителите и устройствата получават само необходимите права за изпълнение на задачите си.*
- ***Постоянна верификация:*** *Автентикацията е непрекъсната и динамична, базирана на контекста (напр. местоположение, устройство).*

**Таблица 2:** Сравнение на традиционни и съвременни подходи за сигурност

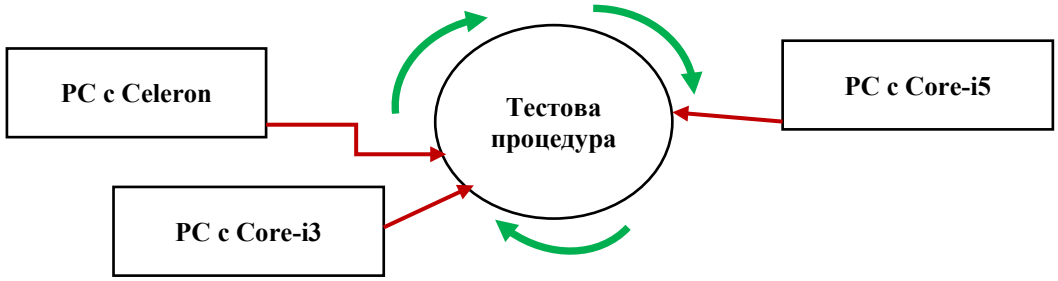
| Критерий | Традиционни подходи | Съвременни подходи |
|---|---|---|
| *Подход към достъпа* | *Централизиран достъп* | *Zero Trust, минимален достъп* |
| *Откриване на заплахи* | *Реактивно, след атака* | *Проактивно чрез AI и ML* |
| *Защита на данните* | *Локално шифроване* | *Шифроване в облачни среди* |
| *Автоматизация* | *Липса на автоматизация* | *Висока степен на автоматизация* |

# 5 Наблюдение и усъвършенстване на мрежовата комуникация в малка компютърна лаборатория

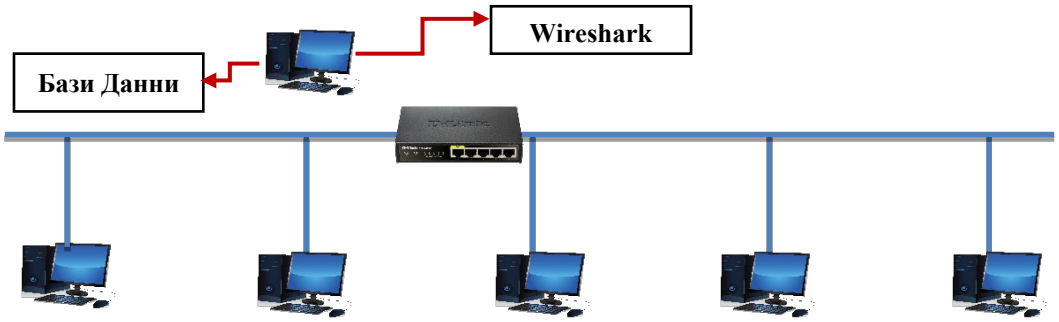
За провеждането на тестова процедура и с целите на изследването, тестовата постановка се организира в три етапа, включващи контролна и тестова група от индустриални устройства и комутатор, който служи като основен тестов елемент. Тестовата постановка е представена съответно на фиг. 5 и 6, показваща контролната и тестовата група. Подходът за организиране на трите етапа на теста е илюстриран на фиг. 4. За изследването са избрани три различни модела персонални компютри с процесори Core-i3, Celeron и Core-i5. Във всяка текуща тестова постановка се използват пет персонални компютъра от съответния тип, които се прилагат за конкретния етап. В допълнение, за тестовата постановка се използва интелигентен комутатор от модел Cisco Business 1100. [6, 9, 10]

И в двата вида тестови постановки се използва работна станция със следното предназначение:

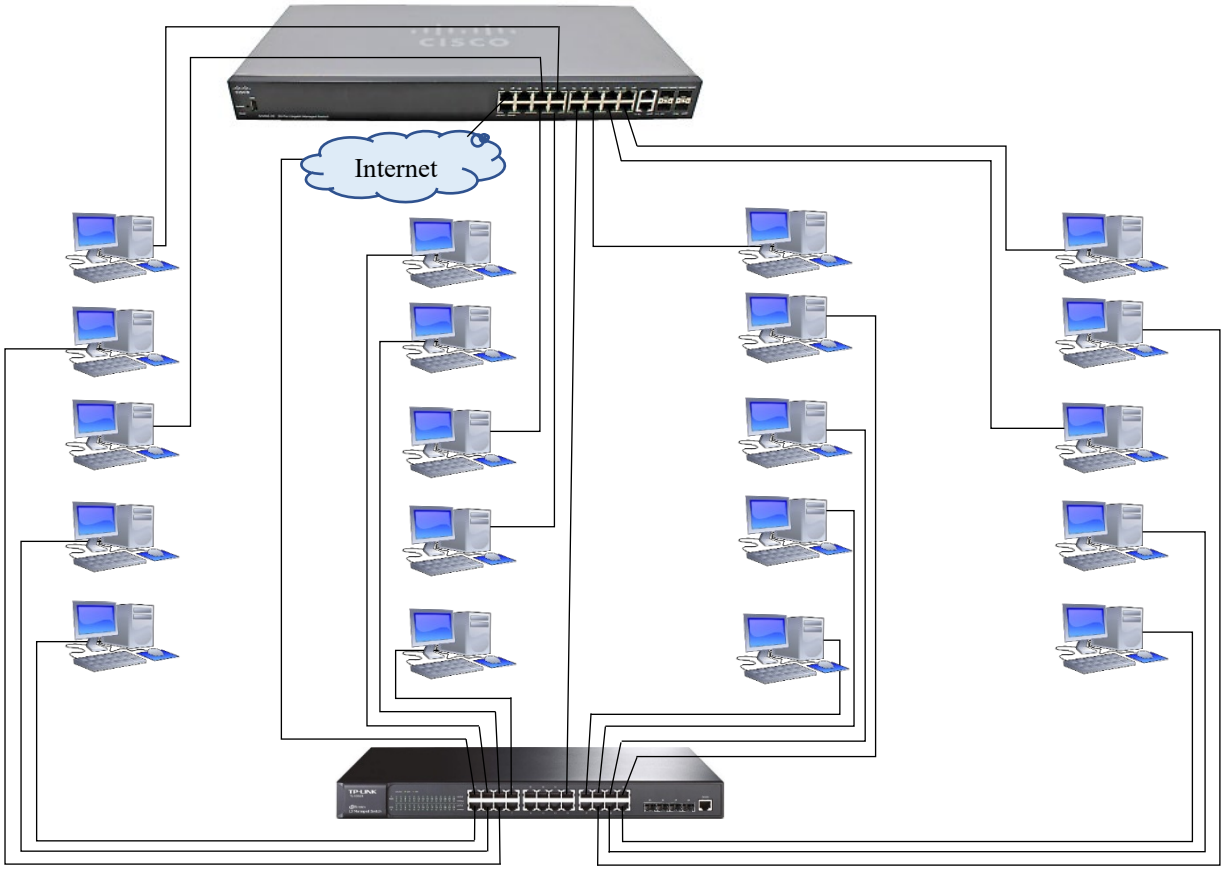
- Управление на тестовите приложения;
- Съхранение на междинни данни;
- Съхранение на тестовите резултати.
- За целите на изследването са подбрани следните приложения:
- Wireshark – приложение за анализ на мрежови протоколи и мрежови данни
- Matlab – интегрирана среда за синтез на скриптове, предназначени за анализиране на данни.




**Фиг. 4.** Подход за организиране на тестовата постановка




**Фиг. 5.** Схема на компютърна мрежа с контролен набор от устройства




**Фиг. 6.** Схема на компютърна мрежа с тестови набор от устройства

За формиране на емпиричен набор от резултати се установява следният набор от критерии:

- Номер на порт;
- Брой пакети;
- Размер на пакетите в байтове;
- Общ брой пакети;
- Брой изпратени пакети;
- Брой приети пакети.

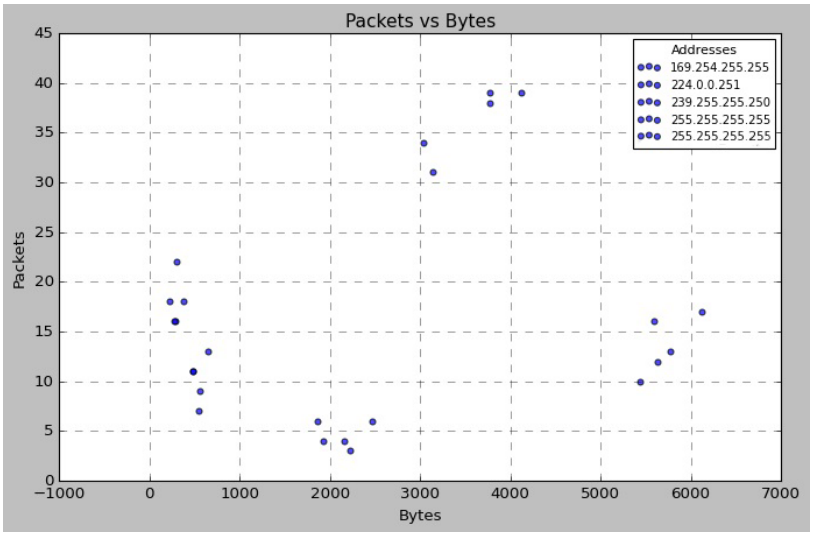
На основание теоретичната постановка е направено статистическото проучване за проверка на хипотези и доказване на резултатите от усъвършенстването на индустриалната мрежа. Графичното представяне на информация и данни, използвайки визуални елементи като диаграми, графики, карти и инструментите за визуализация, осигуряват достъпен начин за виждане и разбиране на тенденции, отклонения и модели в данните. То предоставя отличен начин за представяне на данни на нетехнически аудитории без объркване. За целите на изследването, данните от гореспоменатите компютри са представени в следните графики.

**Таблица 3:** Ethernet числови данни за PC 1

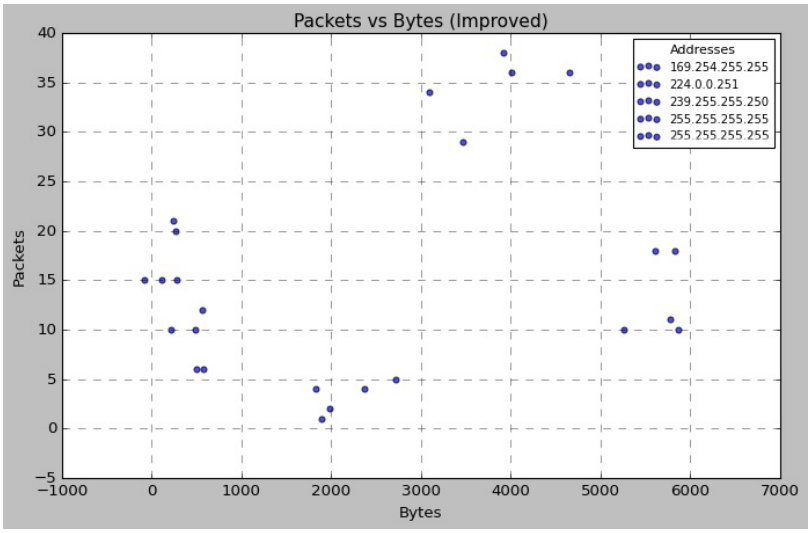
| Addresses | Packets | Bytes | Total Packets | Percent Filtered | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|---|---|
| *PC1* | *650* | *50123* | *1300* | *50.00%* | *0* | *0* | *650* | *50123* |
| *PC1* | *325* | *50123* | *650* | *50.00%* | *325* | *50123* | *0* | *0* |
| *PC1* | *40* | *32078* | *40* | *100.00%* | *0* | *0* | *40* | *32078* |
| *PC1* | *14* | *5256* | *22* | *66.00%* | *0* | *0* | *14* | *5256* |
| *PC1* | *11* | *8512* | *33* | *33.00%* | *0* | *0* | *11* | *8512* |
| *PC1* | *25* | *300* | *30* | *85.00%* | *25* | *300* | *0* | *0* |
| *PC1* | *1200* | *37000* | *1600* | *80.00%* | *1200* | *37000* | *0* | *0* |
| *PC1* | *180* | *40000* | *900* | *20.00%* | *0* | *0* | *180* | *40000* |
| *PC1* | *350* | *28345* | *1050* | *33.00%* | *350* | *28345* | *0* | *0* |
| *PC1* | *113* | *8400* | *113* | *100.00%* | *0* | *0* | *113* | *8400* |

**Таблица 4:** Ethernet числови данни за PC1 след усъвършенстване

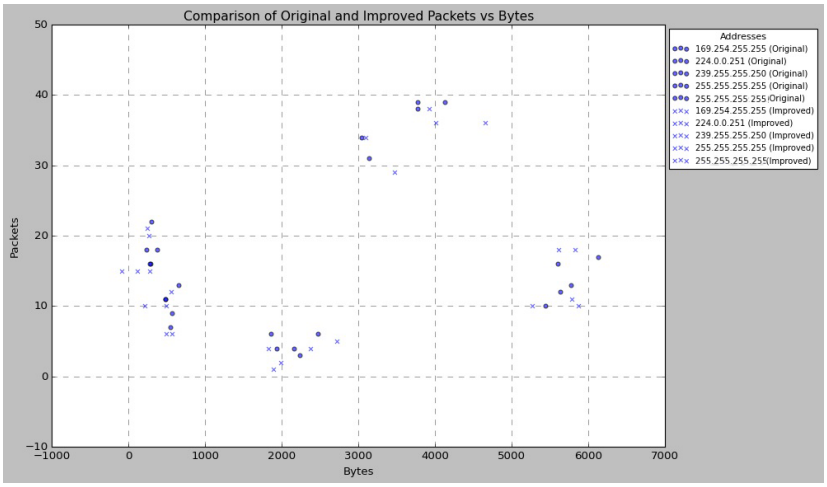
| Addresses | Packets | Bytes | Total Packets | Percent Filtered | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|---|---|---|---|---|---|---|---|---|
| *PC1* | *1170* | *552489* | *1300* | *90.00%* | *0* | *0* | *1170* | *552489* |
| *PC1* | *650* | *523215* | *650* | *100.00%* | *650* | *523215* | *0* | *0* |
| *PC1* | *40* | *32078* | *40* | *100.00%* | *0* | *0* | *40* | *32078* |
| *PC1* | *20* | *6985* | *22* | *90.00%* | *0* | *0* | *20* | *6985* |
| *PC1* | *33* | *9563* | *33* | *100.00%* | *0* | *0* | *33* | *9563* |
| *PC1* | *27* | *999* | *30* | *90.00%* | *27* | *999* | *0* | *0* |
| *PC1* | *1520* | *38458* | *1600* | *95.00%* | *1520* | *38458* | *0* | *0* |
| *PC1* | *900* | *42632* | *900* | *100.00%* | *0* | *0* | *900* | *42632* |
| *PC1* | *1050* | *29654* | *1050* | *100.00%* | *1050* | *29654* | *0* | *0* |
| *PC1* | *113* | *8400* | *113* | *100.00%* | *0* | *0* | *113* | *8400* |




**Фиг. 7.** Точкова диаграма на PC 1




**Фиг. 8.** Точкова диаграма на PC1 след усъвършенстване




**Фиг. 9.** Точкова диаграма съпоставка преди и след усъвършенстване

# 6 Заключение

В заключение, проведеното изследване демонстрира ефективността на използваните технологии и методи за управление на трафика и осигуряване на сигурността в комуникационните мрежи. Чрез използването на иновации като изкуствен интелект, машинно обучение и Zero Trust подход, беше установено, че тези технологии значително подобряват производителността и надеждността на мрежовите инфраструктури. Тестовата постановка, включваща различни типове персонални компютри и интелигентен комутатор, показва как подходящото комбиниране на хардуер и софтуерни решения може да оптимизира мрежовото управление и да намали рисковете от възникване на уязвимости.

Изследването подчертава необходимостта от адаптация към динамично променящите се условия в цифровата среда и важността на използването на проактивни подходи за откриване и предотвратяване на заплахи. В бъдеще, с напредъка в технологиите, ще продължава да бъде от критично значение интегрирането на нови методи за сигурност и управление, които да отговорят на все по-сложните изисквания на съвременните комуникационни мрежи. [1, 2, 3, 6, 8, 9]

**ЛИТЕРАТУРА:**


[1] Ahmedova D., Konstantinova E., Tsankov Ts. The use of packet sniffing tools in computer networks security. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 401-406.

[2] Denev D. Modeled Security in Communication Network Coding. 2022, Annual of Konstantin Preslavski University of Shumen, Vol. XII E, Faculty of technical sciences, ISSN 1311-834X, pp. 153-161.

[3] Denev D. Surveillance with Wireshark and its Use in Communication Networks. 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 104-109.

[4] Denev D., Hristova E., Tsankov Ts., Improving network communication and increasing the reliability of programmable devices in industry, 2023, Annual of Konstantin Preslavski University of Shumen, Volume XIII E, ISSN 1314-8818, pp. 39-52.

[5] Denev D., Konstantinova E., Main Issues in the Protection of Information in the system of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 110-115.

[6] Denev D., Tsankov Ts., Use of Cisco Packet Tracer in Evaluation of Communication Networks, 2023, XVI International Scientific Conference, Belovo, ISBN 978-5-00137-315-5 (item 1), ISBN 978-5- 00137-314-8, pp. 163-171.

[7] Hristova E., Denev D., Tsankov Ts. A Survey of Data Quality in Industrial Networks and Enhancing Their Reliability Complex Indicator for the Needs of the Industry, 2024, Proceedings of the 15th International Scientific and Practical Conference “Environment. Technology. Resources.”, Vol. II, Rezekne, Latvia, ISSN 1691-5402, ISBN 978-171389957-0 and DOI 10.17770/etr2024vol2.8036, pp. 120-126.

[8] 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, 2020, ISSN 2367-7902, pp. 373-378.

[9] Konstantinova E., Tsankov Ts. An overview of sustainable urbanism with the help of Artificial Intelligence. Proceedings of the Ninth student scientific conference “Ecology and environment”, 2021, ISSN 2367-5209, pp. 109-121.

[10] Lilov V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.

# K-NEAREST NEIGHBORS METHOD*

**MAYA P. TODOROVA**

***ABSTRACT:*** *The k-Nearest Neighbors (k-NN) method is a classification algorithm in machine learning that determines the class of new objects based on their similarity to the nearest k neighbors in a multidimensional space, measured using distance functions. The algorithm is characterized by easy interpretation of results, robustness to anomalies, and the ability to work with various types of data.*

***KEYWORDS:*** *k-nearest neighbors method, k-NN, KNN, machine learning*

***DOI: https://doi.org/10.46687/XGZV2227***

# МЕТОД „К-НАЙ-БЛИЗЪК СЪСЕД“

**МАЯ П. ТОДОРОВА**

***АБСТРАКТ:*** *Методът „К-най-близък съсед“ (k-NN) е алгоритъм за класификация в машинното обучение, който определя класа на нови обекти въз основа на сходството им с най-близките k съседа в многомерно пространство, измерено чрез функции за разстояние. Алгоритъмът се отличава с лесна интерпретация на резултатите, устойчивост на аномалии и възможност за работа с различни типове данни.*

## 1 Въведение

Обемът на машинно генерираните данни продължава да нараства с впечатляваща скорост, което поставя предизвикателства пред ефективното им обработване и анализ. Извличането на знания от тези данни е сложен процес, който включва откриване на връзки, закономерности, модели, тенденции и аномалии. Този процес използва алгоритми и техники от различни научни области като машинно обучение, статистика и визуализация на данни.

Машинното обучение, като ключова част от анализа на данни, предлага множество методи за обработка и интерпретация на големи обеми информация. Един от основните и широко използвани подходи е методът на К-най-близък съсед, който се основава на сходството между обектите в многомерно пространство.

## 2 Метод „К-най-близък съсед”

К-най-близък съсед (k-Nearest Neighbors (k-NN)) е метод за класификация и прогнозиране. В основата на алгоритъма на К-най-близък съсед е съществуващата прилика между обектите. Основният принцип на метода е, че обект принадлежи към клас, към който принадлежат повечето от най-близките му съседи в многомерното пространство от признаци [1, 2, 3, 4]. Всеки обект се представя като точка в пространството чрез неговия вектор. При работа с реални данни, чиито етикети на класа са неизвестни, се изчислява разстоянието между вектора на новото наблюдение и предварително запаметеното. Избират се k вектори, които са най-близо до него. Новият обект принадлежи към класа, към който принадлежат повечето от тях. Алгоритъмът изчислява дистанцията между всеки два обекта от обучаващата извадка, чрез използване на подходяща функция за измерване на разстояние

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

между две точки. Намиране на сходство и различие между точките от данни може да се реализира чрез използване на различни функции.

Функцията за измерване на разстояние е функция с реална стойност *Dist*, такава че за всякакви координати *x, y* и *z* са изпълнени следните правила:

1. Dist(x, y) ≥ 0, (1)
   Dist(x, y) = 0, ако x = y;
2. Dist(x, y) = Dist(y, x) (2)
3. Dist(x, z) ≤ Dist(x, y) + Dist(y, z) (3)

Точките *x, y, z* не лежат на една права линия и са вектори на характеристиките на сравняваните обекти [5].

Формулировка:

Зададена е обучителната извадка на двойките „обект-отговор“.

$$X_m = \{(x_1, y_1),(x_2, y_2), \dots \dots . (x_m, y_m)\} \quad (4)$$

Зададена е функцията на разстоянието между множеството обекти.

$$\rho = (x, x') \quad (5)$$

За произволен обект *u* се разполагат обектите от обучаващата извадка $x_i$ в увеличаващ се ред на разстоянията до *u*.

$$\rho\big(u, x_{1;u}\big) \leq \rho\big(u, x_{2;u}\big) \leq \cdots \leq \rho(u, x_{m;u}), \quad (6)$$

Където:

$x_{i;u}$ - обект на обучаващата извадка, който е i-ия съсед на обекта *u*. Произволният обект *u* генерира преномериране на извадката.

Алгоритъмът на К-най-близък съсед се задава като:

$$a(u) = \underset{y \epsilon Y}{argmax} \sum_{i=1}^{m} \big[x_{i;u} = y\big]\omega(i, u), \quad (7)$$

Където:

$\omega(i, u)$ - функция на теглото, която оценява степента на важност на i-ия съседа за класифициране на обекта *u* и $\omega(i, u) = [i \leq k]$.

Преди да се приложи алгоритъмът k-NN е необходимо да се извърши нормализация на данните. Съществуват различни подходи за мащабиране. Първи начин за нормализация е осъществяване на преход от абсолютна стойност на признака към относителна [6].

$$x_i \equiv \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (8)$$

Предимството на новите променливи е, че те приемат стойности от 0 до 1 или в процентно съотношение от 0 до 100.

Втори начин на мащабиране:

$$x_i \equiv \frac{x_i - \bar{x}}{s} \tag{9}$$

Където:

$\bar{x}$ - средна извадка

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, \tag{10}$$

*s* – средноквадратично отклонение

$$s = \sqrt{\frac{1}{n-1}(x_i - \bar{x})^2} \tag{11}$$

Правилният избор на броя на съседите, които ще бъдат приложени в алгоритъма, определя колко добре моделът ще се генерализира към бъдещи данни. Изборът на голяма стойност на $k$ намалява въздействието или отклонението, причинено от шумни данни, но същевременно може да се игнорират малки, но важни модели. Ако стойността на $k$ е равна на общия брой обекти в обучителната извадка, тогава моделът винаги би предсказвал класа на мнозинството, независимо кои съседи са най-близки т.е. игнорира се разстоянието до изучавания обект [7].

**Предимства:**

- добро обучение в случай на линейно неразделими извадки [8];
- резултатът от алгоритъма е лесен за интерпретация [9];
- алгоритъмът е устойчив на аномалии;
- лесен за усвояване и разбиране [10];
- бърза фаза на обучение;
- възможност за работа с различни типове данни.

**Недостатъци:**

- необходимост от голям изчислителен ресурс при наличието на голям обем данни;
- точността на алгоритъма зависи от избор на метрика за разстояние [8];
- номиналните характеристики и липсващи данни изискват допълнителна обработка;
- трудности при избор на подходящо число k;
- не създава модел за намиране на отношения между характеристики [11].

# 3 Заключение

Алгоритъмът „К-най-близък съсед“ (k-NN) демонстрира значителни предимства, включително лесна интерпретация на резултатите, устойчивост на аномалии и възможност за работа с различни типове данни. Освен това, алгоритъмът позволява бързо обучение, което го прави подходящ за приложения с времеви ограничения.

Изискването за голям изчислителен ресурс при работа с големи обеми данни и зависимостта от избора на метрика за разстояние са значителни предизвикателства. Освен това, номиналните характеристики и липсващите данни често налагат допълнителна предварителна обработка, което може да увеличи сложността на метода. Точността на алгоритъма е силно зависима от правилния избор на параметъра $k$, като твърде високи или ниски стойности могат да доведат до погрешни класификации или игнориране на важни детайли в данните.

**ЛИТЕРАТУРА:**

[1] Боровский, А. Перспективы применения технологий машинного обучения к обработке больших массивов исторических данных. Кибернетика и программирование 1, 2015, стр. 77-114, DOI: 10.7256/2306-4196.2015.1.13730

[2] Ха, Л. Оптимизация алгоритма KNN для классификации текстов. Труды Московского физико-технического института 8, no. 1 (29), 2016

[3] Harrington, P. Machine Learning in Action. USA:Manning, ISBN 9781617290183, 2012. pp.1-382.

[4] Khuman, M. Classification of remote sensing data using K-NN method. Journal of information, knowledge and research in electronics and communication engineering, ISSN: 0975 – 6779, Volume 2, Issue 2, 2013, pp. 817-821.

[5] Alfeilat H., et al. Effects of Distance Measure Choice on K-Nearest Neighbor Classifier Performance: A Review. Big Dasta, 2019, DOI: 10.1089/big.2018.0175

[6] Lantz, B. Machine Learning with R. Packt Publishing Ltd, ISBN 978-1-78216-214-8, 2013, pp.1-396.

[7] Daume III, H. A course in machine learning. Published by TODO, 2017, pp.1-227, http://ciml.info/

[8] Батура, Т. Методы автоматической классификации текстов. Программные продукты и системы 30, no. 1, 2017.

[9] Breiman, L., et al. Classification and regression trees. eBook ISBN 9781315139470, 2017, pp. 1-368.

[10] Кирилова, Е. Синтез на класификатори по цветови признаци за откриване на плесени от рода Fusarium Moniliforme по царевични зърна. Научни трудове на Русенския Университет 51, 2012, с. 168-175.

[11] Bellaachia, A., E. Guven. Predicting Breast Cancer Survivability Using Data Mining Techniques. Department of Computer Science The George Washington University Washington DC 20052, 2006, pp.1-4.

# ARTIFICIAL NEURAL NETWORK*

**GINKA K. MARINOVA**

***ABSTRACT:*** *Artificial neural networks are a powerful method for processing information, inspired by biological neurons. They combine parallel processing, self-learning, and adaptability, finding applications in various fields, including analysis and prediction. Their main advantages include noise resistance and the ability to solve problems with unknown patterns, while their disadvantages encompass complexity and the time required for training.*

***KEYWORDS:*** *Artificial neural networks, Neural Network Architecture, Data Analysis*

***DOI: https://doi.org/10.46687/FETK2923***

# ИЗКУСТВЕНА НЕВРОННА МРЕЖА

**ГИНКА К. МАРИНОВА**

***АБСТРАКТ:*** *Изкуствените невронни мрежи са мощен метод за обработка на информация, вдъхновен от биологичните неврони. Те съчетават паралелна обработка, самообучение и адаптивност, като намират приложение в различни области, включително анализи и прогнози. Основните им предимства включват устойчивост на шум и възможност за решаване на задачи с неизвестни закономерности, докато недостатъците включват сложност и продължителност на обучението.*

## 1 Въведение

Изкуствените невронни мрежи представляват иновативен инструмент за обработка на данни, който съчетава паралелна обработка и способността за самообучение. Тяхната структура, вдъхновена от биологичните неврони, осигурява висока ефективност и адаптивност при решаването на сложни задачи в различни области. В контекста на психологическите тестове и анализи, невронните мрежи допринасят за повишаване на точността и обективността на резултатите, като запазват използваните данни за последващи изследвания. Развитието на тези мрежи включва архитектурен дизайн, избор на алгоритми за обучение и прилагането на активиращи функции, които гарантират прецизно обработване и класификация на информацията.

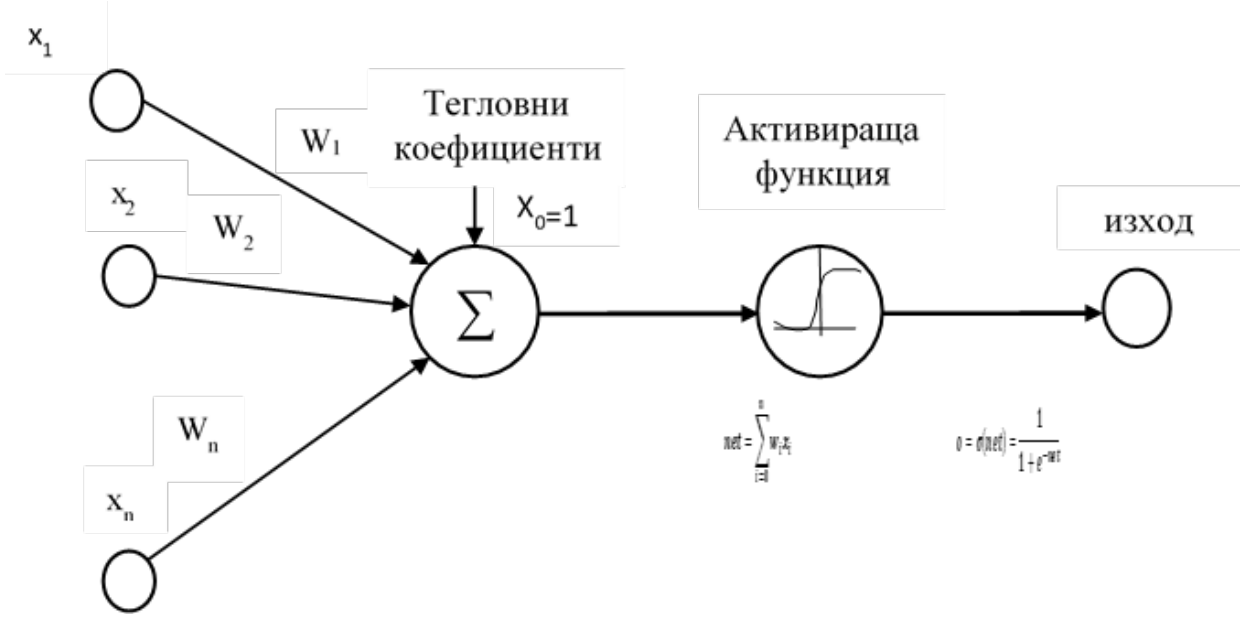
## 2 Изкуствена Невронна Мрежа

Изкуствената Невронната мрежа (НМ) е динамична система използваща се за увеличаване на точността и обективността при прилагането, и в различни психологични тестове, като метод за паралелна обработка на информация, която има качеството да съхранява използваните данни. Всяка невронна мрежа е съставена от елементи за обработка на информация, които са наречени неврони. Входната информация за всеки неврон е претеглена сума от сигналите на останалите неврони.

Информацията се събира в неврона, като изходният сигнал се определя посредством активираща функция. Процесът на обучение при невронните мрежи е целесъобразно изменение на тегловните коефициенти, като целта е да се постигнат необходимите

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

свойства. Информацията в невронната мрежа се наслагва при обучение, като силата на връзките между отделните възли се оформя от теглата на съответните връзки, които се използват за съхранение на информация за дадено определено изследване.




**Фиг. 1.** Модел на невронна мрежа [1]

Невронът се състои от много входове и един изход (фиг.1). На входовете от $\boldsymbol{x_1, x_2, \ldots, x_n}$ се подават сигналите към неврона. Всеки вход се определя с определен тегловен коефициент $\boldsymbol{w_i}$, където $\boldsymbol{i=1, 2, 3, \ldots, n}$, оформящ съответствието за предаване на сигнала. Агрегирането на входните сигнали се моделира чрез суматор, чийто изходен сигнал се изчислява по следната формула [1, 2]:

$$\boldsymbol{net} = \sum_{\boldsymbol{i=0}}^{\boldsymbol{n}} \boldsymbol{w_i x_i} \tag{1}$$

От стъпките за изпълнение на алгоритъма може да бъде определен и прагов елемент (bias), който е обозначен със символа ($w_0$), описан като:

$$\boldsymbol{net} = \boldsymbol{w_0} + \sum_{\boldsymbol{i=0}}^{\boldsymbol{n}} \boldsymbol{w_i x_i} \tag{2}$$

Активиращата функция се изчислява по установена математическа формула, която служи за да се пресметне стойността на изходния сигнал.

Изборът на функция за активиране се дефинира от индивидуалността на решаваната задачата. Функцията за активиране е нелинейна, която изчислява изходния сигнал [1, 2]:

$$\boldsymbol{o} = \boldsymbol{\sigma}(\boldsymbol{net}) = \frac{\boldsymbol{1}}{\boldsymbol{1+e^{-net}}} \tag{3}$$

Класификацията на дадена невронна мрежа се определя от основни елементи, като:

- Архитектура на НМ се определя от начина на свързване между различните неврони;

- Избор на алгоритъм за обучение дефинира се метод, по който се конфигурират теглата на връзките между невроните, така че да се извърши необходимото преобразуване на сигналите.

Архитектурата е характеристика определяща организацията и начина, по който множеството неврони в мрежата са подредени, и свързани по нея се определят, и функционалните им особености. Броят слоеве и неврони във всеки слой зависят от сложността на определената решавана задача. Тези слоеве са три вида: входящ, скрит и изходящ. На входящият слой постъпва информацията а на изходящия слой се извеждат резултатите. Между входящия слой и изходящия слой може да има един или няколко скрити слоеве. Предназначението на тези слоеве е да открият съществуващите взаимовръзки между входните и изходните променливи.

Архитектурите на невронните мрежи са еднослойни или многослойна невронна мрежа. По отношение на характеристиките на невронните мрежи от основно значение е способността им да се учат и да подобряват работата си чрез обучение. Обучението е метод, при който се настройват теглата и връзките между невроните чрез моделиране на средата, в която работи мрежата, като целта е изпълнение задачата за която е проектирана невронната мрежа. По време на обучението мрежата извлича функционални зависимости от входните данни. В края на процеса тези зависимости се запомнят, като теглови стойности и структура на връзките между невроните и впоследствие се използват.

**Предимствата са** [2, 3 4, 5]:
- висока устойчивост на шум при обработка на данни [2, 3];
- възможност за обобщение при оценяване и прогнозиране на дадени стойности [2];
- притежават съвкупност от качества, които позволяват прилагането им в различни области [2, 3];
- използват се за решение на задачи с неизвестни закономерности [2, 3];
- използват се като средство за паралелна обработка [5].

**Недостатъците са** [2, 3, 5]:
- задължителност от обучение на математичен модел [3];
- необходимост от време при промяна входните параметри, за дефиниране и обучение [3];
- необходимост от приспособяване на архитектурата към конкретно решавана задача [3];
- определени изкуствени невронни мрежи се нуждаят от високопроизводителни процесори [3];
- трудоемкост и продължителност на обучение [5].

# 3 Заключение

Изкуствените невронни мрежи предлагат мощен инструмент за анализ и обработка на данни, като комбинират устойчивост на шум, способност за обобщение и възможност за паралелна обработка. Тяхната гъвкавост позволява адаптиране към широк спектър от задачи, като същевременно осигуряват надеждност и ефективност. Въпреки това, предизвикателствата като необходимостта от обучение, дългият времеви процес за адаптация и изискванията към хардуера подчертават нуждата от по-нататъшно оптимизиране на тези технологии. Невронните мрежи остават ключов компонент в съвременния инструментариум за решаване на сложни задачи и моделиране на данни.

**ЛИТЕРАТУРА:**

[1] Mitchell, T. Machine Learning, McGraw-Hill Science, ISBN 0070428077, 1997

[2] Michalski, R., J. Carbonell, T. Mitchell. Machine Learning, 1st Edition, Imprint: Morgan Kaufmann, 2014

[3] Пашова, Л. Приложение на интелигентни методи за обработка на анализ на геоданни, http://www.geophys.bas.bg/discussion/NIGGG_Discusionen_club_LPashova.pdf

[4] Mijwel, M. Artificial Neural Networks Advantages and Disadvantages, https://www.researchgate.net/profile/Maad-Mijwil/publication/323665827_Artificial_Neural_Networks_Advantages_and_Disadvantages/links/5aa2c01faca272d448b5a23d/Artificial-Neural-Networks-Advantages-and-Disadvantages.pdf

[5] G. Zhang. Neural networks for classification: a survey, in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 30, no. 4, pp. 451-462, Nov. 2000.

# COUNTERING AND COMBATING CORRUPTION IN PUBLIC ADMINISTRATIONS*

**ILIANA K. SIMEONOVA, ELITSA YU. KUZMANOVA**

***ABSTRACT:*** *This report addresses the issue of countering and combating corruption in public administrations, offering an overview of the main measures and strategies to curb this phenomenon. The introduction highlights the importance of the problem of corruption and its negative effects on institutional stability and socio-economic development. It discusses the causes and manifestations of corruption and various countermeasures, including institutional reforms, improved transparency, legislative initiatives and staff training. It concludes by stressing the need for a systematic approach and the active involvement of society and the international community to achieve long-term results in the fight against corruption.*

***KEYWORDS:*** *corruption, public sector, public administration*

***DOI: https://doi.org/10.46687/CHKG4621***

# ПРОТИВОДЕЙСТВИЕ И БОРБА С КОРУПЦИЯТА В ПУБЛИЧНИТЕ АДМИНИСТРАЦИИ

**ИЛИАНА К. СИМЕОНОВА, ЕЛИЦА Ю. КУЗМАНОВА**

***АБСТРАКТ:*** *Настоящият доклад разглежда темата за противодействието и борбата с корупцията в публичните администрации, като предлага обзор на основните мерки и стратегии за ограничаване на този феномен. Във въведението се подчертава значимостта на проблема с корупцията и негативните ѝ ефекти върху институционалната стабилност и социално-икономическото развитие. В изложението са разгледани причините и проявленията на корупцията, както и различни мерки за противодействие, включително институционални реформи, подобряване на прозрачността, законодателни инициативи и обучение на служителите. В заключение се акцентира върху необходимостта от системен подход и активното участие на обществото и международната общност за постигане на дългосрочни резултати в борбата с корупцията.*

## 1 Въведение

Корупцията в публичните администрации е глобален проблем, който засяга всички нива на управление. Тя отслабва доверието на гражданите в институциите, нарушава принципите на правовата държава и подкопава социално-икономическото развитие. Корупцията е сложно, социално-икономическо, административно, политическо и правно явление. [1]

Въпреки множеството усилия за нейното ограничаване, корупцията продължава да бъде значително предизвикателство за много държави.

Настоящият доклад има за цел да предостави общ преглед на мерките и стратегиите за противодействие и борба с корупцията в публичния сектор, като разгледа основните подходи и предизвикателства пред тези усилия.

* Докладът е финансиран по проект № РД-08-147/02.02.2024 г., „Усъвършенстване на способностите за създаване на сценарий за тестване на уязвимости в симулационен оперативен център за сигурност“

# 2 Причини и проявления на корупцията в публичните администрации

Корупцията е сложен и многопластов проблем, който може да бъде предизвикан от различни причини и фактори. Те могат да бъдат свързани с политическата, икономическата, социалната или културната среда в дадена държава или организация. Корупцията може да приеме различни форми, като подкупи, злоупотреба с власт, измами и търговия с влияние. Класическо корупционно престъпление по нашето законодателство е подкупът. Както отбелязва Ненов „тежестта на подкупа се определя и от обстоятелството, че той като обществено явление може да нанесе особено тежки вреди на функционирането на държавния апарат. При неговото извършване най-остро се проявява противоречието между морала, общественото съзнание и индивидуалната назадничава психология".[5]

Основни фактори, допринасящи за разпространението на корупционни практики, включват слаби институции, липса на прозрачност, неадекватен контрол и отчетност, както и недостатъчни санкции срещу извършителите. Ниското ниво на доходи на служителите в публичния сектор също често стимулира корупционни практики. Тези фактори могат да взаимодействат и да се влияят взаимно, създавайки условия за възникване и разпространение на корупцията. За борба с корупцията се изисква комплексен и многостранен подход, включващ както правни и институционални реформи, така и културни и образователни мерки

Основните причини и фактори, които допринасят за възникването на корупция в публичните администрации, е от съществено значение за разбирането и борбата с този сериозен проблем.

Корупцията често се развива в обстановка на недостатъчна прозрачност и отчетност в дейността на публичните институции. Когато решенията се вземат в закрити или непрозрачни процеси, се откриват възможности за злоупотреби и корупция. Недостатъчната ефективност на институциите за контрол и надзор може да създаде условия за безнаказаност на корумпирани действия. Липсата на независимост, професионализъм и ресурси на тези институции може да улесни разпространението на корупцията.

Слабите етични стандарти и култура на отговорност водят до това, че корупцията се подхранва в общества, където личната и институционалната отговорност са ниски или липсват.

Недостатъчната етика и лоялност към обществения интерес могат да доведат до разпространение на корупцията.

Неравенството в разпределението на богатството, ниският стандарт на живот и липсата на социална сигурност могат да принудят хората да се обръщат към корумпиране като начин за оцеляване или за постигане на лични цели.

Влиятелни бизнес и политически интереси могат да упражняват натиск върху публичните институции, за да насочат вземането на решения в техните интереси. Това може да доведе до корумпирани практики и злоупотреби с обществените ресурси.

**Анализ на основните причини и фактори, които допринасят за възникването на корупцията в публичните администрации**.

Анализът на основните причини и фактори, които допринасят за възникването на корупция в публичните администрации, е от съществено значение за разбирането и борбата с този сериозен проблем. Ето някои от основните причини и фактори:

Липса на прозрачност и отчетност: Корупцията често се развива в обстановка на недостатъчна прозрачност и отчетност в дейността на публичните институции. Когато решенията се вземат в закрити или непрозрачни процеси, се откриват възможности за злоупотреби и корупция.

Слаби институционални механизми за надзор и контрол: Недостатъчната ефективност на институциите за контрол и надзор може да създаде условия за безнаказаност на корумпирани действия. Липсата на независимост, професионализъм и ресурси на тези институции може да улесни разпространението на корупцията.

Слаби етични стандарти и култура на отговорност: Корупцията се подхранва в общества, където личната и институционалната отговорност са ниски или липсват. Недостатъчната етика и лоялност към обществения интерес могат да доведат до разпространение на корупцията.

Икономически и социални фактори: Неравенството в разпределението на богатството, ниският стандарт на живот и липсата на социална сигурност могат да принудят хората да се обръщат към корумпиране като начин за оцеляване или за постигане на лични цели.

Натиск от бизнес и политически интереси: Влиятелни бизнес и политически интереси могат да упражняват натиск върху публичните институции, за да насочат вземането на решения в техните интереси. Това може да доведе до корумпирани практики и злоупотреби с обществените ресурси.

Анализът на тези причини и фактори е важна стъпка към разработването на стратегии за борба с корупцията в публичните администрации. Такива стратегии трябва да бъдат многостранни и включват законодателни реформи, подобряване на институционалните механизми за надзор и контрол, както и поощряване на култура на отговорност и прозрачност.

## 3 Идентифициране на слабите места в системата и процесите, които улесняват корупцията

Идентифицирането на слабите места в публичните администрации, е от ключово значение за борбата с корупцията. Областите, които обикновено са уязвими към корупция и които трябва да бъдат преодолени са:

*Липсата на прозрачност и отчетност*: Прозрачните процеси и действия на публичните институции са ключови за предотвратяване на корупцията. Ако документацията и решенията не са достъпни за обществото, се създава възможност за скрити сделки и злоупотреби.

*Слаб контрол и надзор*: Недостатъчната ефективност на институциите за контрол и надзор позволява на корумпирани действия да се случват без наказание. Липсата на независимост, професионални квалификации и ресурси на тези институции може да улесни злоупотребите.

*Липса на етични стандарти и култура на отговорност*: Ако в организацията липсва ясна етика и култура на отговорност, служителите могат да бъдат склонни към корумпирани практики. Недостигът на вътрешни правила и механизми за справедливост може да подхранва корупцията.

*Липса на обучение и осведоменост*: Недостатъчната подготовка на служителите по отношение на етиката и законодателството, свързано с корупцията, може да ги направи уязвими към злоупотреби. Обучението и осведомеността за етичните стандарти и рисковете от корупция са от съществено значение за предотвратяване на този проблем.
*Натиск от бизнес и политически интереси*: Влиятелни бизнес и политически интереси могат да упражняват натиск върху публичните институции и служители, за да постигнат свои цели. Това може да включва злоупотреба с обществени ресурси и вземане на решения в полза на определени групи.

Идентифицирането на тези слаби места е първа стъпка към изграждането на система за предотвратяване на корупцията. Заедно със създаването на механизми за надзор, обучение и подкрепа за етични стандарти, може да се намали риска от корупция и да се насърчи по-честно и прозрачно управление.

# 4 Ролята на публичната администрация в обществото

Ролята на публичната администрация в обществото е многопластова и включва различни аспекти, които имат за цел поддържането на ред, защитата на интересите на гражданите и осигуряването на благосъстояние. Основните задължения на публичната администрация в обществото включват:
*Изпълнение на законите и политиките*: Публичната администрация е отговорна за изпълнението на законите и политиките, приети от правителството или законодателните институции. Това включва осигуряването на ефективно управление на държавните институции и изпълнението на правилата и процедурите, установени от законодателството.
*Предоставяне на обществени услуги*: Публичната администрация предоставя различни обществени услуги на гражданите и предприятията. Тези услуги включват здравеопазване, образование, социални грижи, транспорт, комунални услуги и други, които са от съществено значение за благосъстоянието и качеството на живот на гражданите.
*Регулация и надзор*: Публичната администрация установява правила, норми и стандарти за различни области на обществения живот, като се стреми да гарантира сигурността, качеството и справедливостта в тях. Тя осигурява регулаторна рамка за дейността на различни сектори на икономиката и обществото.
*Финансово управление*: Публичната администрация управлява бюджета на държавата, събира данъци, разпределя средства за различни програми и инвестиции, управлява държавните финанси и гарантира финансовата устойчивост на държавата.
*Комуникация и информационни технологии*: Публичната администрация осигурява комуникационни канали за взаимодействие с гражданите и бизнеса, както и управление на информационните технологии за подкрепа на административните процеси и достъпността на информацията.
*Управление на човешките ресурси:* Публичната администрация ръководи набирането на персонал, управлението на служителите, разработването на политики за трудовите отношения и обучението на персонала, което е от съществено значение за ефективното функциониране на държавата.

Тези задължения на публичната администрация са от съществено значение за стабилността, развитието и благосъстоянието на обществото.

Корупцията в публичната администрация може да приема различни форми и да се проявява по различни начини. Ето някои от основните видове корупция и техните примери в публичната администрация са:

*Вземане и даване*: Това включва даване на пари, подаръци или други блага на публични служители в замяна на услуги, благоприятно вземане на решения или улесняване на процеси.

*Злоупотреба с властта*: Това включва използване на властта и позицията на публични служители за лични ползи или полза на други лица или организации.

*Непотизъм и клиентелизъм*: Това включва предпочитане на роднини, приятели или партньори за длъжности или бизнес възможности в ущърб на квалифицирани кандидати.

*Лавино измами*: Това включва фалшифициране на документи, измами при обществени поръчки, измами с финансови средства и други престъпни дейности, свързани със средствата на обществените финанси.

*Забавяне на процесите*: Това включва умишлено забавяне или блокиране на процеси или вземането на решения, които са от значение за обществото, с цел изнудване на хора или организации за лична печалба.

Тези са само някои от примерите за видове корупция в публичната администрация. Всяка ситуация може да бъде уникална и да изисква специфични мерки за предотвратяване и борба с корупцията. Именно тези корупционни практики имат сериозни последствия за обществото, като намаляване на доверието в институциите, намаляване на икономическия растеж, увеличаване на социалните неравенства и други.

За да бъде ефективна борбата с корупцията се изискват не само строги закони и мерки за предотвратяване, но и активно участие на обществото, както и отговорно поведение от страна на публичните служители.

Влиянието на корупцията върху обществото и икономиката на страната е значително и може да има сериозни последствия.

- Корупцията може да намали икономическия растеж, като засяга инвестициите, предприемаческата активност и ефективността на пазарите. Тя води до несправедлива конкуренция, недоверие и оттегляне на инвестиции.
- Корупцията води до неравностойно разпределение на богатството и властта в обществото. Това увеличава социалните неравенства и допринася за по-широкото обедняване на най-уязвимите общности.
- Корупцията може да засегне качеството на обществения живот чрез намаляване на достъпа до образование, здравеопазване, социални услуги и инфраструктура. Това води до намаляване на жизнения стандарт на гражданите.
- Корупцията подкопава доверието в институциите и правовата система на страната. Това затруднява развитието на справедливи и ефективни институции, които са необходими за устойчивото развитие на демократичното общество.
- Корупцията води до загуба на доверие в правителството, обществените институции и демократичния процес. Това влошава легитимността на правителството и институциите и подкопава демократичната стабилност на страната.
- Корупцията може да има негативно въздействие върху международния имидж на страната и да затрудни влизането й в международни икономически и политически организации.

Тези са само някои от основните последици, при които корупцията влияе на обществото и икономиката на страната и точно затова борбата с корупцията е от решаващо значение за устойчивото икономическо и социално развитие на страната.

Оценката на социалните, икономическите и политическите последици от корупцията в публичните администрации е от съществено значение за разбирането на нейното въздействие върху обществото. Затова някои от основните аспекти, които трябва да бъдат взети предвид са: Социални последици, Ограничен достъп до услуги, Икономически последици, Загуба на бизнес възможности, Политически последици, Нарушаване на доверието в институциите, както и Нарушаване на принципите на демокрацията.

Оценката на тези последици е важен елемент за разработването на стратегии за борба с корупцията и за изграждането на по-устойчиви и справедливи общества.

# 5 Стратегии за борба с корупцията

В последните години редица държави и международни организации са разработили различни стратегии за противодействие на корупцията, които включват:

- ✓ Институционални реформи – изграждане на независими органи за борба с корупцията, като комисии и специализирани прокуратури.
- ✓ Повишаване на прозрачността – въвеждане на електронни системи за управление на документи, публични регистри и онлайн платформи за обществено наблюдение.
- ✓ Обучение и етика – повишаване на квалификацията на служителите в публичната администрация, както и създаване на етични кодекси за поведение.
- ✓ Гражданско участие – стимулиране на активното участие на гражданите и неправителствените организации в процеса на наблюдение и сигнализиране на корупционни случаи.

Въпреки прилагането на различни мерки, борбата с корупцията често среща съпротива поради политически интереси, липса на воля за реформи и недостатъчна независимост на институциите. Ефективното противодействие на корупцията изисква не само прилагането на закони и регулации, но и дълбока културна промяна, която да насърчава интегритета и почтеността в публичния сектор.

# 6 Мерки за противодействие на корупцията

Включването на мерки за противодействие на корупцията в публичните администрации е важна част от стратегията за подобряване на управлението и изграждане на доверие в институциите. Ето някои ключови мерки, които се разглеждат в доклада**.**

Борбата с корупцията изисква комплексен подход и прилагането на различни мерки както на национално ниво, така и на ниво на публичните администрации.

- ❖ **Институционални реформи и изграждане на антикорупционни органи:**

*Независими антикорупционни агенции* – Създаването на специализирани агенции с независимост от политическо влияние, които имат мандат да разследват и предотвратяват корупционни престъпления. Примери за такива институции включват Националната агенция за борба с корупцията или антикорупционни комисии.

*Специализирани прокуратури и съдилища* – Учредяване на специални съдебни звена за корупционни дела, които могат да разглеждат такива престъпления по-ефективно и бързо.

❖ **Засилване на прозрачността и отчетността:**

*Електронно управление* – Въвеждане на електронни платформи за обществените поръчки, административни услуги и правителствени решения, които минимизират човешкия фактор и увеличават прозрачността на процедурите.

*Публичен достъп до информация* – Разработване на механизми за лесен достъп на гражданите до правителствени документи и бюджети, което дава възможност за мониторинг и предотвратяване на злоупотреби.

❖ **Подобряване на системите за вътрешен контрол:**

*Засилване на вътрешния одит* – Вътрешните одиторски звена трябва да бъдат усъвършенствани и да работят независимо за контрол на процедурите и финансовите потоци в публичните администрации.

*Усъвършенстване на системата за подаване на сигнали:(whistleblowing***)** – Насърчаване на подаването на сигнали за нередности чрез защитени и анонимни канали, както и гарантиране на защита на лицата, които докладват за корупционни практики.

❖ **Антикорупционно законодателство и санкции:**

*Строги закони срещу корупцията* – Приемане на ясно и всеобхватно законодателство, което предвижда ефективни и строги санкции срещу корупционни действия, включително конфискация на имущество, глобални глоби и затвор.

*Санкции за конфликт на интереси* – Усъвършенстване на законодателството за предотвратяване на конфликти на интереси и злоупотреба с власт от страна на длъжностни лица, включително забрани за заемане на публични длъжности след корупционни скандали.

❖ **Обучение и етични стандарти:**

*Обучение на служителите в публичния сектор* – Организиране на редовни обучения за държавните служители с акцент върху етиката, добрите практики и начините за идентифициране и предотвратяване на корупционни действия.

*Етични кодекси* – Въвеждане на етични кодекси за държавните служители, които да насърчават честността, отчетността и отговорността.

❖ **Активно участие на гражданското общество и медиите:**

*Граждански мониторинг* – Насърчаване на активното участие на гражданите, неправителствените организации и медиите в наблюдението на дейността на публичните администрации. Това включва създаване на механизми за обществено отчитане и обратна връзка.

*Партньорства с международни организации* – Сътрудничество с международни антикорупционни институции като Transparency International и Организацията за икономическо сътрудничество и развитие (ОИСР) за въвеждане на добри практики и обмен на опит.

Тези мерки са основополагащи за изграждането на ефективна стратегия за борба с корупцията в публичните администрации и трябва да се изпълняват в комбинация и в сътрудничество с международната общност и другите заинтересовани страни, за да се постигне значително подобрение в борбата с корупцията в публичната администрация.

За да се прегледат съществуващите и предложени мерки за противодействие на корупцията, може да се използва системен подход, който да включва следните етапи:

*Анализ на текущото състояние*: Преглед на действащото законодателство, институционалната рамка и мерките, вече предприети за борба с корупцията. Изследване на случаи на корупция и причините за тяхното възникване. Оценка на ефективността на вече приложените мерки и програми.

*Изследване на добри практики и предложени решения:* Преглед на успешни примери от други държави или региони, които са били ефективни в борбата с корупцията. Консултиране с международни организации, неправителствени организации и експерти, които имат опит в областта на антикорупцията.
*Идентифициране на слабите места и нуждите:* Анализ на основните причини за възникването на корупция и установяване на слабите места в институционалната рамка и законодателството.
Изследване на областите, в които наличието на корупция е най-голямо и къде са необходими допълнителни мерки за противодействие.
*Формулиране на предложения и решения*: Разработване на конкретни предложения за подобряване на законодателството и институционалната рамка. Изготвяне на програми и мерки за подкрепа на антикорупционни инициативи и проекти. Установяване на механизми за наблюдение и оценка на приложените мерки и програми.
*Имплементация и мониторинг*: Изпълнение на предложените мерки и програми за противодействие на корупцията. Постоянен мониторинг на прилагането на мерките и оценка на тяхната ефективност. Въвеждане на корекции и промени в случай на необходимост.
*Обществено участие и участие на гражданското общество:* Активно включване на гражданското общество, бизнес сектора и други заинтересовани страни в процеса на борба с корупцията. Подкрепа и насърчаване на участие на гражданите и неправителствените организации в контрола и наблюдението на дейностите на публичните институции.

Този цикъл на анализ, планиране, изпълнение и мониторинг може да бъде непрекъснат и постоянно подобряван във времето, за да се гарантира ефективността на мерките за противодействие на корупцията.

Подобряването на законодателството за борба с корупцията е ключов елемент за ефективната борба с този сериозен проблем. Ето няколко препоръки за подобряване на законодателството:
*Строги санкции и прозрачност*: Законите трябва да предвиждат строги санкции за корупционните престъпления, като същевременно осигуряват ясни и прозрачни процедури за тяхното прилагане. Тези санкции трябва да бъдат пропорционални и ефективно да отвличат от крайните цели на корупционните дейци.
*Създаване на независими институции*: Важно е да се създадат независими институции за борба с корупцията, които да разполагат с достатъчни ресурси и власт за провеждане на редовни и неутрални разследвания.
*Усъвършенстване на системата за деклариране на имущественото състояние на държавните служители*: Законодателството трябва да изисква пълна прозрачност по отношение на имуществото на държавните служители и да налага строги мерки за наказание на тези, които не спазват задължението си да декларират своето имущество.
*Подкрепа за жертвите на корупцията*: Законодателството трябва да предвижда мерки за подкрепа на лицата, които са станали жертви на корупцията, включително механизми за компенсация и защита на техните права.
*Укрепване на ролята на гражданското общество и медиите*: Законодателството трябва да насърчава активното участие на гражданското общество и медиите в борбата с корупцията, като осигурява защита на техните права и свободи.

*Международно сътрудничество*: Законодателството трябва да предвижда мерки за укрепване на международното сътрудничество в борбата с корупцията, включително обмен на информация и доказателства между различни държави.

Тези препоръки представляват само начало и трябва да се приложат в съчетание с други мерки и стратегии за борба с корупцията, за да се постигне истинска промяна в обществото.

# 7 Заключение

Докладът предоставя анализ на състоянието на корупцията в публичните администрации, като разглежда разпространеността, възникването, вида, последиците и мерките за борба с нея. Някои от ключовите изводи и наблюдения от доклада включват:

- Корупцията е разпространен проблем, който засяга различни сектори и институции в публичната администрация.
- Тя има сериозни икономически, социални и политически последици за обществото и икономиката на страната.
- Законодателството и институционалната рамка за борба с корупцията са от решаващо значение за ефективното й преодоляване.
- Важно е да се идентифицират слабите места в системата и процесите, които улесняват корупцията, и да се предприемат съответните мерки за тяхното подобряване.
- За борба с корупцията е необходимо да се прилагат комплексни мерки, които включват както законодателни промени, така и подкрепа за общественото мнение и гражданското общество.
- Изготвеният доклад представлява важен инструмент за разбиране на проблема с корупцията и може да бъде използван като основа за разработване на стратегии и мерки за нейното преодоляване в публичните администрации.

Борбата с корупцията в публичните администрации изисква систематичен и многопластов подход, който включва институционални реформи, повишаване на прозрачността и отчетността, както и активно гражданско участие. Успехът на тези усилия зависи от политическата воля, обществената подкрепа и международното сътрудничество. За да се постигнат устойчиви резултати, е необходимо продължително наблюдение и адаптиране на прилаганите стратегии в зависимост от конкретните обстоятелства и контексти.

**ЛИТЕРАТУРА:**

[1] Груев, Л, Велчев, Б. (2000). Наказателно правни аспекти на борбата с корупцията. София.

[2] Диманова, Д., Управление на риска, УИ „Епископ Константин Преславски“, Шумен, 2016, ISBN: 978-619-201-095-9.

[3] Metodieva, Ts. Problems of the economic development of Bulgaria, SocioBrains, бр. 89, January, 2022. pp. 148-150, ISSN: 2367-5721. http://sociobrains.com.

[4] Методиева, Ц. Парашкеванова, Г., Махмуд, А. " Заплахи в интернет. Фишинг и финансово муле.", международна научна конференция „Киберсигурността в информационното общество“, НВУ „Васил Левски“ факултет „Артилерия, ПВО и КИС“ - гр.Шумен, 20-21 Април 2017г., ISBN 978-954-9681-82-6, с. 157- 160

[5] Ненов, И. (1999). Въведение в особената част на наказателното право. Престъпления против републиката. Лекция. Варна

[6] Слатински, Н. (2010). Петте нива на сигурност. София.

[7] Закон за администрацията, обнародван с ДВ. бр. 130 от 05.11.1998 г., последно изменен и/или допълнен с ДВ бр. 33 от 12.04.2024 г.

[8] Закон за вътрешния одит в публичния, обнародван с ДВ. бр. 27 от 31.03.2006 г., последно изменен и/или допълнен с ДВ бр. 100 от 20.12.2019 г.

# BEST PRACTICE FOR ENDPOINT SECURITY*

**DENIS I. ZVEZDELINOV, DIMITAR N. GRESHKOV**

***ABSTRACT:*** *As technology advances faster and faster in our modern world, endpoint penetration also increases - from mobile devices to IoT gadgets. That poses a significant challenge for organizations to mitigate risks and achieve better security overall. The best strategies to deal with endpoint penetration include the use of advanced endpoint detection and response (EDR) solutions with monitoring, regular software updates and zero-trust security user profiles. Additionally, the education of users for security mindfulness is crucial as human factor is the lead problem with security penetration.*

***KEYWORDS:*** *endpoint security, risk mitigation, monitoring, human factor*

***DOI: https://doi.org/10.46687/CGCF1904***

# НАЙ-ДОБРИ ПРАКТИКИ ЗА СИГУРНОСТ НА КРАЙНИТЕ УСТРОЙСТВА

**ДЕНИС И. ЗВЕЗДЕЛИНОВ, ДИМИТЪР Н. ГРЕШКОВ**

***АБСТРАКТ:*** *С все по-бързото развитие на технологиите в нашия модерен свят, пробиването на крайни устройства също нараства - от мобилни устройства до IoT устройства. Това е голямо предизвикателство за организации да управляват риска и да подобрят своята сигурност като цяло. Най-добрите стратегии за справяне с пробиването на крайни устройства включват използването на усъвършенстван софтуер с мониторинг и отговор за опит за пробив на крайни устройства (EDR), чести актуализации на софтуера и потребителски профили със сигурност на ниво "нулево доверие". Допълнително, подготовката на потребителите за повишено внимание към сигурността е ключова, защото човешкият фактор е главният проблем, когато става дума за пробиви в сигурността.*

## 1 Въведение

В днешния дигитализиран свят, крайните устройства (т. нар. "endpoint") - например лаптопи и смартфони - са портите, през които се изпълняват повечето кибератаки. Докато работенето от разстояние става все по-често срещано и киберпрестъпниците разработват все по-усъвършенствани тактики, подсигуряването на тези устройства става все по-важно.

През 2023 година голяма финансова институция страда от опустошително нарушение на данните, което струва милиони и значително наранява нейната репутация, само заради едно компрометирано крайно устройство [8]. Подобни инциденти подчертават спешността да се приложат висококачествени мерки за сигурност на крайните устройства. Със съществуването на регулации като GDPR, които налагат строги изисквания относно това как данните се управляват и защитават, сигурността на крайните устройства става не само най-добра практика, но и законно необходимо. Неуспешното подсигуряване на крайните устройства може да доведе до големи глоби, губене на доверието на потребителя, и дори до съдебни дела.

В ранните дни на компютърния свят, сигурността на крайните устройства е представлявала антивирусен софтуер и прости защитни стени (т. нар. "firewall"). Но с

* Докладът е финансиран по проект № РД-08-147/02.02.2024 г., „Усъвършенстване на способностите за създаване на сценарий за тестване на уязвимости в симулационен оперативен център за сигурност"

напредването на технологиите, заплахите също стават все по-развити. Въпреки бързото развитие на технологиите за киберсигурност, човешката грешка продължава да бъде водещият фактор при нарушенията на данни. Много от слабостите на крайните устройства произхождат от прости грешки като кликване на злонамерени линкове или слаби пароли.

Целта на изложението е да покаже начините за изграждане на многослоен подход за подсигуряване на крайните устройства, отнасящ се както до технологичните, така и до човешките фактори.

## 2 Изложение

Кибератаките, насочени към крайните устройства, могат да доведат до огромни финансови загуби. Според скорошни изследвания, средната загуба от нарушаване на целостта на данните надвишава милиони долари, като по-малките организации са изложени на най-голям риск [4,7]. За да се намали рискът от нарушение с катастрофални последици, организациите трябва да комбинират силните технологични защити с обширни програми за обучение на служителите.

Внедряването на EDR (EDR – Endpoint Detection and Response) решения за крайните устройства е най-важният и лесен начин за предотвратяване на тяхното пробиване. Въпреки че са сравнително скъпи системи, ползите от EDR са огромни, особено за малки организации, които нямат възможност да назначат специалисти по киберсигурност. С голям набор от технологии, EDR позволява непрекъснат мониторинг, откриване на заплахи и отговор на заплахата в реално време. Цялата тази автоматизация освобождава цели екипи специалисти от рутинни задачи и, ако организацията разполага с такива, им позволява да обърнат вниманието си към по-сериозни задължения. Освен бързо откриване на заплахата и реагиране, още позволяват за следене на активността на устройствата - стартиране на приложения, промени във файлове и мрежова активност. Още, след инцидент инструментите на EDR помагат за извършване на анализ на причините и установяване на други уязвимости в системата. Най-използваните EDR решения са CrowdStrike Falcon, Trend Micro XDR, Sentinel One, Microsoft Defender for Endpoint и др. Наборът от технологии на EDR включва антивирусна защита от следващо поколение (NGAV – Next-Generation Antivirus), основата на EDR решенията. NGAV анализира поведението на файлове и приложения чрез изкуствен интелект и/или машинно обучение за адаптиране към заплахи в реално време. Правят анализ на контекста на активността в мрежата, за да идентифицират потенциалните заплахи като следи взаимодействията между приложенията, потребителите и самите крайни устройства. Ако се открие заплаха, предприемат се автоматично действия – блокиране и изолация на злонамерени файлове и пробити устройства, за да се минимизира риска от разпространение. Наборът инструменти на EDR включва и система за информация за защита и управлението на събития (SIEM – Security Information and Event Management). Те събират, анализират и сравняват данни от крайните устройства за цялостен поглед на състоянието на защитата на мрежата, правят мониторинг на събития и анализ на инциденти в реално време. Още позволяват и централизирано наблюдение на всички крайни устройства в мрежата, управлява инцидентите и оптимизира ресурсите, за да няма притеснение от фалшиви положителни сигнали за пробив. Използва се и защита от загуба на данни (DLP – Data Loss Prevention), която идентифицира чувствителна информация и осигурява нейната защита. Заедно тези технологии се допълват и най-често EDR решенията са съвкупност или хибрид от изброените.

EDR ни предлага няколко системи събрани в една, но има още начини за добавяне на допълнителни слоеве за сигурност, като нещо задължително за високопоставени

длъжности в организации - многофакторната автентикация (MFA). Вече има много начини за прихващане на двуфакторната автентикация (2FA). Например, при онлайн банкиране и плащане, банките преди искаха само CVV кода на картата, който може много лесно да се прихване с пробиване на крайното устройство. След това направиха система за двуфакторна автентикация като допълнително изпращаха SMS с код на указания телефонен номер, който да послужи за автентицирането. С напредването на технологиите обаче стана много лесно да се пробиват дори и клетъчните комуникации, да се прихващат обаждания и SMS-и без знанието на крайният потребител или сигнал от крайното устройство. Затова банките решиха да преминат към многофакторна автентикация, като сега изискват създаването на статичен ПИН-код като допълнение към CVV код и SMS с код. Вече стана обща практика на много места да се изисква многофакторна автентикация, като поне един фактор трябва да бъде биометричен, за да не може да се пробие лесно крайното устройство. При интегриране на двуфакторна или многофакторна автентикация за достъп до крайните устройства се добавя много сериозен слой защита. Така само даденият потребител, чрез пръстов отпечатък или лицево разпознаване има достъп до лаптоп, смартфон или работна станция в дадената организация.

Архитектурата нулево доверие (ZTA – Zero Trust Architecture) е модерна рамка за киберсигурност, която предизвиква традиционната представа за доверие на потребители или устройства въз основа на тяхното местоположение в периметъра на мрежата. В традиционния модел на сигурност на потребителите или устройствата в мрежата на организацията често се предоставя имплицитно доверие, но този подход е станал неадекватен, тъй като организациите все повече приемат облачни услуги, мобилни устройства и отдалечени работни среди. Zero Trust работи на принципа “никога не вярвай, винаги проверявай”, което означава, че всеки потребител, устройство и връзка трябва да бъдат удостоверени и оторизирани, преди да получат достъп до който и да е ресурс, независимо дали са вътре или извън периметъра на мрежата. В основата на Zero Trust е идеята за непрекъсната проверка. Вместо да предоставя широк достъп въз основа на еднократна проверка, Zero Trust непрекъснато оценява състоянието на сигурност на устройството и потребителя. Това включва проверка на самоличността, проверка на изправността на устройството и оценка на контекстна информация като местоположението на потребителя и часа на заявката за достъп. Дори след като даден потребител получи достъп, поведението му се наблюдава непрекъснато, за да се открият аномалии или подозрителна дейност, които биха могли да бъдат знак за пробив в сигурността. Това наблюдение в реално време намалява риска от вътрешни заплахи или компрометирани идентификационни данни, водещи до неоторизиран достъп.

Ключов компонент на Zero Trust е микросегментирането, което включва разделяне на мрежата на по-малки зони и ограничаване на достъпа до специфични ресурси на принцип “необходимост да се знае”. Вместо да позволи на потребителите да се движат свободно в мрежата, след като бъдат удостоверени, Zero Trust позволява достъп само до ресурсите, необходими за тяхната роля. Това минимизира потенциалните щети, ако нападател наруши мрежата, тъй като той би бил ограничен до определена зона с непълен достъп, намалявайки повърхността на атака. Внедряването на Zero Trust изисква комбинация от многофакторно удостоверяване (MFA), криптиране, сигурност на крайното устройство и решения за управление на самоличността. Интегрирането на тези технологии гарантира, че всички заявки за достъп са проверени, наблюдавани и контролирани. Zero Trust е особено полезен в съвременни ИТ среди, където потребителите често имат достъп до ресурси от различни местоположения и устройства, като настройки за отдалечена работа или базирани на облак

приложения. Чрез премахване на имплицитното доверие, дадено на вътрешните потребители и устройства, организациите, използващи архитектурата Zero Trust, могат значително да подобрят своята сигурност и да защитят чувствителните данни в среда на динамични заплахи.

Друг задължителен слой на защита на крайните устройства трябва да бъде мрежовата сигурност. С днешните технологии, които се развиват непрестанно все повече устройства оперират само на Wi-Fi, без опция за LAN връзка. Това означава, че е добре да се подсигури локалната мрежа на дадената организация. Представете си една голяма организация с широко мрежово покритие, където се връзват телефони, лаптопи, компютри, принтери и всякакви други IoT устройства, които при проникване само при едно крайно устройство стават уязвими. Цял клъстър от устройства могат да бъдат сринати за минути, заедно със самата мрежа. За тази цел може да се използва виртуална частна мрежа (VPN). Така се осигурява сигурна и криптирана връзка между крайните устройства и IoT - чрез създаването на защитен тунел, като се получава допълнителен слой за защита на данните от несанкциониран достъп и пази анонимността на потребителите. Освен криптирането на данните, скрива се реалният IP адрес на устройствата, а и може безопасно служители да качват и свалят данни отдалечено ако имат контрол на достъпа. Тук може да се прибавят и виртуални локални мрежи (VLAN) за още един слой на мрежова сигурност. Още познато като сегментация на мрежата, това е техника за управление на мрежов трафик, която разделя голяма мрежа на по-малки. Така се постига по-добро управление на хардуерни мрежови ресурси и защита на данни.

Човешкият фактор е причината за огромна част от проблемите, свързани със сигурността на крайните устройства [3]. За да се преодолее този проблем е нужен многостранен подход, състоящ се от образоване на служителите, политики на работа, както и технологии, предназначени да сведат до минимум слабостите, причинени от потребителя. Един от най-ефикасните начини за справяне с проблема с човешкия фактор е цялостно обучаване за осведоменост относно сигурността [6]. Служителите трябва редовно да бъдат тренирани, за да могат да разпознават опити за фишинг, да избягват подозрителни линкове, да създават силни пароли, които не са записани никъде, и да следват протоколи за правилно управление на данните [5]. Чрез въоръжаването на работниците със знания, организациите могат значително да ограничат риска от пробив в сигурността, предизвикан от човешка грешка.

В допълнение към обучението, прилагането на строги политики за сигурността е от съществено значение за намаляването на рисковете, свързани с човешкия фактор. Организациите трябва да изискват използването на силни пароли, както и многофакторна автентикация във всички системи и приложения. Редовната смяна на паролите трябва да бъде задължителна и достъпът до чувствителна информация трябва да бъде ограничен на основата на служителските роли, следвайки принципа на най-малко привилегии.

Освен това трябва да има ясни правила, които да регулират използването на лични устройства за работа, поради факта, че тяхното използване може да доведе до слабости в сигурността [1]. Това се постига чрез управление на мобилни устройства (MDM - Mobile Device Management). MDM представлява комбинация от софтуерни решения за подсигуряване на устройствата, както и фирмени политики, чрез които се регулира достъпа до чувствителна информация. По този начин се ограничава риска от нарушаване на данните. Това е важна част от сигурността на крайните устройства, понеже тези устройства лесно могат да бъдат загубени или откраднати.

Сигурността на крайните устройства играе основна роля при спазването на GDPR (General Data Protection Regulation - Общ регламент относно защитата на данните) и колекцията от стандарти ISO/IEC 27000, като и двете подчертават значението на защитата на личните данни и сигурността на информационните системи. Сигурността на крайните устройства е от голямо значение, тъй като те често стават входни точки за кибератаки.

Съгласно GDPR организациите, които обработват лични данни на граждани на ЕС, са длъжни да прилагат подходящи технически и организационни мерки, за да гарантират сигурността на тези данни. Сигурността на крайните устройства е ключов елемент от тези мерки, тъй като те често са най-слабото звено във веригата за сигурност. GDPR не описва конкретни технологии, а вместо това налага основан на риска подход към сигурността на данните. Това означава, че организациите трябва сами да оценят рисковете, свързани с техните крайни устройства, и да предприемат необходимите стъпки за тяхното ограничаване, като например криптиране на данните, съхранявани на крайни устройства, прилагане на системи за контрол на достъпа, както и често актуализиране на софтуера на тези устройства. От организациите също се изисква да прилагат защита на данните "на етапа на проектирането" и "по подразбиране", като гарантират, че мерките за защита на данните, включително тези, свързани с крайни устройства, са интегрирани в техните системи още от най-ранните етапи от проектирането.

Стандартът ISO/IEC 27001, който очертава изискванията за една система за управление на информационната сигурност (СУИС), също подчертава значението на сигурността на крайното устройство. Организациите, търсещи сертификат по ISO 27001, трябва да идентифицират рисковете, свързани с информационната сигурност - включително рисковете, породени от крайните устройства - и да прилагат контролни дейности за управление на тези рискове [2]. Приложение А към ISO 27001 съдържа специфични контроли, свързани със сигурността на крайното устройство. Един ключов аспект на ISO 27001 е изискването за редовни оценки на риска и прилагането на мерки за ограничаване на риска. Освен това ISO 27001 подчертава важността на обучаването за информираност на служителите.

ISO/IEC 27002 предоставя допълнителни насоки за прилагане на контролите за сигурност. Той предлага специфични мерки за сигурност на крайното устройство, като например криптиране на информацията и контролиран достъп. Този стандарт е в съответствие с изискванията на GDPR за защита на личните данни, което го прави полезна рамка за организации, които търсят както съответствие с GDPR, така и ISO сертифициране.

## 3 Заключение

Подсигуряването на крайните устройства е от основно значение за предпазването на чувствителна информация от заплахи. Прилагането на най-добри практики за сигурност, като например непрекъснат мониторинг, многофакторна автентикация и редовно обучаване на служителите, може значително да ограничи рисковете, свързани с човешка грешка и технически слабости. Спазването на регулациите гарантира всеобхватен подход към проблема със сигурността на крайните устройства.

**ЛИТЕРАТУРА:**

[1] Таиров, И. Управление на мобилните устройства като компонент на корпоративната информационна инфраструктура (2019).

[2] Dimanova, D., Kuzmanov, Z., Risk management in information security, Conference proceedings MATTEX 2018. Information, Technical and Economical Problems of Security Systems, October 2018, Shumen, ISSN: 1314-3921, vol. 2, part. 1, pp. 139-145.

[3] IBM Global Technology Services. 2014 Cyber Security Intelligence Index (май 2014).

[4] IBM Security. Cost of a Data Breach Report 2024.

[5] Nixon, J., McGuinness, B. Framing the human dimension in cybersecurity. European Alliance for Innovation Endorsed Transactions on Security and Safety (2013), с. 5.

[6] Ogundare, E. The human factor in cyber security. TECHiT (март 2024).

[7] Rahmonbek, K. 35 Alarming Small Business Cybersecurity Statistics for 2024 (1 февруари 2024).

[8] Vibert, R. The Biggest Financial Data Breaches in 2023. Metomic (23 септември 2024).

# PHISHING ATTACKS – DETECTION AND PROTECTION*

**YOVKO M. HRISTOV, DESISLAV M. HRISTOV**

***ABSTRACT:*** *Phishing attacks are a type of cybercrime where fraudsters use social engineering to obtain confidential information from users, such as passwords and personal data. These attacks typically involve fake emails and websites that mimic legitimate organizations. Key methods of protection include two-factor authentication, antivirus software, and raising user awareness. Education and good practices in online communication play a crucial role in preventing phishing attacks.*

***KEYWORDS:*** *phishing attacks, social engineering, cybersecurity, websites, e-mail*

***DOI: https://doi.org/10.46687/MNRB8162***

# ФИШИНГ АТАКИ – РАЗПОЗНАВАНЕ И ЗАЩИТА

**ЙОВКО М. ХРИСТОВ, ДЕСИСЛАВ М. ХРИСТОВ**

***АБСТРАКТ:*** *Фишинг атаките са вид киберпрестъпления, при които измамници използват социално инженерство, за да получат конфиденциална информация от потребителите, като пароли и лични данни. Те обикновено включват фалшиви имейли и уебсайтове, които имитират легитимни организации. Основните методи за защита включват двуфакторна автентификация, антивирусен софтуер и повишаване на информираността на потребителите. Образованието и добрите практики в онлайн комуникацията играят ключова роля в превенцията на фишинг атаките.*

## 1 Въведение

Целта на този доклад е да предостави цялостен преглед на фишинг атаките – една от най-често срещаните и опасни форми на киберпрестъпност. Ще бъдат разгледани различните техники, използвани от атакуващите за измама на потребители и организации с цел получаване на чувствителна информация, като лични данни, пароли и финансова информация. Освен това, докладът ще предложи стратегии и мерки за защита, които могат да помогнат на индивидите и компаниите да се предпазят от подобни атаки. Разпознаването на признаците на фишинг и предприемането на превантивни действия ще бъдат основни акценти, като целта е да се повиши информираността и способността за защита срещу тези киберзаплахи. [1]

## 2 Дефиниция за фишинга

Фишинг атаките представляват вид киберизмама, при която нападателите се опитват да измамят потребителите, за да получат достъп до чувствителна информация като потребителски имена, пароли, банкови данни или друга лична информация. Това обикновено се постига чрез изпращане на фалшиви имейли, съобщения или създаване на копия на легитимни уебсайтове, които изглеждат автентични, но целят да заблудят жертвата. [1]

Фишинг атаките са опасни, защото могат да доведат до сериозни последствия като кражба на самоличност, финансови загуби и достъп до лични или корпоративни данни,

* Докладът е финансиран по проект № РД-08-147/02.02.2024 г., „Усъвършенстване на способностите за създаване на сценарий за тестване на уязвимости в симулационен оперативен център за сигурност“

които могат да бъдат използвани за по-нататъшни атаки или измами. Те са трудни за разпознаване и представляват значителна заплаха както за индивидуалните потребители, така и за бизнеса.

Разпознаването и предотвратяването на фишинг атаки е от ключово значение както за индивидуалните потребители, така и за организациите, защото тези атаки могат да доведат до сериозни финансови загуби, кражба на лични данни и компрометиране на сигурността. За потребителите фишинг атаките често водят до кражба на самоличност, източване на банкови сметки и злоупотреба с лична информация.

За организациите рисковете са дори по-големи – успешните фишинг атаки могат да отворят врати за по-мащабни кибератаки, като пробиви в корпоративни мрежи, кражба на бизнес данни или изнудване. В резултат, това може да доведе до загуба на доверие от клиенти, глоби за неспазване на регулации и сериозни щети върху репутацията. Ето защо е от жизненоважно значение всички да бъдат информирани и предпазливи, за да могат да разпознават фишинг опитите и да предприемат мерки за защита.

# 3 Какво представляват фишинг атаките?

Фишингът като техника за измама възниква в средата на 90-те години, когато интернет започва да става масово достъпен. Първоначалните фишинг атаки са насочени към потребителите на популярни платформи като AOL (America Online). Хакерите използват фалшиви имейли и съобщения, за да измамят потребителите да разкрият паролите си и лична информация. През това време терминът "фишинг" се появява, произхождайки от думата "fishing" (риболов), тъй като нападателите "ловят" жертвите с измамни примамки.

С развитието на интернет и електронната търговия, фишингът еволюира и стана по-сложен. През 2000-те години той започва да се разпространява чрез имейли, прикрити като съобщения от банки, онлайн търговци и популярни социални мрежи. Техниките се усъвършенстват, включително насочени атаки (spear phishing), които използват персонализирани съобщения за по-голяма ефективност.

През последните години фишинг атаките стават още по-сложни и широко разпространени с появата на нови платформи за комуникация, като социални мрежи и приложения за съобщения, както и с използването на методи като "whaling" (насочени атаки към високопоставени лица) и "clone phishing" (клониране на легитимни съобщения). Тази еволюция прави фишинга една от най-значимите и персистиращи заплахи в киберпространството.

**Основни цели на фишинга**

Фишинг атаките имат няколко основни цели, които са насочени към получаване на чувствителна информация или достъп до ресурси на жертвите. Ето някои от ключовите цели:

- кражба на лични данни: една от най-честите цели на фишинг атаките е събирането на лични данни като име, адрес, телефонен номер и дори ЕГН. Тази информация може да бъде използвана за кражба на самоличност или за създаване на фалшиви акаунти.

- кражба на потребителски имена и пароли: атакуващите често се опитват да измамят жертвите да разкрият своите потребителски имена и пароли за достъп до електронни пощи, социални мрежи или други онлайн услуги. След това тези данни могат да бъдат използвани за пробив в акаунтите и извършване на престъпления от тяхно име.

- достъп до банкови данни: много фишинг атаки са насочени към измама на жертвите да предоставят своите данни за банкови карти, номера на сметки или данни за онлайн

банкиране. Това може да доведе до директни финансови загуби за жертвата, като парите бъдат изтеглени или прехвърлени.

- компрометиране на корпоративни системи: в корпоративна среда целта на фишинга може да бъде получаване на достъп до вътрешни мрежи, бази данни и системи, което може да доведе до големи загуби за организацията. Атакуващите могат да използват достъп до корпоративни имейли за кражба на бизнес информация, индустриален шпионаж или изнудване.

- инсталиране на зловреден софтуер: фишинг атаките често се използват за разпространение на зловреден софтуер, като вируси, троянски коне или рансъмуер. Тези програми могат да заразят компютрите на жертвите, като предоставят на нападателите достъп до тяхната информация или блокират достъпа, докато не бъде платен откуп.

Основната цел на фишинг атаките е да измамят жертвите да предоставят ценни ресурси, които след това могат да бъдат използвани за финансови измами, изнудване или по-нататъшни киберпрестъпления.

Фишинг атаките могат да засегнат всеки, но някои групи са по-уязвими поради липса на информираност, ресурси за защита или специфични слабости в техните системи. Ето кои са най-уязвимите групи:

- Обикновени потребители:

Причини за уязвимост: Липса на киберсигурност знания и неспособност да разпознаят фалшиви съобщения или уебсайтове. Те често не прилагат практики като многофакторна автентикация или използване на силни пароли.

Тип атаки: Обикновените потребители са най-често мишена за фишинг имейли, насочени към кражба на лични данни или достъп до онлайн акаунти, социални медии и банкови сметки.

- Малки бизнеси:

Причини за уязвимост: Малките бизнеси често разполагат с ограничени ресурси за киберсигурност и обучения на персонала, което ги прави уязвими на фишинг атаки. Липсата на специализирани ИТ отдели и защитни системи също увеличава риска.

Тип атаки: Нападателите могат да използват фишинг, за да получат достъп до финансови и бизнес данни, както и да компрометират електронната поща на служителите. Често срещани са атаките чрез имейли, които изглеждат като изпратени от бизнес партньори или клиенти.

- Големи организации:

Причини за уязвимост: Въпреки че големите организации обикновено имат по-сложни системи за киберсигурност, тяхната мащабност и многобройният персонал създават повече точки за потенциални атаки. Големите компании също така съхраняват повече чувствителни данни, което ги прави примамлива цел.

Тип атаки: Големите организации често са жертва на насочени фишинг атаки (spear phishing), при които нападателите персонализират съобщенията с цел компрометиране на конкретни служители или отдели. "Whaling" атаки, които са насочени към ръководни кадри, също са често срещани.

- Други уязвими групи:

Служители в здравни и финансови сектори: Тези индустрии са особено уязвими поради обема на чувствителна информация, която обработват, и стриктните регулации, които трябва да спазват.

Държавни институции: Често мишена за атаки, свързани с шпионаж или дестабилизация, тъй като те обработват критична информация.

Всички тези групи трябва да бъдат внимателни и да прилагат съвременни мерки за защита, за да намалят риска от фишинг атаки. [5]

# 4 Често срещани техники за фишинг

а) Имейл фишинг:

- Описание: Имейл фишингът е най-разпространената форма на фишинг, при която нападателите изпращат фалшиви имейли, които изглеждат като съобщения от легитимни организации или служби. Целта е да измамят получателя да предостави чувствителна информация, като пароли, банкови данни или да кликне върху зловреден линк.

- Как работи: Имейлите често съдържат съобщения, които предизвикват спешност например: фалшиви известия за сигурност, фалшиви фактури или уведомления за проблеми с акаунт. Те могат да включват линкове към фалшиви уебсайтове, където жертвата въвежда своите данни.

- Защо е ефективен: Тази техника разчита на психологически манипулации като страх и спешност, което води до бързо вземане на решения от страна на жертвата, без тя да се замисли за достоверността на съобщението. [6]

б) Spear фишинг:

- Описание: Spear фишингът е по-целенасочена форма на фишинг атака, която е насочена към конкретни индивиди или организации. Атакуващите персонализират имейлите или съобщенията въз основа на наличната информация за жертвата, за да изглеждат легитимни.

- Как работи: Атакуващите често използват информация от социални мрежи, корпоративни уебсайтове или публично достъпни данни, за да създадат доверие у жертвата. Те могат да се представят като колега, партньор или дори клиент, за да накарат жертвата да предостави ценна информация или да кликне на зловредна връзка.

- Защо е ефективен: Персонализацията увеличава доверието и е по-трудно да бъде разпозната измамата, тъй като жертвата вярва, че комуникира с легитимен източник. [2]

в) Smishing и Vishing:

- Smishing:

• Описание: Smishing (SMS фишинг) е фишинг атака, която използва текстови съобщения, за да измами потребителите да разкрият чувствителна информация или да кликнат на зловреден линк.

• Как работи: Съобщенията обикновено съдържат известия за фалшиви награди, промоции или сигнали за сигурност и често включват линкове към фалшиви уебсайтове.

- Vishing:

• Описание: Vishing (Voice фишинг) използва телефонни обаждания, за да подмами жертвите да разкрият чувствителни данни или да извършат финансови операции.

• Как работи: Атакуващите се представят като представители на банки, държавни институции или техническа поддръжка и използват социална инженерия, за да убедят жертвата да предостави пароли, банкови данни или друга информация.

• Защо са ефективни: И двете техники разчитат на бързото действие на жертвата. Телефонните и текстовите съобщения създават усещане за доверие или спешност, което води до по-лесна манипулация. [6]

г) Clone фишинг:

- Описание: При clone фишинг атаката нападателите копират легитимни имейли или съобщения, които жертвата вече е получавала, и заменят съдържанието или прикачените файлове със зловредни версии.

- Как работи: Атакуващите използват имейл, който жертвата вече е получила от доверен източник, и го клонират, като същевременно добавят зловредни линкове или прикачени файлове. Имейлът изглежда почти идентичен с оригинала, което затруднява жертвата да открие измамата.

- Защо е ефективен: Тази техника разчита на доверието, което вече е изградено от оригиналния имейл. Жертвата е по-малко подозрителна, тъй като съобщението изглежда познато.

д) Whaling:

- Описание: Whaling е специфична форма на spear фишинг, насочена към високопоставени личности в организацията, като изпълнителни директори, мениджъри и бизнес лидери.

- Как работи: Атаките обикновено се представят като важни бизнес комуникации или легални документи, като напр. фактури, договори или данъчни формуляри. Целта е да се излъжат тези лица да разкрият чувствителна информация или да извършат важни финансови операции.

- Защо е ефективен: Високопоставените личности имат достъп до ключова информация и ресурси в организацията, което прави успешната атака срещу тях особено разрушителна. Освен това, тяхното натоварено ежедневие може да доведе до по-малко внимание при проверка на съобщенията.

Тези техники за фишинг са успешни, защото разчитат на манипулация на доверието и чувството за спешност. Защитата срещу тях изисква информираност и прилагане на добри практики за киберсигурност.

# 5 Разпознаване на фишинг атаки

а) Признаци на фалшиви имейли:

Фишинг имейлите често имат редица характеристики, които ги правят разпознаваеми. Ето някои от най-често срещаните признаци:

- Необичайни линкове: Линковете в фишинг имейлите може да изглеждат легитимни, но ако се задържи курсорът върху тях, ще се покаже реалният URL адрес. Често има малки промени в домейните (например „bank-secure.com“ вместо „bank.com“), които могат да бъдат трудно забележими.

- Неправилна граматика и правопис: Фишинг имейлите често съдържат граматически грешки или необичаен синтаксис, който не е типичен за легитимни компании. Това е ясен сигнал, че имейлът може да не е автентичен.

- Необичайни или нетипични изпращачи: Имейл адресът на изпращача може да изглежда легитимен на пръв поглед, но ако се разгледа по-внимателно, може да се забележат дребни изменения в името или домейна. Например, вместо „support@company.com“, може да има „support@company1.com“ или „@companny.com“.

- Неочаквани прикачени файлове или линкове: Легитимни компании рядко изпращат прикачени файлове в непоискани имейли. Прикачени файлове с разширения като ".exe", ".zip" или ".doc" могат да съдържат зловреден софтуер.

- Спешни съобщения или заплахи: Фишинг имейлите често се опитват да създадат чувство на спешност, като твърдят, че акаунтът ви ще бъде заключен или че сте пропуснали важен платеж, за да ви накарат да действате бързо и неразумно. [3]

б) Фалшиви уебсайтове:

Фалшивите уебсайтове се създават така, че да изглеждат идентични или много близки до оригиналните, но има начини да бъдат разпознати:

- Разлики в URL адресите: Фалшивите уебсайтове обикновено имат URL адреси, които изглеждат почти идентични с оригиналните, но съдържат малки изменения. Пример може да е „www.bank-login.com“ вместо „www.bank.com“. Потребителите трябва винаги да проверяват внимателно URL адреса, особено преди да въведат лични данни.

- Липса на сертификати за сигурност: Легитимните уебсайтове използват SSL сертификати, което се обозначава с „https://“ преди URL адреса и иконка на заключен катинар в адресната лента. Ако уебсайтът не разполага с тези символи, това е сигнал за потенциална измама.

- Неочаквано визуално несъответствие: Дори да изглеждат легитимни, фалшивите уебсайтове могат да имат дребни разлики в дизайна или функционалността, като странно оформление или липса на интерактивни елементи, които обикновено присъстват на оригиналния сайт.

- Отсъствие на фирмени детайли: Легитимните сайтове често предоставят информация за контакт, включително физически адрес, телефонен номер и данни за компанията. Липсата на такава информация или нейното представяне по неубедителен начин може да бъде знак за фалшив сайт. [5]

в) Социална инженерия:

Фишинг атаките разчитат на психологическата манипулация на жертвите, като използват различни техники, свързани с емоции и доверие:

- Използване на страх и спешност: Нападателите често се опитват да накарат жертвата да реагира бързо и без да мисли, като създават усещане за спешност. Те може да твърдят, че акаунтът ви ще бъде блокиран, че има спешен проблем с вашите банкови данни или че сте спечелили награда, която трябва да заявите веднага.

- Злоупотреба с доверие: Атакуващите често се представят за хора или институции, на които жертвата има доверие, като банки, колеги, правителствени агенции или дори приятели. Те използват имена и брандове, за да създадат чувство на легитимност.

- Апелиране към емоциите: Някои фишинг съобщения са насочени към емоциите на жертвата, като молби за помощ, свързани с благотворителни организации или семейни извънредни ситуации. Това може да накара хората да дарят пари или да предоставят информация, вярвайки, че помагат.

- Персонализирани атаки: При spear фишинга нападателите често използват информация за жертвата (например от социални мрежи), за да направят съобщението по-достоверно и персонализирано. Това повишава вероятността жертвата да повярва и да предостави исканите данни.

Разпознаването на тези признаци е ключово за предотвратяването на фишинг атаки. Обучението и информираността могат значително да намалят вероятността за успешна атака.

# 6 Мерки за защита

а) Образование и информираност:

Най-добрата защита срещу фишинг атаки е информираността. Обучението на служители и потребители играе ключова роля за разпознаване и предотвратяване на подобни заплахи.

Как помага:

- Разпознаване на признаци: Чрез обучение потребителите се научават да разпознават признаците на фалшиви имейли, като неправилни URL адреси, необичайни прикачени файлове и необичайни искания за информация.

- Симулирани фишинг атаки: Много организации провеждат тестове с фалшиви фишинг имейли, за да обучат служителите си да реагират правилно на подобни атаки и да ги разпознават по-лесно.

- Насърчаване на внимателност: Обучението помага да се създаде култура на внимателност и предпазливост сред потребителите, които биха могли да станат жертви на социална инженерия.

б) Технологични решения:

- Антивирусни програми и анти-фишинг софтуер:

Антивирусните програми и анти-фишинг софтуер предлагат многостепенна защита срещу зловреден софтуер и фишинг атаки. Те могат да откриват и блокират опасни имейли и уебсайтове.

Как помага:

• Сканиране за зловреден софтуер: Антивирусният софтуер анализира прикачените файлове и линкове, за да открие потенциално опасни файлове или зловреден код.

• Предупреждения за опасни уебсайтове: Анти-фишинг инструменти могат да предупреждават потребителите, ако опитат да отворят фалшив или опасен уебсайт, предотвратявайки възможността за предоставяне на лични данни.

• Обновяване на базите данни: Постоянното обновяване на антивирусните програми гарантира, че те са в състояние да разпознаят нови заплахи и методи на фишинг атаки.

- Многофакторна автентикация (MFA):

Описание: Многофакторната автентикация (MFA) изисква от потребителите да предоставят две или повече форми на идентификация при вход в акаунти, което значително намалява вероятността за успешна фишинг атака.

Как помага:

- Двуфакторна идентификация (2FA): Дори ако нападателите успеят да получат парола чрез фишинг атака, 2FA изисква допълнителна стъпка за влизане в акаунта, като изпращане на код по SMS или използване на приложение за генериране на кодове. Това прави неоторизирания достъп изключително труден.

- Защита срещу кражба на пароли: Чрез използване на допълнителен метод за автентикация (като биометрия, токени или еднократни кодове), MFA добавя допълнителен слой защита, дори когато основната парола е компрометирана.

с) Филтриране на имейли:

Имейл филтрите анализират съдържанието на входящите съобщения и могат да блокират потенциално опасни имейли, преди те да достигнат до потребителя.

Как помага:

- Филтриране на подозрителни съобщения: Филтрите могат да блокират имейли с подозрително съдържание, необичайни линкове, фалшиви домейни или съобщения с неправилна граматика и правопис.

- Спам филтри: Много имейл системи използват спам филтри, които разпознават и блокират нежелани или фишинг имейли, като ги изпращат директно в папката за нежелана поща.

- Обучение на филтрите: Системите за филтриране на имейли могат да бъдат „обучавани“, за да разпознават нови и по-сложни фишинг атаки, което подобрява тяхната ефективност с течение на времето.

Тези мерки за защита са от съществено значение за намаляване на риска от фишинг атаки. Комбинацията от образователни и технологични подходи предоставя силна защита както за индивидуалните потребители, така и за организациите.

# 7 Практики за безопасност

а) Не кликване върху съмнителни линкове:

Потребителите трябва да бъдат изключително внимателни при кликване на линкове в имейли, текстови съобщения или съобщения в социални мрежи, особено ако не разпознават подателя или ако съобщението изглежда подозрително.

Как помага:

- Избягване на опасни сайтове: Кликването върху съмнителни линкове може да доведе до достъп до фалшиви уебсайтове, където може да се поиска предоставяне на лични данни или пароли. Не кликването върху такива линкове намалява вероятността за компрометиране на информацията.

- Използване на курсор: Преди да кликнете, можете да задържите курсора над линка, за да видите действителния URL адрес. Ако адресът изглежда подозрително или не е свързан с известен сайт, е по-добре да не се кликва. [4]

б) Проверка на URL адреси и податели:

Проверка на URL адресите и имейл подателите преди предоставяне на лични данни или кликване на линкове е ключова практика за безопасност.

Как помага:

- Разпознаване на фалшиви домейни: Легитимните уебсайтове имат определени URL адреси. Проверка на описанието и домейна (например ".com", ".net") помага за разпознаване на фалшиви сайтове. Потребителите трябва да се уверят, че домейнът е идентичен на този на легитимната компания.

- Потвърждаване на идентичността на подателя: Потребителите трябва да проверят имейл адреса на подателя и да се уверят, че той съвпада с официалния адрес на компанията. Често атакуващите използват подобни адреси с малки разлики, за да заблудят жертвите. [4]

в) Редовно обновяване на пароли:

Периодичното обновяване на паролите е важна практика за поддържане на сигурността на акаунтите.

Как помага:

- Предотвратяване на неоторизиран достъп: Редовното променяне на паролите намалява риска от компрометиране на акаунти. Ако паролата е била изтекла или откраднатa, обновяването ѝ намалява шансовете за неоторизиран достъп.

- Използване на сложни пароли: При обновяване на паролите е важно да се създават силни пароли, които включват комбинации от букви (горен и долен регистър), цифри и

специални символи. Избягвайте използването на лична информация или лесни за отгатване пароли.

- Пароли за различни акаунти: Никога не използвайте същата парола за различни акаунти. Ако една парола бъде компрометирана, това може да доведе до достъп до множество акаунти. Използването на различни пароли е основен принцип за сигурност.

Следвайки тези практики за безопасност, потребителите могат да се защитят по-добре срещу фишинг атаки и да намалят риска от загуба на лични данни или финансова информация. Важно е да се развие култура на предпазливост и информираност, която да помага за предотвратяване на потенциални заплахи.

# 8 Заключение

В доклада разгледахме основните аспекти на фишинг атаките, техните техники и начините, по които потребителите и организациите могат да се защитят. Основните техники за фишинг включват:

- Имейл фишинг: Най-разпространеният метод, при който се изпращат фалшиви имейли, които имитират легитимни източници, за да получат лични данни.
- Spear фишинг: Насочени атаки, които целят конкретни индивиди или организации с персонализирани съобщения.
- Smishing и Vishing: Фишинг чрез текстови съобщения и телефонни обаждания, които също целят да измамят потребителите.
- Clone фишинг: Използване на клонирани уебсайтове или съобщения, за да се манипулират жертвите.
- Whaling: Атаки, насочени към високопоставени лица, при които нападателите използват информация за конкретни цели.

За защита срещу тези заплахи, важно е да се прилагат следните мерки:

- Образование и информираност на потребителите относно разпознаването на фишинг атаки.
- Използване на технологични решения, като антивирусни програми, многофакторна автентикация и имейл филтри.
- Практики за безопасност, включително избягване на съмнителни линкове, проверка на URL адреси и редовно обновяване на пароли.

# 9 Значимост на превенцията

Превенцията на фишинг атаки е от съществено значение в съвременния дигитален свят. Проактивните мерки и постоянното обучение на служители и потребители могат значително да намалят риска от успешни атаки. Организациите и индивидуалните потребители трябва да осъзнават важността на безопасността в онлайн среда и да инвестират в ресурси и обучения, които ще ги подготвят да се справят с тези заплахи.

Чрез създаване на култура на сигурност, където информираността и внимателността са приоритет, можем да защитим личните си данни и финансовата информация. Важно е да продължаваме да актуализираме знанията си за новите техники на фишинг и да се адаптираме към променящата се природа на киберзаплахите. Само така можем да се защитим ефективно в дигиталния свят.

**ЛИТЕРАТУРА:**

[1] Ангелова М., Phishing и защита от фишинг, 2013, Икономически университет Варна, https://www.slideshare.net/slideshow/phishing-28331402/28331402 посетено на 02.10.2024.

[2] Велу В., Бегс Р., Изучете Kali Linux: Етично хакване в примери, 2021, Издателство Асеневци, ISBN 9786197586275

[3] Daengsi T., Wuttidittachotti P., Pornpongtechavanich P., Utakrit N., A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization, 2021, International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Electronic ISBN:978-1-6654-3222-1DOI: 10.1109/ICSCEE50312.2021.9498208, pp. 12-15.

[4] Ivanov M., Kliuchnikova B., Chugunkov I., Plaksina A., Phishing Attacks and Protection Against Them, 2021, Conference of Russian Young Researchers in Electrical and Electronic Engineering, Electronic ISBN:978-1-6654-0476-1, DOI: 10.1109/ElConRus51938.2021.9396693, pp. 21-24.

[5] Madleňák M., Kampová K., Phishing as a Cyber Security Threat, 2022, International Conference on Emerging eLearning Technologies and Applications, Electronic ISBN:979-8-3503-2033-6, DOI: 10.1109/ICETA57911.2022.9974817, pp. 32-39.

[6] Sannd P. Cook D., Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks, 2018, Fourteenth International Conference on Information Processing (ICINPRO), Electronic ISBN:978-1-5386-7796-4, DOI: 10.1109/ICINPRO43533.2018.9096878, pp 102 – 110.

# RISK MANAGEMENT IN THE ORGANIZATION*

**DESISLAVA D. GEORGIEVA**

***ABSTRACT:*** *The process of risk management includes the identification and assessment of risks as well as active response by implementing strategies to minimize or transfer risk. The goal is to ensure sustainability and adaptability of the organization in conditions of uncertainty and dynamic changes in the environment.*

***KEYWORDS:*** *risk management, risk analysis, risk assessment, risk response, risk management monitoring*

***DOI: https://doi.org/10.46687/PYRQ2171***

# УПРАВЛЕНИЕ НА РИСКА В ОРГАНИЗАЦИЯТА

**ДЕСИСЛАВА Д. ГЕОРГИЕВА**

***АБСТРАКТ:*** *Процесът на управление на риска включва идентифициране и оценка на рисковете както и активна реакция, чрез прилагане на стратегии за минимизиране или прехвърляне на риска. Целта е да се осигури устойчивост и адаптивност на организацията в условия на несигурност и динамични промени в околната среда.*

Управлението на риска играе ключова роля в стратегическото управление на всяка компания. Това е процес, при който организацията систематично изследва рисковете, свързани с нейните дейности, с цел постигане на устойчив положителен резултат както в отделните инициативи, така и в цялостния портфейл от проекти. Ефективното управление на риска се фокусира върху разпознаването и адекватното управление на тези рискове, като основната му цел е да създаде максимална стойност за всяка дейност на организацията.

Политиката за управление на риска се движи от стремежа за разбиране и анализ на всички фактори, които могат да повлияят на растежа или спада на организацията, с оглед постигане на стратегическите ѝ цели. Този процес подпомага разпознаването на потенциални възможности и заплахи, които могат да окажат влияние върху бъдещето на компанията.

Управлението на риска обхваща ключови компоненти, които са критични за успеха на всяка фирма, включително процеси, култура, практики, структура и защитни мерки. Целта на тези елементи е да идентифицират и оценят рисковете, както и да подпомогнат вземането на важни решения, свързани с дейностите за управление на тези рискове. Този процес се прилага в минало, настояще и бъдеще, като основната му задача е да осигури сигурност и устойчив успех на компаниите. Управлението на риска спомага за поддържане на сигурността в приемливи граници както за организацията, така и за обществото като цяло. Специалистите в областта на системите за управление на риска разглеждат риск мениджмънта като комплексна система, която е тясно свързана с финансовите функции, възникнали в хода на бизнес процесите. [2]

Определението на понятието „риск мениджмънт“ е: целенасочен процес на формиране на компромис между изгодата от намалението на риска и необходимите за това

* Докладът е финансиран по проект № РД-08-147/02.02.2024 г., „Усъвършенстване на способностите за създаване на сценарий за тестване на уязвимости в симулационен оперативен център за сигурност“

разходи, а също така и вземане на решение за това какви действия трябва да се предприемат, в това число и дори въобще да не се предприемат никакви определени действия.“

Според наръчника ISO/IES Guide 73:2009 „Речник за риск мениджмънт“: „ Съгласувани дейности за ръководство и контрол на една компания по отношение на риска. Процес на идентифициране, оценяване, управление и контролиране на потенциални събития или ситуации (рискове), предназначен да даде разумно ниво на увереност, че целите на организацията ще бъдат постигнати.“ [4]

ISO 31000:2018 е международен стандарт, който предоставя насоки за управление на риска и е приложим за всякакъв тип организации – от малки фирми до големи корпорации и публични институции. Това е актуализирана версия на предходния стандарт, разработена от Международната организация по стандартизация (ISO), с цел да подпомогне организациите в идентифицирането, оценяването и управлението на рисковете, които могат да повлияят на техните цели. Представени са по-ясни, сбити и по-прецизни насоки, които подпомагат организациите в прилагането на принципите за управление на риска, с цел подобряване на планирането и вземането на по-обосновани решения. Основните актуализации спрямо предходното издание са следните:

- Принципите за управление на риска са преработени, за да служат като ключови критерии за успех при ефективното управление на рисковете.
- Акцентът е поставен върху ролята на висшето ръководство, което трябва да осигури интегриране на управлението на риска във всички аспекти на дейността на организацията, започвайки от нейното управление.
- Подчертана е важността на повторяемостта в процеса на управление на риска, като се насърчава използването на нови знания, опит и анализи за преглед на всички елементи, мерки и действия във всяка фаза.
- Съдържанието е рационализирано с фокус върху поддържането на отворени системи, които позволяват редовен обмен на обратна връзка с външната среда, за да се отговори на променящите се нужди и обстоятелства.

Всяка точка от стандарта е преразгледана, така че той да стане по-ясен и да го направи достъпен за всички заинтересовани. Изданието от 2018 г. акцентира върху създаването и поддържането на стойност като основен двигател на управлението на риска и обръща внимание на свързани принципи като непрекъснато усъвършенстване, ангажиране на всички заинтересовани страни, адаптиране към спецификата на организацията и отчитане на човешките и културни аспекти. [4]

Рискът се определя като „влияние на неопределеността върху постигането на целите“, което акцентира върху ролята на непълните или несигурни знания за събития и обстоятелства при вземане на решения в организацията. Това изисква промяна в традиционното възприемане на риска, като насърчава организациите да адаптират управлението на риска според своите специфични нужди и цели — едно от основните предимства на стандарта. [1]

Управлението на риска е приложимо не само за корпорации и публични компании, но и за всякакви видове дейности — както краткосрочни, така и дългосрочни. Ползите от управлението на риска следва да се разглеждат не само в контекста на организационната дейност, но и от гледна точка на интересите на различните участници в процеса, които могат да бъдат засегнати. Има различни подходи за постигане на целите на управлението на риска. Компаниите, които обхващат основните елементи на стандарта, макар и по индивидуален начин, могат да считат, че изпълняват целите на политиката за управление на риска.[2]

Управлението на риска е съществена част от корпоративната стратегия, особено при наличие на непредвидими глобални събития. Успешните компании прилагат структурирани подходи за управление на риска, които ги подготвят по-ефективно за кризи, помагат им да минимизират потенциалните загуби и дори да превърнат някои рискове в нови възможности.[10]

За големите корпорации ефективното управление на риска включва създаване на солидна стратегическа основа и нейното оперативно прилагане. Според проучване на *Boston Consulting Group (BCG*), компаниите, които са имали зрели практики за управление на риска преди последните глобални кризи – като пандемията COVID-19 – са били по-способни да се справят с несигурността, като 71% от най-добре представилите се признават важността на това. Тези компании комбинират стратегическо планиране със специални екипи за управление на риска, за да се справят с предизвикателствата. От друга страна, компаниите, които започват своя път към управление на риска, трябва да се съсредоточат върху изграждането на основни рамки за справяне с вътрешния и външния риск. [6]

**Управлението на риска** се разглежда като процес за идентифициране, анализ, противодействие, наблюдение и контрол на риска, насочен към максимизиране на резултатите от позитивните събития и минимизиране на ефектите от негативните. Това е системен процес за ефективно редуциране – намаляване или съкращаване влиянието на несигурността, която застрашава организационните цели[9].

**Основните дейности от процеса по управление** на риска [3]:

**1 - Иницииране на процеса**. Поставят се началните условия на процеса и се съставят: задание (заявка за провеждане), организационна заповед за сформиране на екипите и провеждане, както и програма за реда, начина и периодичността за оценка на риска при планирането на дейността с цел постигате на основните цели.

**2 - Дефиниране на средата.** Определят се процесите, които са в обхвата на средата, заинтересованите страни и какви са техните цели. Това е рамката, в която ще се търсят рискове с цел тяхното управление. Крайни продукти от етапа са критериите за оценка и значимите външни и вътрешни фактори на средата.

**3 - Идентифициране на рисковете**. При идентифицирането на риска се изследват и определят рисковите области и източниците на риск за организационната дейност. Това се извършва с различни методи за идентификация на рисковите събития, които най – общо се изразяват чрез следните подходи:

- *Определяне на риска на базата на целите* – определят се целите на организацията, а всички събития или обстоятелства, които могат частично или напълно да застрашат постигането на тези цели, се определят като рискове.
- *Определяне на риска на базата на сценарии* – разиграват се различни сценарии за развитието на определено събитие или изпълнението на определен процес. Всяко събитие, което предизвиква реализирането на нежелан резултат, се третира като риск и/или заплаха.
- *Определяне на риска на базата на класификацията* – определят се възможните източници на риск. На базата на тази класификация и на информацията за общо използваните добри практики се разработва въпросник, от отговорите на който се извличат рисковете, които трябва да се контролират. Крайните продукти от етапа са описание на дейностите от процеса, идентифициране на потенциалните рискове и източниците на риск.

Идентификацията на риска има за цел да оцени доколко организацията може да бъде уязвима към несигурност и неопределеност. Тя изисква задълбочено разбиране на структурата и дейността на организацията, пазара, социалната, нормативната, политическата и културната среда, както и яснота относно стратегическите и оперативните

цели, включително критичните фактори за успех. Тази фаза включва идентифициране на потенциалните заплахи и възможности, които могат да повлияят на постигането на целите.[11]

Процесът на идентификация на риска се извършва методично, за да гарантира, че всички значими дейности и рискове са обхванати. Неопределеностите, свързани с тези дейности, трябва да бъдат разпознати и категоризирани систематично. [2]

**4 - Анализ на риска.** При анализа на риска се разглеждат вече идентифицираните рискове и техните причини. Този етап е комплексен и включва създаване на структура за ефективно оценяване на риска. Анализът се фокусира върху параметрите на риска и потенциалното му въздействие върху изпълнението на специфични дейности по различни сценарии. Основните резултати от този етап са определяне на допустимите нива на риска и създаване на карти за оценка, които включват вероятността за възникване на рисковете и стойността на техните последици за организацията.

| | |
|---|---|
| 1. Обхват на риска | Качествено описание на събитията, техния мащаб, вид, брой и зависимости |
| 2. Характер на риска | Например: стратегически, оперативен, финансов, риск от несъответствие |
| 3. Фактори, които влияят на риска | Различни групи от хора, фактори, среди, както и техните очаквания, предвидимост |
| 4. Количествена характеристика на риска | Въздействие и вероятност |
| 5. Праг на поносимост | Потенциал за загуба и финансови последствия<br>Максимална възможна загуба<br>Вероятност и размер на потенциалната загуба/печалба<br>Цели за контрол на риска и желано ниво на изпълнение |
| 6. Механизми за контрол и трансфер | Основни средства за текущ трансфер с риска<br>Ниво на доверие в съществуващите механизми<br>Протоколи за мониторинг и преглед |
| 7. Възможни мерки за подобрение | Препоръки за минимализиране на риска |
| 8. Стратегия и развитие на политики | Определяне на функционално отговорен екип за развитие на стратегия и политика |

**5 - Оценка на риска**. Извършва се на база потенциалните вредни последици и вероятността те да настъпят. Това е един от най-критичните и сложни етапи в управлението на риска. Изпълнението му често се затруднява поради липсата на достатъчно адекватна информация, върху която да се базират анализите. В резултат на оценката се съставят различни варианти, които описват желаните възможности и рисковите събития, изискващи реакция. Също така се определят случаите, в които може да се пренебрегнат или приемат определени рискови събития, при условие че не надхвърлят допустимото ниво на риск.

След анализа на рисковете следва те да бъдат сравнени спрямо критериите, установени от компанията. Тези критерии могат да включват оценки на разходи и приходи, нормативни изисквания, социално-икономически и екологични фактори, както и интереси на заинтересованите страни. Чрез качествена оценка на рисковете се дава възможност за приоритизирането им според тяхната значимост за организацията и се взема решение дали всеки риск да бъде запазен или прехвърлен.[2]

Основните елементи на процеса на оценка на риска включват:

1. **Идентификация на рискове**: Определяне на всички възможни рискове – както вътрешни (като оперативни или стратегически проблеми), така и външни (икономически, природни бедствия, регулаторни промени).

2. **Анализ на рисковете**: Оценка на вероятността всяко събитие да се случи и какви биха били последствията за компанията.

3. **Оценка на въздействието**: Оценка на влиянието на тези рискове върху различни аспекти на бизнеса – финанси, репутация, операции.

4. **Разработване на стратегии за управление на рисковете**: Това включва действия като избягване на риска, намаляване на неговото въздействие, прехвърляне на риска (например чрез застраховки) или приемането му като част от нормалната дейност на компанията.

Ефективната оценка на риска подпомага корпорациите в създаването на по-устойчива стратегия, помага за избягване на големи загуби и засилва доверието на инвеститорите и заинтересованите страни. Често за оценка на риска се използват различни методологии като картографиране на рискове, сценарийни анализи и анализ на чувствителността.[5]

**6- Противодействие на риска.** Прави се определяне, оценка, избор и прилагане на подходящи техники за противодействие на идентифицираните (установените, разкритите) и оценени рискове с цел намаляване на влиянието им до приемливи нива. Противодействието на риска в корпорацията включва различни стратегии и подходи, които целят да намалят или елиминират влиянието на рисковете върху бизнеса. Основните начини за управление и противодействие на риска са:

1. *Избягване на риска:* Тази стратегия включва избягване на дейности или ситуации, които създават значителни рискове. Например, ако даден проект или инвестиция носи прекомерен риск за компанията, тя може просто да се откаже от него. Това обаче не винаги е възможно, особено ако рисковете са свързани с ключови бизнес процеси.

2. *Намаляване на риска (минимизиране):* Предприемане на мерки за намаляване на вероятността или въздействието на определен риск. Това може да бъде чрез подобряване на вътрешни процеси, автоматизация, обучение на персонала или използване на нови технологии като системи за киберсигурност, за да намалят риска от хакерски атаки.

3. *Прехвърляне на риска:* Често срещана практика е рехвърлянето на риска към трета страна чрез застраховки, договори или аутсорсинг. Например, компания може да се застрахова срещу загуби от природни бедствия или да прехвърли част от операционния риск чрез възлагане на аутсорсинг на важни функции.

4. *Приемане на риска*: Ако рисковете са неизбежни или незначителни, компанията може да реши да ги приеме. Това означава, че организацията съзнателно поема риска с ясното съзнание за последствията, ако събитие се случи. Това се случва, когато потенциалните ползи надвишават риска или когато намаляването му е твърде скъпо или невъзможно.

5. *Диверсификация:* Намаляването на риска може да стане и чрез диверсификация на инвестициите, дейностите или доставчиците. Чрез разпръскване на риска върху различни сектори или пазари, компанията може да смекчи влиянието на едно негативно събитие върху целия бизнес.

6. *Сценарийни анализи и планиране на кризи:* Това включва предварителна подготовка за различни сценарии, като природни бедствия, финансови кризи или технологични инциденти. Чрез анализ на потенциалните сценарии и разработване на планове за действие, корпорациите могат да реагират по-бързо и ефективно в случай на криза

Тези подходи за противодействие на риска помагат на корпорациите да изградят устойчивост и способност за реакция в условия на несигурност.[6]

**7 - Мониторинг и проследяване на процеса на управление на риска.** Това е дейност за систематично следене и оценяване на прилаганите техники за противодействие на риска. На този етап могат да се разработват нови или да се усъвършенстват старите техники. Краен продукт от етапа е изготвянето на коригиран план за управление на риска.

Процесът на наблюдение трябва да потвърди наличието на необходимите контролни механизми за дейността на организацията и да гарантира, че процедурите се разбират и изпълняват коректно. Промените в организацията и в средата, в която тя функционира, следва да бъдат идентифицирани, за да се направят съответните корекции в системата. Всеки процес на преглед и наблюдение също така трябва да установи дали:

• Предприетите мерки са дали желания резултат;

• Възприетите процедури и събраната информация за оценката са били подходящи;

• По-добро познаване на проблема би довело до по-сполучливи решения и до по-добри представи за това, какво ново трябва да се научи за по-добро бъдещо оценяване и управление на рисковете. [2]

„**Иницииране на процеса”** е първият етап от процеса на управлението на риска и се състои основно от следните дейности:

- изясняване на задачата;
- определяне на работните групи;
- изготвяне на програма за дейността по оценяването на риска.

За начало на процеса се счита постъпването на заявка, указание или разпореждане за провеждане на изследването, което е водеща линия и фокус на извършваните дейности. Заявката трябва да съдържа рамката, в която следва да се идентифицират целите и да се отчете тяхното постигане.

▪ **Изясняване на задачата**

Това е критична първа стъпка, която поставя основите за успешно изпълнение на управлението на риска. Основните елементи на този процес включват:

1. *Определяне на целите на управлението на риска:* Дефинират се конкретните цели, които управлението на риска трябва да постигне. Това може да включва защита на активите, намаляване на финансовите загуби или защита на репутацията на компанията. Целите трябва да бъдат ясни и измерими.

2. *Идентифициране на ключовите заинтересовани страни:* Определят се всички участници, които ще бъдат ангажирани в процеса на управление на риска. Това са мениджъри, екипи и външни партньори, които имат роля в идентифицирането и управлението на рисковете.

3. *Оценка на рисковете:* Изяснява се какви типове рискове ще бъдат анализирани (оперативни, стратегически, финансови), за да се разбере как всеки от тези рискове може да повлияе на организацията и да се разработи план за тяхното оценяване и управление.

4. *Разработване на методология за управление на риска:* Дефинира се конкретният подход или рамка, която ще се използва за идентификация, оценка и управление на рисковете.

5. *Определяне на ресурси*: Установява се какви ресурси (финансови, човешки и технологични) ще бъдат необходими за изпълнение на процеса на управление на риска.

6. *Определяне на времеви рамки:* Ключово е да се зададе ясен времеви хоризонт за изпълнение на оценката и управлението на риска. Това включва определяне на сроковете за всяка стъпка от процеса.

Правилното изясняване на задачата при иницииране на управление на риска помага за координирането на усилията на всички звена в компанията и за осигуряване на ясна посока към целите на управление на риска.

▪ **Определяне на работна група**

Това е ключова стъпка, тъй като правилният подбор на членове на екипа гарантира ефективност и координиране в управлението на рисковете в корпорацията. Работната група за управление на риска обикновено включва хора с различен опит и умения, които обхващат всички аспекти на бизнеса:

- *Ръководител на управлението на риска (Risk Manager):* човек, който ръководи целия процес, координира дейностите и следи за изпълнението на плана за управление на риска.

- *Представители на висшето ръководство:* гарантират, че процесът за управление на риска е в съответствие със стратегическите цели на компанията.

- *Експерти по отдели:* мениджъри от различни звена като финанси, ИТ, човешки ресурси, които познават най-добре специфичните рискове за техния отдел.

- *Юридически специалисти:* следят за регулаторните изисквания и правните рискове, които могат да възникнат.

- *Външни консултанти:* при липса на вътрешна експертиза, външни консултанти могат да допринесат с експертен опит.

Всеки член на екипа има ясни отговорности, които се разпределят в зависимост от тяхната експертиза. Специалисти от различни отдели идентифицират и оценяват рисковете, свързани с техните зони на работа, извършва се и редовното наблюдение на рисковете и докладване за тях пред ръководството. Работната група трябва да премине специализирано обучение по управление на риска, за да се запознае с инструментите и методите, които ще използва. Това обучение трябва да бъде постоянно и адаптирано към промените в средата, както и новите рискове, които възникват. Ефективната работна група за управление на риска гарантира, че компанията е подготвена да се справи с възможни предизвикателства, като подобрява устойчивостта и адаптивността на бизнеса. [7]

▪ **Изготвяне на програма**

Изготвянето на програма за управление на риска в корпорацията е основна част от стратегическото управление. Програмата се фокусира върху систематичен подход за идентифициране, оценяване, минимизиране и наблюдение на рисковете. Следващите стъпки очертават основните етапи в създаването на такава програма:

• ***Определяне на целите и обхвата на програмата***

Първата стъпка е да се определи какви конкретни цели и задачи трябва да изпълни програмата за управление на риска. Това включва:

- Идентифициране на критични активи, процеси и цели на компанията;

- Определяне на ключовите показатели за успех и допустимите нива на риск;

- Обхватът трябва да включва всички звена на организацията, както и външни фактори като пазарни условия, регулаторни изисквания и конкуренция.

• ***Идентифициране на рисковете***

Това е един от основните елементи в управлението на риска. На този етап се идентифицират всички възможни рискове, които могат да въздействат на компанията. Това включва вътрешни рискове (като оперативни, финансови и технологични) и външни рискове (икономически, природни бедствия, политически промени).

• ***Оценка и класификация на рисковете***

След като рисковете са идентифицирани, те трябва да бъдат оценени по два основни критерия: вероятност и въздействие. Рисковете могат да бъдат класифицирани по:

- Вероятността от настъпване на даден риск.
- Потенциалното въздействие върху бизнеса (финансово, репутационно, оперативно).

- ***Разработване на стратегии за управление на риска***

След като рисковете са класифицирани, трябва да се разработят стратегии за тяхното управление. Основните подходи включват:

- Избягване на риска– премахване на дейности или процеси, които създават неприемливи рискове.
- Намаляване на риска– въвеждане на мерки за минимизиране на вероятността или въздействието на риска.
- Прехвърляне на риска – използване на застраховки или външни доставчици, за да се намали тежестта на риска.
- Приемане на риска– осъзнато решение за поемане на риска, когато той е в допустими граници.

Ефективното управление на риска изисква непрекъснато наблюдение на рисковете и актуализиране на плановете за действие като например: регулярни одити на риска, докладване за нововъзникнали рискове или промени в съществуващите и използване на софтуерни решения за управление и мониторинг на риска, които автоматизират част от процеса. Програмата за управление на риска не трябва да бъде статична. Тя трябва да се преглежда и актуализира редовно, за да отразява промените във вътрешните и външните условия на компанията. Систематичното и структурирано изготвяне на програма за управление на риска подобрява устойчивостта на корпорацията и намалява негативното въздействие на потенциални събития.

Управлението на риска е процес на определяне на остатъчния риск в една информационна система въз основа на измерения по конкретна методология риск и минимизирането му чрез внедряване на средства за защита. Средствата за защита, гарантиращи този приемлив риск, залягат в разработваната от организацията политика за информационна сигурност. Той включва три основни елемента: анализ на потенциалните заплахи и уязвимостта на системата; оценка на възможните загуби; избор на оптимални мерки и средства за минимизиране на остатъчния риск до приемливо ниво. Контролът на риска за информационна сигурност се обсъжда детайлно в стандартите на Международната организация по стандартизация и Международната електротехническа комисия (ISO/IEC 17799, ISO/IEC 27001 ).

В пасивна позиция компаниите не могат да формират оптимален рисков профил според своите бизнес модели, нито да управляват адекватно бързо развиваща се криза. Избягвайки рисковия подход, състоящ се от краткосрочни инициативи за ефективност, фокусирани върху приходите и разходите, най-добре представящите се смятат управлението на риска за стратегически актив, който може да поддържа значителна стойност в дългосрочен план. [8]

В заключение, управлението на риска е ключов елемент за устойчивостта на организацията в динамичната бизнес среда. То позволява идентифициране и минимизиране на потенциални заплахи, които могат да повлияят на оперативната ефективност. Чрез интегриран подход и сътрудничество между различните отдели, организациите могат да разработят ефективни стратегии за управление на риска. Постоянното актуализиране на тези стратегии осигурява готовност за реагиране на нови предизвикателства и възможности. В крайна сметка, инвестирането в управление на риска не само защитава активите, но и допринася за дългосрочния успех на организацията.

**ЛИТЕРАТУРА:**

[1] „Новият стандарт ISO 31000 опростява управлението на риска“, Български институт за стандартизация, (https://bds-bg.org/), посетено на 15/10/2024;

[2] СТАНДАРТ ПО УПРАВЛЕНИЕ НА РИСКА, FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS, (https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-bulgarian-version.pdf), посетено на 20/10/2024;

[3] ЧАСТ ВТОРА – УПРАВЛЕНИЕ НА РИСКА, Национален военен университет „Васил Левски, (https://www.nvu.bg/sites/default/files/norm_baza/adm_mod/2013/03_adm_4ast2.pdf), посетено на 24/10/2024;

[4] Assessment and Risk Management, (https://arm953.wordpress.com/), посетено на 19/10/2024;

[5] Managing Risks: A New Framework, Harvard Business School, (https://www.hbs.edu/faculty/Pages/item.aspx?num=42549), посетено на 28/10/2024;

[6] Mature Risk Management in Uncertain Times, BCG, (https://www.bcg.com/publications/2023/risk-management-strategies-in-uncertain-times), посетено на 27/10/2024;

[7] Risk management is for all companies — not just the giants, World Economic Forum, (https://www.weforum.org/agenda/2023/09/risk-management-is-for-all-companies-not-just-the-giants/), посетено на 24/10/2024;

[8] Value and resilience through better risk management, McKinsey, (https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/value-and-resilience-through-better-risk-management), посетено на 28/10/2024.

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

[10] Методиева Ц, Национална и корпоративна сигурност, НК с международно участие „MATTEX 2018“, ШУ ”Епископ Константин Преславски”, 25-27октомври 2018 г., Шумен, ISSN: 1314-3921, т. 2, 2018.

[11] Методиева, Ц., „Корпоративната сигурност и нейните компоненти“. Годишник на Шуменския университет „Епископ Константин Преславски“, с. 338-341, ISSN 1311-834X, 2020 г. (български език).

# APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY*

**STOYAN R. STOYANOV**

***ABSTRACT:*** *The paper discusses the applications of artificial intelligence (AI) in cybersecurity, focusing on areas such as: anomaly detection, automated incident response, user behavioral analysis, and the use of machine learning in antivirus programs. AI is proving to be an effective solution to address complex and evolving cyber threats, building on traditional approaches with better precision, automation and real-time analysis. Techniques such as deep learning (DL), natural language processing (NLP), and behavioral models provide proactive protection, quickly adapting to new threats and minimizing false positives. The paper presents real-world applications and development prospects that highlight the importance of AI for the future of cybersecurity.*

***KEYWORDS:*** *artificial intelligence, technologies, applications, cybersecurity*

***DOI: https://doi.org/10.46687/KQJS3601***

# ПРИЛОЖЕНИЯ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В КИБЕРСИГУРНОСТТА

**Стоян Р. Стоянов**

***АБСТРАКТ:*** *В доклада се разглеждат приложенията на изкуствения интелект (ИИ) в киберсигурността, като се обръща внимание на области като: откриване на аномалии, автоматизирано реагиране на инциденти, анализ на поведението на потребителите и използване на машинно обучение в антивирусните програми. ИИ се оказва ефективно решение за справяне със сложните и еволюиращи киберзаплахи, като надгражда традиционните подходи с по-добра прецизност, автоматизация и анализ в реално време. Техники като deep learning (DL), natural language processing (NLP) и поведенчески модели осигуряват проактивна защита, като бързо се адаптират към новите заплахи и свеждат до минимум фалшивите положителни резултати. Документът представя реални приложения и перспективи за развитие, които подчертават значението на ИИ за бъдещето на киберсигурността.*

## 1 Въведение

Съвременното ни общество става все по-зависимо от дигиталните технологии. Това превръща киберсигурността в критично предизвикателство за организации и потребители. Обемът на данните и сложността на кибератаките нарастват, което изисква нови и по-ефективни подходи за защита на информацията. Традиционните методи все по-често не успяват да се справят с модерните заплахи, които стават все по-трудни за предсказване и предотвратяване. Тук на помощ идва изкуственият интелект (ИИ) със своите иновативни решения и възможности, които могат значително да подобрят ефективността на защитата в киберпространството.

Технологиите на ИИ могат да идентифицират заплахите по-бързо и точно, да реагират на атаки автоматично и в реално време и да откриват аномалии и подозрително поведение чрез дълбок анализ на данни. Те могат да откриват неочаквани модели и да предсказват атаки още преди да са настъпили, като извършват машинно обучение и анализ на големи

* Докладът е финансиран по проект № РД-08-147/02.02.2024 г., „Усъвършенстване на способностите за създаване на сценарий за тестване на уязвимости в симулационен оперативен център за сигурност“

масиви от данни. Приложенията на ИИ в областта на киберсигурността са много, но в този доклад ще бъдат разгледани само някои от ключовите. Това са засичането на аномалии, автоматизираното реагиране при инциденти, поведенческият анализ на потребителите и субектите, машинното обучение при антивирусните програми и обработката на естествен език за разузнаване и анализ на заплахите.

## 2 Засичане на аномалии (Anomaly Detection)

***Определение и преимущества:*** В киберсигурността засичането на аномалии е процес на идентифициране на необичайни, отклоняващи се от нормата модели или поведение в системите или мрежите. Аномалиите могат да сочат за наличието на потенциални заплахи за сигурността, като например неоторизиран достъп, злонамерен софтуер или нарушаване на сигурността на данните.

Базираното на ИИ откриване на аномалии предлага обещаващо решение за киберсигурност в реално време, като използва усъвършенствани алгоритми за машинно обучение. Този подход подобрява способността за откриване на нови и незасичани досега заплахи, които традиционните системи, базирани на сигнатури, могат да пропуснат. Системите, управлявани от ИИ са в състояние да анализират огромни количества данни в реално време. Съществено предимство на базираното на ИИ откриване на аномалии се крие в способността на моделите непрекъснато да се самообучават и адаптират. Те могат да бъдат обучавани върху обширни набори от данни, за да разпознават нормалното поведение в рамките на мрежа или система. След това тези модели могат да наблюдават потоци от данни в реално време, като отбелязват всички аномалии, отклоняващи се от нормата[1].

***Техники:*** Основни техники за обучение, използвани за засичане на аномалии, са дълбоко обучение (DL) и машинно обучение (ML). С тяхна помощ се правят прогнози въз основа на събраните данни.

Изследвани са различни методи за откриване на аномалии: с помощта на DL; базирани на структури от типа "напълно свързана мрежа" (FCN); вариационен автоенкодер (VAE); "последователност към последователност" (Seq2Seq)[2]; техники за контролирано обучение като “дървета на решенията”, машини с поддържащи вектори (SVM) и невронни мрежи. Методите за неконтролирано обучение, като клъстериране и анализ на главните компоненти (PCA), също са широко проучени заради способността им да откриват аномалии. Ефективни при откриването на мрежови проникванията са и скритите модели на Марков (HMM)[1]. С цел откриване на заплахи в реално време са разработени алгоритми за поточно предаване, които могат да обработват непрекъснати потоци от данни. Предложени са техники като онлайн обучение и инкрементални актуализации на моделите за машинно обучение, за да се гарантира, че системите за откриване на аномалии могат бързо да се адаптират към нови заплахи[1].

***Приложения:*** Установено е, че динамиката на натискане на клавишите на клавиатурата може да се използва ефективно за разпознаване на легитимни потребители. Това може да се използва за първоначално и мултифакторно удостоверяване на потребителя, и за откриване на аномалии[3].

В [2] авторите предлагат нова архитектура за киберзащита, специално адаптирана за 5G технологии, която значително подобрява идентифицирането на заплахи по отношение на скорост и ефективност. Използвано е дълбоко обучение (DL) за да се извлекат характеристики на мрежовия трафик и е въведена система за откриване на мрежови аномалии.

Използването на модели за DL за откриване на проникванията в индустриални системи за управление (ICS) показва обещаващи резултати. С цел откриване на аномалии в тези системи са прилагани дълбоки невронни мрежи (DNN), като постигат високи нива на откриване и минимални фалшиво положителни резултати[1].

# 3 Автоматизирано реагиране при инциденти (Automated Incident Response)

***Определение и преимущества:*** Автоматизираното реагиране на инциденти (AIR) в областта на киберсигурността е свързано с използването на автоматизирани инструменти и системи за откриване, анализиране и реагиране на инциденти, без или с минимално участие на човешкия фактор. AIR рационализира процесите на идентифициране на заплахите, локализиране на атаките и намаляване на щетите, чрез изпълнение на предварително определени действия. Тези действия включват изолиране на засегнатите системи, блокиране на злонамерения трафик и/или задействане на предупреждения.

Изкуственият интелект може да помогне за подобряване на реакцията при инциденти чрез автоматизиране на няколко аспекта на процеса, като откриване и анализиране на потенциални заплахи, приоритизиране на сигналите и предприемане на незабавни действия. Той може също така да подобри скоростта и точността на усилията за реагиране и да намали работното натоварване на човешките екипи[4].

Според изследвания посочени в [5], подходът, управляван от ИИ, постига 95,7 % точност на откриване на заплахи, като значително превъзхожда подхода, базиран на правила, който има точност 82,4 %. Средното време за реакция на системите, управлявани от ИИ, е 12 милисекунди (ms), докато средното време за реакция на системата, базирана на правила, е 48 ms. Това четирикратно намаляване на времето за реакция демонстрира повишаване на ефективността. По-краткото време за реакция позволява на организациите да се справят със заплахите по-бързо и да сведат до минимум потенциалното им въздействие върху мрежовите операции. При проведените експерименти е установено, че честотата на фалшивите положителни резултати на система, управлявана от ИИ, е била 3,2 %, докато при системата, базирана на правила, те са били 12,5 %. По-ниският процент на фалшивите положителни резултати на системата, управлявана от ИИ, показва по-високо ниво на прецизност при идентифицирането на истински заплахи за сигурността, като същевременно се свеждат до минимум фалшивите аларми. Това намаляване на фалшивите положителни сигнали повишава надеждността и ефективността на работните процеси за откриване и реагиране на инциденти.

***Инструменти и техники:*** Ключовите компоненти на AIR, задвижвано от ИИ, включват усъвършенствани механизми за откриване на заплахи, адаптивни стратегии за реагиране и интелигентни възможности за вземане на решения. Тези системи използват алгоритми като контролирано, неконтролирано и усилено обучение, за да анализират огромни количества данни, да откриват аномални поведения и да идентифицират потенциални заплахи за сигурността. Тенденция е и интегрирането на техники за обработка на естествен език (NLP) с цел подобряване на контекстуалното разбиране на събитията, свързани със сигурността, и за автоматизиране на генерирането на доклади за инциденти[5].

Примери за техники за машинно обучение, които се използват за изследване на мрежовия трафик и рамковото поведение на модели и аномалии, са дълбоките мозъчни организации и нерегулярните гори (Random Forest)[6].

***Приложения:*** Автоматизирано реагиране при инциденти, управлявано от ИИ, е използвано в продуктите Splunk и IBM QRadar. Такова има и в платформите за управление на информация и събития (SIEM) и системите за наблюдение и защита на крайни точки (EDR), като например Carbon Dark и CrowdStrike. Използването на услуги за разузнаване на заплахите като MISP и програми като Infection Complete също предоставят жизненоважна информация за възникващи заплахи и уязвимости. Решенията за автоматизация като Ansible и Apparition рационализират усилията за реагиране, а компютъризираните криминологични инструменти като Dissection и EnCase улесняват разследването на случаите[6].

Една конкретна област, в която ИИ може да намери полезно приложение, е анализът на логове, като намалява работното натоварване на персонала и освобождава ресурси за по-сложни задачи[4].

Адаптивността и мащабируемостта на системите, управлявани от ИИ, им позволяват ефективно да откриват и да реагират на променящите се пейзажи от заплахи, включително експлойти от нулев ден и напреднали устойчиви заплахи (APT). Тази адаптивност осигурява цялостно покритие и защита в големи и сложни мрежови среди, като повишава устойчивостта на организациите срещу широк спектър от киберзаплахи[5].

# 4 Поведенчески анализ на потребителите и субектите (User and Entity Behavioral Analysis)

***Определение и преимущества***: Анализът на поведението на потребителите и субектите (UEBA) е процеса на наблюдение и анализ на поведението на потребителите, устройствата и другите субекти в мрежата с цел откриване на аномалии, които биха могли да означават заплахи за сигурността. Основният принцип при UEBA е установяването на базова линия на нормално поведение чрез използването на машинно обучение и анализи. Идентифицирането на отклонения от тази базова линия може да показва наличието на заплахи от вътрешен човек, компрометирани акаунти или зловреден софтуер. По този начин могат да бъдат разкрити сложни атаки, които традиционните инструменти, базирани на правила и сигнатури, могат да пропуснат.

Включването на изкуствен интелект при поведенческия анализ позволява по-динамичен подход към откриването на заплахи. Използвайки този метод, системите с ИИ могат да обработват множество данни за крайни точки в мрежата на организацията. След това тази информация се използва за разработване на изчерпателни профили на приложенията, които предоставят цялостна представа за нормалните модели на работа[7].

***Техники:*** Техниките на машинното обучение (ML) играят решаваща роля в UEBA, като позволяват автоматизирано изучаване на моделите на поведение на потребителите и идентифициране на отклоненията от тях. Методите за неконтролирано обучение, като например клъстеризацията или откриването на аномалии, обикновено се използват за групиране на потребителите въз основа на сходствата в поведението им и за откриване на отклонения или аномалии. Алгоритми за контролирано обучение, като дървета на решенията, SVM или невронни мрежи, могат да бъдат обучени върху маркирани набори от данни, съдържащи нормално и аномално потребителско поведение, и въз основа на техните характеристики да класифицират нови случаи. Тези характеристики могат да включват модели на влизане, достъп до ресурси, навици за сърфиране в електронна поща и интернет или дейности по прехвърляне на файлове. Извличането на последователни модели и моделите на Марков също са прилагани за моделиране на времевата динамика на

поведението на потребителите, като са улавяни последователностите и преходите на действията на потребителите във времето. Отклоненията от научените поведенчески модели могат да се използват за откриване на аномални или подозрителни дейности[8].

Анализът на поведението на потребителите с цел откриване на потенциални заплахи е една от най-застъпените ИИ техники в областта на сигурността в облака. Тези техники включват алгоритми за машинно обучение, невронни мрежи и модели за дълбоко обучение[9].

***Приложения:*** Внедряването на UEBA във финансовите институции е значителен напредък в използването на ИИ и ML за целите на киберсигурността в облачни среди. Системите UEBA анализират моделите на поведение на потребителите, за да откриват аномалии, които могат да показват заплахи за сигурността като вътрешни атаки, неоторизиран достъп или измами. Тези системи са особено умели в идентифицирането на необичайни модели на транзакции и достъп до чувствителни финансови данни, като предлагат проактивен подход към сигурността. Те проучват моделите на покупки и достъпа до данни на клиентите, като използват усъвършенствани алгоритми за идентифициране на необичайни дейности, които могат да сигнализират за компрометиране на акаунти или кражба на данни. Този подход демонстрира стойността на ИИ за подобряване на мерките за сигурност в сектори, в които доверието на клиентите и сигурността на данните са от първостепенно значение[9].

В облачните среди, където постоянно се появяват нови услуги, технологии и модели на поведение на потребителите, способността на ИИ да се учи от нови набори от данни и да се адаптира към тези промени е безценна. Той дава възможност на системите за сигурност в облака да разпознават и реагират по-ефективно на нововъзникващите заплахи, като по този начин подобряват цялостната сигурност[9].

ИИ може да разработи профили на всяко едно приложение, които да служат като еталон за откриване на аномалии в реално време, където всяко отклонение от нормата може да означава потенциален риск за сигурността, като например наличието на атаки от типа "zeroday". ИИ и UEBA могат да идентифицират тези атаки на значително по-ранен етап от жизнения им цикъл. ИИ дава възможност за проактивна защита срещу потенциални пробиви, дори преди уязвимостите да бъдат разкрити и отстранени публично[7].

Конкретен пример за приложение на ИИ в UEBA е безплатният софтуер за машинно обучение Weka (Waikato Environment for Knowledge Analysis). Той е написан на Java и е разработен в Университета на Waikato, Нова Зеландия. Съдържа набор от алгоритми за класификация и клъстеризация, които могат да се използват за анализ на поведението на потребителите[8].

# 5 Машинно обучение при антивирусните програми (Machine Learning in Antivirus)

***Определение***: Използването на машинно обучение (ML) в антивирусните програми се изразява в употребата на алгоритми, анализиращи големи масиви от данни за злонамерен софтуер, както и за безвредни файлове, за да откриват нови и модифициращи се заплахи. Тези модели изучават моделите и поведението на зловредния софтуер, което позволява на антивирусните програми да го идентифицират и блокират по-ефективно, без да разчитат на предварително съществуващи бази данни със сигнатури.

***Техники:*** С цел подобряване на методите за идентифициране, с които разполагат антивирусните програми, са прилагани подходи, основани на правила за машинно

обучение, включващи следните основни задачи: моделиране на база от знания; формиране на набори от правила за разпознаване на известни вируси; диагностициране и откриване на специфични правила с помощта на алгоритми за извличане на данни; откриване на скрити атрибути и прогнозиране на неизвестни вируси с помощта на инструменти за генетично програмиране[10].

В един от важните етапи на машинното обучение при антивирусните системи се използват две основни техники: „директен извод“ и „обратно извеждане“ (forward and backward inference). Директният изводът е насочен към разпознаване на известни вируси чрез анализ на специфични кодови правила, докато обратното извеждане е фокусирано върху откриване на симптоми на инфекция, които може да сочат за наличието на неизвестен вирус. При диагностициране на известни вируси се прилагат предварително зададени правила, докато при неизвестни вируси от наличните данни се извличат нови правила. Понякога и двете техники се комбинират за постигане на оптимални резултати. С помощта на алгоритми за извличане на данни, като Tree Decision и Association Rule, могат да се откриват и неизвестни вирусни инфекции. Освен това могат да бъдат открити и някои скрити вариации на вече известни вируси[10].

В [11] е предложен метод за откриване на компютърни вируси, основан на техника за извличане на данни (Data Mining). Методът е оценен, като е използван набор от изпълними файлове, включващ безобидни и злонамерени такива. Доказано е, че той превъзхожда други методи за класификация, както по отношение на степента на откриване, така и по отношение на точността.

В [12] е илюстриран алгоритъма Random Forest (RFA). Това е класификационен алгоритъм за ML, който конструира класификатор за откриване на зловреден софтуер. Той е много тежък за процесора и не е подходящ за домашни потребители, но може да бъде осъществен на ниво корпоративен шлюз. Така може да действа като централен антивирусен софтуер, допълващ антивирусните програми, инсталирани на компютрите на крайните потребители.

В [13] се оценява ефективността на техниките за машинно обучение при откриване на прониквания в мрежата. Разглежда се модел, предназначен за мрежови системи за откриване на прониквания (NIDS). Моделът, създаден с помощта на ML класификатори, може да се използва заедно с настоящите технологии за откриване на проникване, за да се повиши степента на откриване, да се намалят фалшивите положителни резултати и да се открият неизвестни заплахи.

***Приложения:*** Правилата, създадени от ML модела, разглеждан в [13], могат да се използват в системи за откриване на аномалии, което може да намали усилията, необходими за извършване на обобщение от страна на човешкия експерт. След проведени експерименти на модела с други антивирусни програми става ясно, че мрежова система за засичане на прониквания (NIDS), успява да открие ефикасно злонамерен трафик там, където повечето други програми дават фалшиво отрицателни резултати. Това ясно показва, че ML класификаторите са много по-ефективни от традиционните антивирусни програми. Изграденият в изследването модел е в състояние да открива злонамерен трафик със степен на защита от заплахи (TPR) от около 99,6 % и работи добре и при неизвестни досега данни с точност от 97,5 %. Този модел е в състояние да открива и фалшиви положителни резултати.

Като пример за реално приложение на ML в антивирусните програми може да се посочи софтуерът Hidost[14]. Това е първата статична система за откриване на зловреден

софтуер, базирана на ML, която е проектирана да работи с множество файлови формати. С цел още по-добра точност на откриване, тя комбинира логическата структура на файловете с тяхното съдържание. Hidost надминава всички антивирусни енджини, използвани от уебсайта VirusTotal, в откриването на най-голям брой злонамерени PDF файлове и се нарежда сред най-добрите по отношение на SWF зловреден софтуер. Hidost е по-устойчив срещу непрекъснатото адаптиране от страна на зловредния софтуер към актуализираните защити, като периодично се самообучава.

# 6 Обработка на естествен език за разузнаване и анализ на заплахите (NLP for Cyber Threat Intelligence and Threat Analysis)

***Определение и преимущества***: Разузнаването на киберзаплахите (CTI) се изразява в събирането, обработката и анализа на данни, полезни за разбиране на целите и поведението на атакуващите агенти. В наши дни CTI придобива все по-решаваща роля за идентифициране и намаляване на заплахите и за създаване на проактивни стратегии за защита. В този контекст обработката на естествен език (NLP), се очертава като мощен инструмент, увеличаващ възможностите за разузнаване на заплахите. Изкуственият интелект, и особено техниките на NLP, играят решаваща роля, защото:

• голяма част от информацията е представена като неструктурирани текстови данни (доклади за заплахи, публикации в социалните медии, новинарски статии и хакерски форуми). NLP позволява автоматично обработване на тези текстови данни и разкриването на съответните заплахи и тенденции.

• NLP може да разкрие връзките между субектите и събитията, фигуриращи в текстовите данни, като по този начин помага за контекстуализирането на информацията и за изграждането на по-пълна представа за киберзаплахите и действащите лица, стоящи зад тях.

• може да бъде получена информация за участниците, като се анализират онлайн комуникации, форуми и други текстови източници.

• NLP може да помогне за интегрирането на информация от различни източници и формати в един цялостен поглед, като също така подпомага специалистите по киберсигурност в съставянето и споделянето на доклади.

• NLP се използва и като мощен инструмент за идентифициране на нововъзникващи заплахи и тенденции чрез анализ на големи масиви от данни с текстова информация, като по този начин проактивно се предотвратяват потенциални кибератаки.[15]

***Приложения:*** В [16] е предложена система, която може да се използва за сканиране на Интернет с цел създаване на ситуационна осведоменост и подпомагане на анализаторите на сигурността в идентифицирането на рисковете и заплахите. Модул за филтриране на естествен език класифицира и филтрира текстови документи, свързани с киберсигурността. Събраните и филтрирани документи се анализират от модул Analyzer, за да се определи значимостта и релевантността им за потребителя. Ако анализираните документи са значими и релевантни за потребителя, те се подават към модул Mapper, за да се обогатят с информация за тактиките и техниките на противника, като по този начин се подпомага процесът на анализ на заплахите.

Друг пример за приложение в практиката е SECCMiner - нова система, използваща различни подходи (NLP, stemming, POS tagging и TF-IDF weighting) за извличане на информация от текст и обработка на естествен език. Тя позволява на специалистите по сигурността да анализират неструктурирани доклади за APT (Advanced Persistent Threats) и

да извличат от тях ключови концепции за сигурността, като например техники и тактики на противника[17].

# 7 Заключение

В наши дни ИИ заема ключово място в модернизацията на киберсигурността. Той предлага новаторски подходи за справяне с напредналите и динамично развиващи се заплахи в дигиталното пространство. Технологиите на ИИ демонстрират съществени предимства със своите възможности за автоматизирано засичане и реагиране на атаки, анализ на поведението и обработка на големи обеми от данни в реално време. Приложенията им, разгледани в този доклад, демонстрират висока ефективност и прецизност, надминаващи по точност и адаптивност традиционните методи. Възможността за самообучение и предвиждане на бъдещи заплахи ги превръща в мощен инструмент за проактивна защита.

**ЛИТЕРАТУРА:**

[1] Goswami, M., AI-Based Anomaly Detection for Real-Time Cybersecurity, IJRRT, vol. 3, no. 1, pp. 45–53, Feb. 2024.

[2] Chaudhary, H., Detroja, A., Prajapati, P., Shah P., A review of various challenges in cybersecurity using Artificial Intelligence, 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020.

[3] Bergadano, F., Drago, I., AI for Cybersecurity: from Adversarial Anomaly Detection to Intelligent Network Security Systems, Dipartimento di Informatica, Università di Torino, 2022.

[4] Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., Obunadike, E., Using Artificial Intelligence for automated incidence response in Cybersecurity, International Journal of Information Technology (IJIT) Vol. 1, No. 4, November 2023.

[5] Maddireddy, B., Maddireddy, B., Enhancing Network Security through AI-Powered Automated Incident Response Systems, ijaeti, vol. 1, no. 02, pp. 282–304, May 2023.

[6] Reddy, A., Ayyadapu, A., Automating Incident Response: AI-driven Approaches to Cloud Security Incident Management, CCB, vol. 15, no. 2, pp. 1–10, Dec. 2020.

[7] Kumar, S., Gupta, U., Singh, A. K., Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era, J. Comput. Mech. Manag, vol. 2, no. 3, pp. 31–42, Aug. 2023

[8] Katiyar, N., Tripathi, S., Kumar, P., Verma, S., Sahu A., Saxena, S., AI and Cyber-Security: Enhancing threat detection and response with machine learning, kuey, vol. 30, no. 4, pp. 6273–6282, Apr. 2024.

[9] Olabanji, S., Marquis, Y., Adigwe, C., Ajayi, S., Oladoyinbo, T., Olaniyi, O., AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection (January 29, 2024). Asian Journal of Research in Computer Science 17(3):57-74 (2024)

[10] Truong, M.N.Q., Hoang, T.N., A Multi-agent Mechanism in Machine Learning Approach to Anti-virus System. In: Nguyen, N.T., Jo, G.S., Howlett, R.J., Jain, L.C. (eds) Agent and Multi-Agent Systems: Technologies and Applications. KES-AMSTA 2008.

[11] Altaher, A., Ramadass, S., Ali, A., Computer Virus Detection Using Features Ranking and Machine Learning Australian Journal of Basic and Applied Sciences, 5(9): 1482-1486, 2011, ISSN 1991-8178.

[12] Ahmed, A., Hussan, M.I., Rajesh, D., Implementing Machine Learning Techniques in Malware Detection, International Journal for Research in Engineering Application & Management (IJREAM), Vol-04, Issue-09, Dec 2018, ISSN: 2454-9150.

[13] Kumar, S., Viinikainen, A., Hamalainen, T., Machine Learning Classification Model for Network Based Intrusion Detection System, 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, 5-7 December 2016.

[14] Šrndić, N., Laskov, P. Hidost: a static machine-learning-based detector of malicious files, EURASIP J. on Info. Security 2016, 22 (2016). https://doi.org/10.1186/s13635-016-0045-0

[15] Arazzi, M., et al. NLP-Based Techniques for Cyber Threat Intelligence. ArXiv abs/2311.08807 (2023): n. pag.

[16] Otgonpurev, M., Effective application of Natural Language Processing techniques in Automated Cyber Threat Intelligence, Doctoral thesis, Nagoya University, 2021

[17] Niakanlahiji, A., Wei, J., Chu, T., A Natural Language Processing Based Trend Analysis of Advanced Persistent Threat Techniques, 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 2995-3000

# CYBERATTACKS AND EMERGING TECHNOLOGIES – A DOUBLE-EDGED SWORD*

**ZORNITSA N. MLADENOVA-ANGELOVA, GEORGI T. MANEV**

***ABSTRACT:*** *As our understanding of technology, and technology itself keep progressing, so are the vast possibilities and risks that come with it, one of them being cyberattacks. Essentially cyberattacks are a deliberate attempts to exploit or disturb computer systems, networks or numerous devices, either one at a time, or multiple at once. Their range of targets can consist of individuals, businesses, or governments and often aim to steal data, cause financial damage, or disrupt operations. Cybercrime includes activities like hacking, phishing, ransomware, and more. Notably, if carried out by nation-states, such activities may escalate to cyberwarfare.*

***KEYWORDS:*** *exploit, stealing data, hacking, cyber warfare*

***DOI: https://doi.org/10.46687/UWWU2085***

# КИБЕРАТАКИ И НОВОВЪЗНИКВАЩИ ТЕХНОЛОГИИ – НОЖ С ДВЕ ОСТРИЕТА

**ЗОРНИЦА Н. МЛАДЕНОВА-АНГЕЛОВА, ГЕОРГИ Т. МАНЕВ**

***АБСТРАКТ:*** *С напредването на нашето разбиране за технологията, и самата технология, се развиват и огромните възможности и рискове, които идват с нея, един от които са кибератаките. По същество кибератаките са умишлени опити за използване или нарушаване на компютърни системи, мрежи или множество устройства, едно по едно или няколко наведнъж. Диапазонът им от цели може да се състои от физически лица, фирми или правителства и често целят кражба на данни, причиняване на финансови щети или прекъсване на операции. Киберпрестъпността включва дейности като хакване, фишинг, рансъмуер и др. По-специално, ако се извършват от национални държави, подобни дейности могат да ескалират до кибервойна.*

## 1 Въведение

Кибератаките са нарастваща заплаха за съвременното общество, която може да засегне мрежи, системи и устройства. Те използват слабости в технологиите и човешкото поведение, за да осъществят достъп до важна информация или ресурси. С напредъка на цифровите технологии и все по-голямото им приложение в живота и работата, рисковете стават все по-сериозни. Основният проблем при кибератаките е, че често разчитат не само на технически пропуски, но и на човешки грешки. Липсата на адекватна защита, остарели системи или недостатъчно познания сред потребителите улесняват успеха на подобни атаки. Защитата срещу тях изисква усилия както в технологиите, така и в обучението на хората как да разпознават и предотвратяват заплахите.

Справянето с кибератаките изисква балансиран подход – внедряване на сигурни технологии, редовни актуализации на системите и повишаване на осведомеността на потребителите. Само с координирани усилия и постоянна подготовка могат да се намалят рисковете и да се гарантира сигурност в дигиталния свят. [4, 7, 8]

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

## 2 Видове фишинг атаки

**2.1. Имейл фишинг**: Най-често срещаният метод. Изпращат се подвеждащи имейли, съдържащи фалшиви линкове;

**2.2. Spear фишинг:** Нацелва конкретни хора или организации с персонализирани съобщени**;**

**2.3. SMiShing**: Атаки чрез текстови съобщения (SMS);

**2.4. Clone фишинг**: Дублиране на легитимни имейли с променени линкове**;**

**2.5. Evil twin**: Създаване на фалшиви Wi-Fi мрежи за прихващане на данни**.** Фишинг атаките могат да доведат до значителни финансови загуби и кражба на самоличност, затова е важно да сме информирани и бдителни. Във такъв случай, как бихме могли да се защитим? И за какви знаци и признаци трябва да бъдем внимателни? Защитата не е сръвнително трудна, трябва най вече внимателно да проверяваме подателя на имейлите**,** да не натисмаке върху съмнителни линкове, и да използваме двуфакторна автентация (2FA).




**Фиг 1.** Фишинг атаки

Знаци за опит на фишинг атака са най често следните: Грешки в граматиката или правописа. Искане за спешно действие. Линкове, които не съответстват на очаквания URL адрес. Освен това, често се използват подвеждащи визуални елементи, като например логота или дизайни, наподобяващи легитимни организации. Фишинг имейлите могат да съдържат и прикачени файлове, които след отваряне инсталират злонамерен софтуер. Съобщенията обикновено използват обобщени обръщения като „Уважаеми клиент“, вместо персонализирано име, което е знак за масова атака.

Често срещано е и създаването на усещане за неотложност, например твърдения, че акаунтът ще бъде заключен или че има проблем с плащане. Липсата на контактна информация или използването на подозрителни имейл адреси е друг индикатор за фишинг. Съобщенията могат да съдържат предложения за награди или бонуси, които звучат твърде добре, за да са истина. Допълнително, тези атаки често експлоатират слабости в протоколи за сигурност като SMB, както се случи с WannaCry. [1, 2, 3]

Измамниците често адаптират съобщенията си, за да имитират добре познати компании или институции, което увеличава доверието на жертвите. Те също така може да разчитат на социално инженерство, за да манипулират хората да предоставят достъп до системи или поверителна информация. Защитата от тези заплахи изисква използването на двуфакторна автентификация, редовни актуализации на софтуера и обучение на потребителите за разпознаване на подозрителни съобщения.

# 3 Други видове кибератаки

## 3.1. Ransomware

Това е зловреден софтуер, който криптира данните на жертвата и изисква откуп (обикновено в криптовалута) за възстановяване на достъпа. Най-известните атаки използват фалшиви имейли или заразени уебсайтове. Освен криптиране на данните, някои версии на ransomware също така заплашват да публикуват лична информация, ако откупът не бъде платен. Атаки като WannaCry и Petya са примери за такива заплахи, като те използват известни уязвимости като EternalBlue, за да се разпространяват в мрежите. В много случаи организациите, които не поддържат редовни резервни копия на своите данни, са изправени пред сериозни загуби.

## 3.2. Denial-of-Service (DoS) атаки

Целта е да се претовари мрежов ресурс (уебсайт или сървър) чрез изпращане на огромен обем трафик, което прави услугата недостъпна. DDoS (дистрибутирани DoS) използва множество източници за мащабна атака. DDoS атаките често се осъществяват чрез ботнети – мрежи от компрометирани устройства, които се използват за генериране на трафик. Те не само блокират достъпа до услугата, но могат и да се използват като отвличаща маневра, докато атакуващите проникват в системите. Някои модерни атаки включват използване на IoT устройства, които често са слабо защитени, за мащабни атаки.

## 3.3. Man-in-the-Middle (MITM)

Този тип атаки включват прихващане на комуникацията между две страни. Атакуващият може да чете, променя или подслушва обменените данни без знанието на участниците. За да осъществят MITM атака, киберпрестъпниците често използват несигурни публични Wi-Fi мрежи, за да прихванат данни, изпратени между устройствата и сървърите. Допълнително, атакуващите могат да създадат фалшиви точки за достъп, които изглеждат легитимни, но всъщност служат за събиране на чувствителна информация.

## 3.4. Malware

Общ термин за зловреден софтуер, включващ вируси, червеи, троянски коне и шпионски софтуер. Целта му е кражба на данни, повреда на системи или контрол на устройства. Зловредният софтуер често се използва за инсталиране на бекдор (backdoor) в системите, което позволява на атакуващите да получат постоянен достъп и контрол върху устройствата. Новите варианти на malware използват полиморфни техники, които им позволяват да променят кода си, за да избегнат откриването от антивирусен софтуер. Освен това, зловредният софтуер може да бъде част от по-голяма атака, например да съдейства за разпространение на ransomware или да бъде използван за шпионаж.

# 4 Влиянието на кибератаките върху новите технологии

Кибератаките значително влияят на новите технологии, като поставят предизвикателства пред сигурността на данни, мрежи и устройства. Те засягат както индивидуални потребители, така и цели компании и правителства, създавайки рискове за критичната инфраструктура. [5, 6, 9]

**Информационна сигурност:** Технологиите за съхранение на данни и облачните услуги често са обект на атаки, които могат да доведат до изтичане на чувствителна информация. Това увеличава необходимостта от по-добра защита и криптиране на данните.

**Интернет на нещата (IoT):** Устройства, свързани към интернет, стават все по-уязвими. Атаките срещу тях могат да компрометират цели системи в домакинства или индустриални. Съоръжения.

**Изкуствен интелект и машинно обучение:** Атаките, насочени към тези технологии, могат да манипулират данни, което влияе на точността на алгоритмите и вземането на решения.

**Финансова и критична инфраструктура:** Кибератаките върху банки или електропреносни мрежи могат да доведат до мащабни прекъсвания и икономически щети.

# 5 Как бихме могли да се защитим от тях?

### 5.1. Технически мерки:

**Актуализации на софтуера:** Редовно обновявайте операционните системи, антивирусните програми и приложенията, за да отстраните уязвимости.

**Антивирусен софтуер:** Инсталирайте и поддържайте актуални защитни програми.

**Двуфакторна автентикация (2FA):** Добавете втори слой защита за достъп до акаунти.

**Криптиране на данни:** Защитете чувствителната информация чрез криптиране, особено при съхранение или изпращане онлайн.

**Защитна стена (Firewall):** Използвайте, за да контролирате входящия и изходящия трафик на мрежата.

### 5.2. Добри практики:

**Силни пароли:** Създавайте уникални и сложни пароли, които не съдържат лична информация.

**Внимание към имейли и линкове:** Не отваряйте подозрителни линкове и прикачени файлове от непознати източници.

**Резервни копия (Backup):** Правете редовни резервни копия на важни данни на външни устройства или облачни услуги.

### 5.3. Осведоменост и обучение:

**Обучение на служителите:** Редовно информирайте служители и членове на вашето семейството за нови заплахи и методи на атака (като фишинг и социално инженерство).

### 5.4. Мрежова сигурност:

**Използване на VPN:** Защитете връзката си при използване на публичен Wi-Fi.

**Ограничен достъп:** Ограничете достъпа до чувствителна информация само за оторизирани потребители.

### 5.5. Мониторинг и реакция:

**Системи за мониторинг:** Инсталирайте софтуер за наблюдение на мрежовата активност и откриване на аномалии.

**План за реакция:** Разработете план за действие при инциденти с киберсигурността, който да включва стъпки за ограничаване на щетите и уведомяване на засегнатите страни.

Тези мерки могат значително да намалят риска от кибератаки и да предпазят личната или бизнес информация от злонамерени действия.

# 6 Признаци за предстояща кибератака:

### 6.1 Необичайна мрежова активност:

Рязко увеличаване на входящия или изходящия трафик.

Необяснимо натоварване на сървъри или системи.
Чести опити за влизане (login) от неизвестни IP адреси.

**6.2 Съмнителни имейли или съобщения:**

Получаване на фишинг имейли с линкове или прикачени файлове.
Съобщения, изискващи лична информация или пароли.
Имейли от адреси, които имитират легитимни организации, но съдържат правописни грешки.

**6.3 Неочаквани системни съобщения:**

Предупреждения за неуспешен достъп или активност на акаунта.
Антивирусният софтуер отчита многократни заплахи или опити за проникване.

**6.4 Промени в поведението на системата:**

Забавяне на операционната система или чести сривове.
Необясними промени в конфигурациите или настройки.
Нова инсталирана програма или файл, който не сте добавяли сами.

**6.5 Активност на потребителски акаунти:**

Неоторизирани влизания в акаунти.
Дейности от странни местоположения или устройства.
Опити за смяна на пароли без ваше знание.

**6.6 Необичайна комуникация от вътрешни устройства:**

Непознати устройства, свързани към мрежата.
Опити за комуникация с външни сървъри от устройства, които нямат такъв тип връзка.

**6.7 Достъп до чувствителни данни:**

Следи от опити за достъп до защитени файлове.
Промени в права на достъп, направени без одобрение.
Как да реагирате при съмнение за кибератака:
Изолирайте засегнатата система.
Уведомете IT отдела или специалист по сигурност.
Сканирайте за зловреден софтуер.
Променете паролите на засегнатите акаунти.

**Таблица 1:** *Признаци и действия при предстояща кибератака*

| Признак | Действие за реакция | Отговорен екип |
|---|---|---|
| *Рязко увеличаване на входящия трафик* | *Изолирайте системата от интернет. Проведете мрежов анализ.* | *IT отдел, специалист по сигурност* |
| *Фишинг имейли с линкове* | *Не отваряйте линка.* | *Всички потребители, IT отдел* |
| *Съмнителни логин опити* | *Блокирайте IP адреса. Сканирайте за зловреден софтуер.* | *IT отдел* |
| *Забавяне на системата* | *Проверете активните процеси. Анализирайте последните инсталации.* | *IT отдел* |
| *Неоторизирани влизания в акаунти* | *Смяна на пароли. Проведете проверка на логове.* | *Потребител, IT отдел* |
| *Непознати устройства в мрежата* | *Изключете устройството от мрежата. Проверете за уязвимости.* | *IT отдел* |

## 7 Има ли риск човешкият живот от кибератаките?

Да, кибератаките могат да представляват сериозен риск за човешкия живот, особено когато са насочени към критична инфраструктура или здравни системи. Заразяване на болнични системи може да блокира достъпа до жизненоважна информация за пациенти, като медицински досиета или резултати от изследвания. Например, през 2020 г. в Германия жена почина, след като болница не можа да я приеме поради кибератака. Медицински устройства, като инфузионни помпи или сърдечни монитори, също могат да бъдат компрометирани, което да доведе до опасни ситуации за пациенти. Атаки срещу електроцентрали или водоснабдителни системи могат да доведат до прекъсвания на услугите, застрашавайки живота на хората, особено в болници или по време на природни бедствия. Хакерска намеса в авиационни, железопътни или автомобилни системи може да доведе до катастрофи. Киберзаплахите не са само технологичен проблем, но и директна заплаха за човешкия живот, особено в съвременния дигитално свързан свят.

**Таблица 2:** Категории рискове от кибератаки за човешкия живот

| Категория на риск | Пример за атака | Възможно въздействие върху човешкия живот |
|---|---|---|
| *Здравеопазване* | *Заразяване на болнични системи* | *Забавяне на лечението, липса на достъп до критична информация.* |
| *Медицински устройства* | *Хакване на инфузионни помпи или сърдечни монитори* | *Животозастрашаващи ситуации за пациенти.* |
| *Критична инфраструктура* | *Атаки срещу електроцентрали* | *Прекъсване на ток и вода в болници, застрашаващо пациентите.* |
| *Транспорт* | *Хакване на авиационни, железопътни или автомобилни системи* | *Възможни катастрофи и човешки жертви.* |
| *Природни бедствия* | *Атаки по време на бедствия, когато хората разчитат на дигитални системи за помощ* | *Удължаване на времето за реакция, което увеличава риска за засегнатите хора.* |



**Фиг. 2.** Рискове при кибератаки

# 8 Заключение

Човешкото общество винаги е било в процес на адаптация към новите технологии, което е позволило бързо напредване в различни области. Това обаче не е без своите рискове, особено в контекста на кибератаките, които постоянно се развиват и стават все по-сложни и опасни. Бъдещето на технологиите ще е все по-свързано с цифровизация и автоматизация, като ще бъде важно да се справяме с рисковете, свързани с киберсигурността. [3, 4, 5, 6, 9]

Кибератаките не са просто технологично предизвикателство – те имат потенциал да засегнат критични инфраструктури, здравеопазване, транспортни системи и дори човешкия живот. Атаки като ransomware, DoS, MITM и други показват, че киберзаплахите могат да доведат до сериозни икономически, социални и дори фатални последици. Това налага нуждата от по-добра защита чрез внедряване на съвременни технологии, редовни актуализации на системите и повишаване на осведомеността на потребителите.

За да бъде осигурено бъдеще, в което технологиите служат за напредък, а не за злоупотреби, е необходимо балансирано съчетаване на технически решения, образование и глобално сътрудничество в сферата на киберсигурността. Усъвършенстването на методи за защита, като криптиране, двуфакторна автентификация и мрежов мониторинг, трябва да върви ръка за ръка с обучението на потребителите и разработването на стратегии за реакция при инциденти. В крайна сметка, развитието на технологиите и тяхното интегриране в ежедневието изискват постоянна бдителност и готовност да се справяме с киберрисковете. Само с обединени усилия – както на индивидуално, така и на организационно и национално ниво – можем да изградим устойчиво и сигурно цифрово бъдеще.

**ЛИТЕРАТУРА:**


[1] Ahmedova D., Konstantinova E., Tsankov Ts. The use of packet sniffing tools in computer networks security. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 401-406.

[2] Denev D., Konstantinova E., Main Issues in the Protection of Information in the System of National and Corporate Security, 2020, Conference with international participation MATTEH 2020, Conference proceeding, vol. 2 Communication and Computer Technologies, Shumen, ISSN 1314-3921, pp. 110-115.

[3] 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, 2020, ISSN 2367-7902, pp. 373-378.

[4] Konstantinova E., Tsankov Ts. The invisible Internet and cyber security. International scientific conference 2019, “Vasil Levski” National military university, “Artillery, aircraft defense and CIS” faculty, Shumen, 2019, ISSN 2367-7902, pp. 519-524.

[5] Lilov V., Konstantinova E., Tsankov Ts. Cyber intelligence in protecting organizations from malicious activity. International Scientific Conference “Defense Technologies” DefTech 2020, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2020, ISSN 2367-7902, pp. 386-392.

[6] https://www.microsoft.com/bg-bg/security/business/security-101/what-is-phishing

[7] https://help.abv.bg/какво-е-фишингphishing-и-как-да-се-предпазя/

[8] https://bg.wikipedia.org/wiki/Атака_за_отказ_на_услуга

[9] https://www.infosecinstitute.com/resources/security-awareness/understanding-cyberattacks-types-risks-and-prevention-strategies/

# THE DIGITAL REPRESENTATION OF VIRTUAL IMAGES*

**KIRIL F. YANCHEV**

***ABSTRACT:*** *The paper presents a developed concept for the digital representation of virtual images through the use of three features as pixel values.*

***KEYWORDS:*** *laser scanning, virtual images, spatial data*

***DOI: https://doi.org/10.46687/BKXE4643***

# ЦИФРОВОТО ПРЕДСТАВЯНЕ НА ВИРТУАЛНИ ИЗОБРАЖЕНИЯ

**КИРИЛ Ф. ЯНЧЕВ**

***АБСТРАКТ:*** *Доклада представя разработена концепция за цифровото представяне на виртуални изображения чрез използването на три характеристики като стойности на пиксели.*

## 1 Въведение

Развитието на инструменти за лазерно сканиране до голяма степен стимулира разработването на нови методи за представяне на информация за района, превеждайки информационните технологии от равнина в триизмерно пространство. Триизмерните или виртуалните геоинформационни системи получиха значително развитие, което наложи разработването на принципно нови методи за съхранение, обработка и анализ на пространствени данни.

## 2 Виртуални изображения

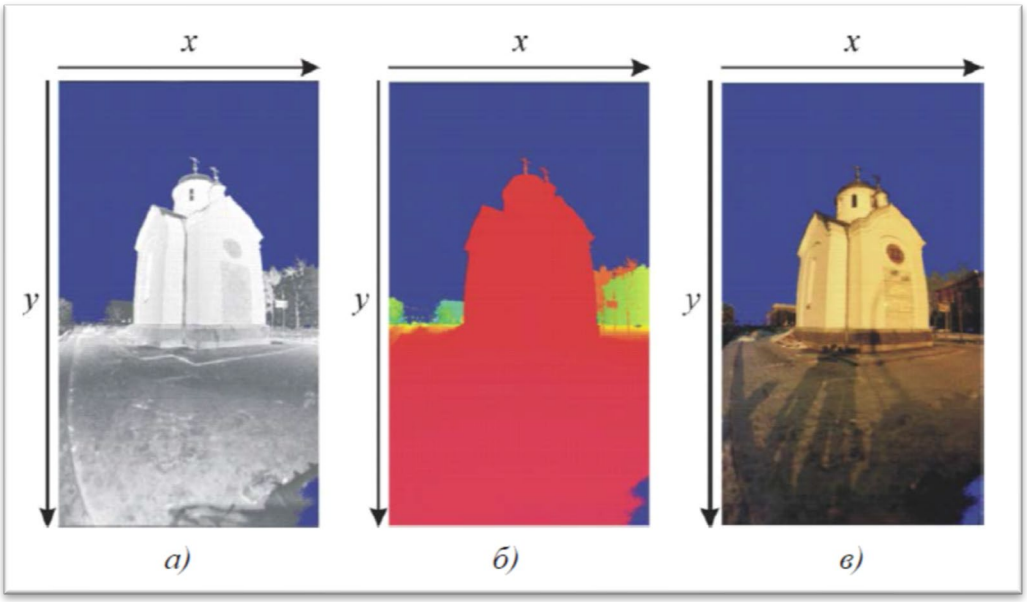
За цифровото представяне на виртуални изображения се използват три характеристики като стойности на пиксели: интензитет, разстояние от скенера до снимания обект и реален цвят (Фиг. 1).

По-целесъобразно е да се използват цифрови виртуални изображения за автоматизирано декодиране, компресиране на изображения и изграждане на цифрови модели.

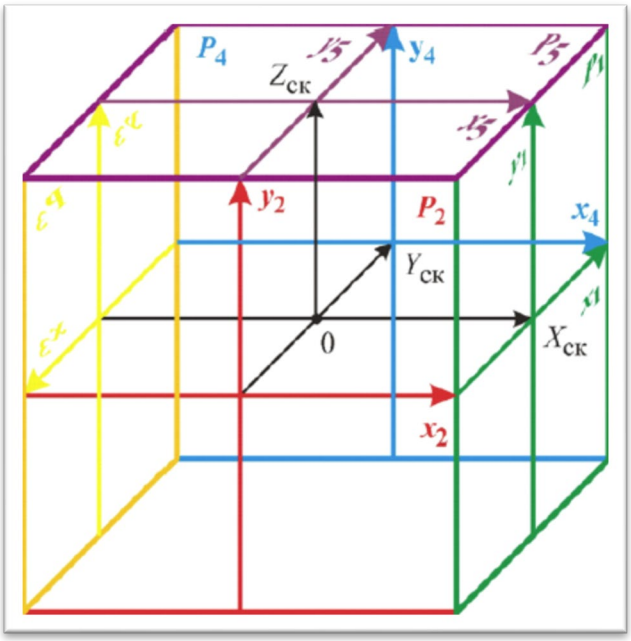
За практическото приложение на тази предложена теория възникват два въпроса: изборът на броя на кадрите и изборът на фокусното разстояние на виртуалните кадри.

Изборът на броя на изображенията трябва да се реши по пътя на минимални разходи за преобразуване на данни и оптимално възприемане на данни. Въз основа на това е най-ефективно да се използват пет изображения на скенера, главните оптични оси, които са разположени за четири изображения в равнината на сканиране $X_{ск}Y_{ск}$ през 90°, а петото изображение е перпендикулярно на равнината $X_{ск}Y_{ск}$. Това позволява да се покрие областта на сканиране на всички произведени скенери само с пет снимки [5, 7]. Тази схема за поставяне на виртуални изображения е показана на (Фиг.2).

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“




**Фиг. 1 Представяне на резултатите от наземно лазерно сканиране под формата на двуизмерни виртуални изображения: а) интензитет на отразения сигнал; б) разстоянието от скенера до снимания обект; в) реални цветове на обекта**




**Фиг. 2 Схема за преобразуване на данните от скенера в пет виртуални изображения**

Подобна схема за поставяне на виртуални изображения не води до видими изкривявания, причинени от преизчисляване от сферична повърхност към централна проекция. По цялото поле на изображението тези изкривявания не надвишават 11% от размера на пиксела (Фиг. 3), което е визуално незначително. В този пример няма видими изкривявания, причинени от сферичността, за разлика от снимките, показани на фигура 1.



**Фиг. 3 Пример за виртуално изображение 90°×90° с цифрово наслагване**

Освен това изборът на такава схема за подреждане на оптични оси значително намалява времето за външна ориентация [6]. Тъй като елементите на направляващата косинусова матрица за всички изображения, получени от една станция, са едни и същи и при преместване от изображение на изображение вътре в сканирането елементите на косинусовата матрица на посоката променят само своето местоположение и знак (Таблица 1), това значително намалява машинното време за математически операции, които могат да се извършват с виртуални изображения.

**Таблица 1 - Изглед на матрицата от косинуси на посоката в рамките на едно сканиране за пет виртуални изображения**

| номер на снимка | снимка 1 | снимка 2 | снимка 3 | снимка 4 | снимка 5 |
|---|---|---|---|---|---|
| ъгъл на завъртане не снимката | $\chi = 0°$; $\tau = 0°$ | $\chi = 90°$; $\tau = 0°$ | $\chi = 180°$; $\tau = 0°$ | $\chi = 270°$; $\tau = 0°$ | $\chi = 0°$; $\tau = 90°$ |
| вид на косинусиновата матрица | $\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$ | $\begin{vmatrix} -a_2 & a_1 & a_3 \\ -b_2 & b_1 & b_3 \\ -c_2 & c_1 & c_3 \end{vmatrix}$ | $\begin{vmatrix} -a_1 & -a_2 & a_3 \\ -b_1 & -b_2 & b_3 \\ -c_1 & -c_2 & c_3 \end{vmatrix}$ | $\begin{vmatrix} a_2 & -a_1 & a_3 \\ b_2 & -b_1 & b_3 \\ c_2 & -c_1 & c_3 \end{vmatrix}$ | $\begin{vmatrix} a_1 & -a_3 & a_2 \\ b_1 & -b_3 & b_2 \\ c_1 & -c_3 & c_2 \end{vmatrix}$ |

Фокусното разстояние трябва да бъде избрано от по-нататъшните задачи, които трябва да бъдат решени. В първия случай, ако е необходимо изображения, получени от цифров фотоапарат да се наслагват върху виртуални изображения, т.е. да се получат виртуални изображения в реални цветове, тогава за тях е необходимо да се избере фокусно разстояние, равно на фокусното разстояние на насложеното цифрово изображения [2, 4]. Ако няма такава задача, тогава е по-целесъобразно да зададете кратно на 100. Това позволява значително да се намали времето, прекарано на машината за конвертиране на виртуални изображения. Тъй като задачата за изчисляване на координатите на плоски

виртуални изображения всъщност се свежда до изчисляване само на тангенси, т.е., като по този начин се намалява операцията на умножение по фокусното разстояние.

# 3 Заключение

От цялото разнообразие на нови технически средства специално място заемат лазерните геодезични системи, които с оглед на своите предимства значително разширяват възможностите на теорията и практиката на фототопографския метод за събиране на пространствени данни [1, 3]. Основните предимства на такива системи са: автоматизация на процеса на събиране на информация, висока степен на детайлност и др. В днешно време теорията и технологията на лазерното сканиране не са достатъчно развити.

**ЛИТЕРАТУРА:**

[1] Диманова Д, "Алгоритъм на програма за моделиране честотата на природни бедствия". НК MATTEX 2014, ШУ "Епископ Константин Преславски" 20-22 ноември 2014, Шумен, ISSN: 1314-3921. pp. 172-176.

[2] Добрев, С., (2020). Изследване на бреговата ивица на водоеми с фотограметрични методи. MATTEX 2020, 24-26 ОКТОМВРИ 2020 г., ISSN: 1314-3921.

[3] Иванов С. ”Картографски приложения от дистанционни методи”. MATTEX 2020 - сборник научни трудове. Университетско издателство ”Еп. К. Преславски”. Шумен 2020. ISSN 1314-3921. стр. 262-265.

[4] Иванов, И., Проблемът кадастър и регулация – изменение на кадастралната карта чрез използване на графични материали, MATTEX 2022: Сборник научни трудове, Том 2, Университетско издателство “Епископ Константин Преславски“, Шумен, 2022, ISSN: 1314-3921, стр. 258 - 264.

[5] Пламен Михайлов, Божидар Стоянов, Евгени Стойков, „Заснемане на шуменската крепост с безпилотно летателно средство и орторектифициране – оценка на точността“ сп. "Геодезия, Картография, Земеустройдтво", Брой 5-6/2017 г., год. LVII, Издание на Съюза на геодезистите и земеустроителите в България - ФНТС, 9-13 стр., ISSN 0324-1610.

[6] Хасан, С., Ниязи-Юсуф, М., „Източници на йонизиращи лъчения“, Сборник доклади от Международна научна конференция „Радиационната безопасност в съвременния свят“ 15-17 ноември 2023 година, Велико Търново, Том 2, Издателски комплекс на НВУ „Васил Левски“, ISSN 2738-7607 Print, ISSN 2603-4689 CD, DOI: 10.34660/INF.2023.92.38.028, стр. 73-78

[7] Янчев К., Кирилова К., Наземно лазерно сканиране. Шумен: Научна конференция с международно участие MATTEX 2022. Сборник научни трудове, Том 2, Шумен, ISSN: 1314-3921, стр. 226-230..

# CONVERTING SCANNER DATA INTO VIRTUAL IMAGES*

**KIRIL F. YANCHEV**

***ABSTRACT:*** *The report presents a developed concept for new methods of presenting information about the area, translating information technology from a plane to a three-dimensional space.*

***KEYWORDS:*** *laser scanning, virtual images, spatial data*

***DOI: https://doi.org/10.46687/ABKV7580***

# ПРЕОБРАЗУВАНЕ НА ДАННИТЕ ОТ СКЕНЕРА ВЪВ ВИРТУАЛНИ ИЗОБРАЖЕНИЯ

**КИРИЛ Ф. ЯНЧЕВ**

***АБСТРАКТ:*** *Доклада представя разработена концепция за нови методи за представяне на информация за района, превеждайки информационните технологии от равнина в триизмерно пространство.*

## 1 Въведение

Развитието на инструменти за лазерно сканиране до голяма степен стимулира разработването на нови методи за представяне на информация за района, превеждайки информационните технологии от равнина в триизмерно пространство [2, 4]. Триизмерните или виртуалните геоинформационни системи получиха значително развитие, което наложи разработването на принципно нови методи за съхранение, обработка и анализ на пространствени данни.

## 2 Цифрови изображения.

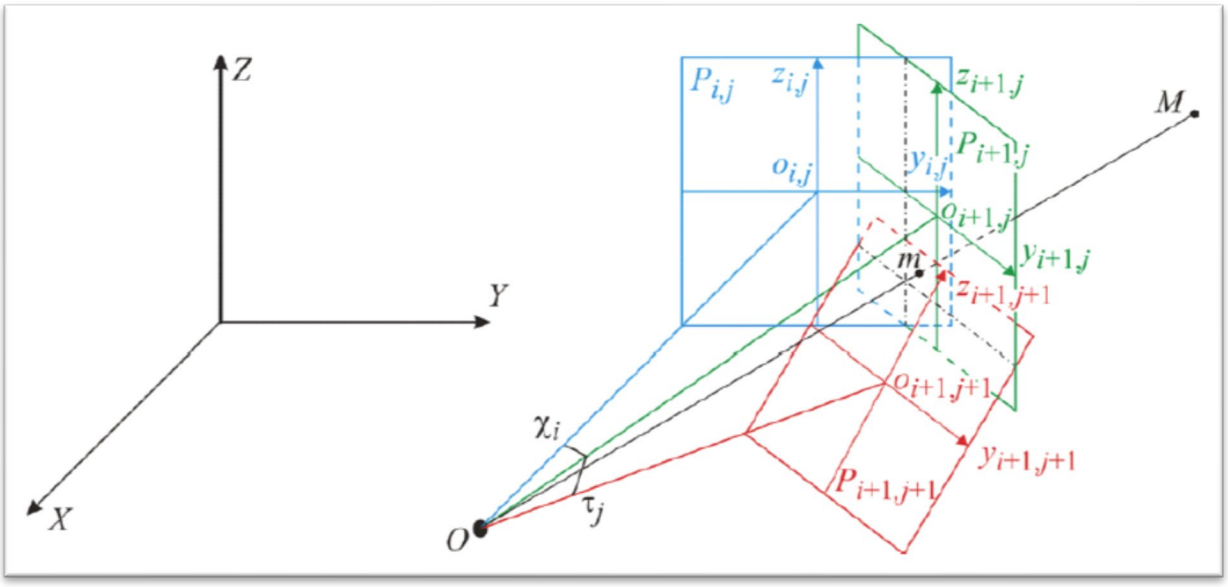
Един от основните проблеми на обработката на данни за наземно лазерно сканиране е ниската производителност. Така например в съществуващите софтуерни продукти времето, прекарано за изграждане на триизмерни модели или цифрови планове или чертежи на фасади, спрямо продължителността на лазерното заснемане е пропорционално $\frac{(5-9)}{1}$. Това обстоятелство компенсира предимството на значителното намаляване на обема на работа на терен, което възпрепятства развитието на технологията за наземно лазерно сканиране. Поради това се предлага използването на фотограметрични принципи за обработка на данни от наземно лазерно сканиране.

Същността на идеята за използване на фотограметрични принципи се крие в трансформирането на данните от наземно лазерно сканиране в набор от виртуални изображения, съответстващи на централната проекция [6].

За да се реализира тази идея, сканирането трябва да бъде представено като набор от измерени посоки, т.е. група лъчи, които на определено разстояние *f* от точка *O* от равнината *P*, сякаш получаваме картина. В този случай един от лъчите, излизащи от точка *O*, трябва

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

да пресича равнината *P* ортогонално (Фиг.1). В този случай формираните плоски виртуални изображения отговарят на централна проекция.




**Фиг. 1 Формиране на изображения от данни от наземно лазерно сканиране**

Фигура 1 показва, че линейните елементи на външната ориентация за всички изображения, направени от една скенерна станция, са еднакви. Ъгловите елементи на външно ориентиране се различават по ъгли $\chi_i$, $\tau_i$, т.е. аргументите на матрицата на косинусите на посоката ще бъдат $\varepsilon + \tau_i$, $\eta$, $\xi + \chi_j$, където $i = (0, 1, 2,\ldots, n)$, $j = (0, 1, 2,\ldots, k)$. Тази матрица в общ вид може да бъде представена по следния начин

$$A_{\varepsilon+\tau_j,\eta,\xi+\chi_i} = A_{\varepsilon,\mu,\xi} * A_{\chi_i} * A_{\tau_j}, \qquad (1)$$

където:

$$A_{\varepsilon,\eta,\xi} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix},$$

$$A_{\chi_i} = \begin{vmatrix} cos\chi_i & sin\chi_i & 0 \\ -sin\chi_i & cos\chi_i & 0 \\ 0 & 0 & 1 \end{vmatrix},$$

$$A_{\tau_j} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & cos\tau_j & sin\tau_j \\ 0 & -sin\tau_j & cos\tau_j \end{vmatrix}.$$

Нека умножим матриците $A_{\varepsilon,\mu,\xi}$, $A_{\chi_i}$, $A_{\tau_j}$. Тогава изразът (1) приема формата

$$A_{\varepsilon+\tau_j,\eta,\xi+\chi_i} = \begin{vmatrix} e_1 & e_2 & e_3 \\ g_1 & g_2 & g_3 \\ q_1 & q_2 & q_3 \end{vmatrix}, \qquad (2)$$

където:

$$
\begin{aligned}
e_1 &= a_1 cos_{\chi_i} - a_2 sin_{\chi_i},\\
e_2 &= (a_1 sin_{\chi_i} + a_2 cos_{\chi_i}) cos_{\tau_j} - a_3 sin_{\tau_j},\\
e_3 &= (a_1 sin_{\chi_i} + a_2 cos_{\chi_i}) sin_{\tau_j} + a_3 cos_{\tau_j},\\
g_1 &= b_1 cos_{\chi_i} - b_2 sin_{\chi_i},\\
g_2 &= (b_1 sin_{\chi_i} + b_2 cos_{\chi_i}) cos_{\tau_j} - b_3 sin_{\tau_j},\\
g_3 &= (b_1 sin_{\chi_i} + b_2 cos_{\chi_i}) sin_{\tau_j} + b_3 cos_{\tau_j},\\
q_1 &= c_1 cos_{\chi_i} - c_2 sin_{\chi_i},\\
q_2 &= (c_1 sin_{\chi_i} + c_2 cos_{\chi_i}) cos_{\tau_j} - c_3 sin_{\tau_j},\\
q_3 &= (c_1 sin_{\chi_i} + c_2 cos_{\chi_i}) sin_{\tau_j} + c_3 cos_{\tau_j}.
\end{aligned}
$$

Правоъгълните координати в изображението се изчисляват, както следва:

$$
\left.
\begin{aligned}
x_{i,j} &= ftg(\varphi - \chi_i)\\
y_{i,j} &= ftg(\theta - \tau_j - 90)
\end{aligned}
\right\}. \tag{3}
$$

За свързване координатите на точките на изображението с пространствените координати на съответните точки се използват уравнения за колинеарност:

$$
\left.
\begin{aligned}
y_{i,j} - y_0 &= f\frac{e_2(X_M - X_0) + g_2(Y_M - Y_0) + q_2(Z_M - Z_0)}{e_1(X_M - X_0) + g_1(Y_M - Y_0) + q_1(Z_M - Z_0)}\\
z_{i,j} - z_0 &= f\frac{e_3(X_M - X_0) + g_3(Y_M - Y_0) + q_3(Z_M - Z_0)}{e_1(X_M - X_0) + g_1(Y_M - Y_0) + q_1(Z_M - Z_0)}
\end{aligned}
\right\}, \tag{4}
$$

където:

$x_0$, $y_0$ – координати на центъра за проекция на изображението;

$X_M$, $Y_M$, $Z_M$ – пространствени координати на точките на обекта.

За изображения, образувани от данни от наземно лазерно сканиране, $x_0$, $y_0$ са равни на нула.

В допълнение към вертикалните и хоризонталните ъгли, НЛС измерва разстоянието $R$, което е свързано с линейни елементи за външна ориентация и пространствени координати на точките на обекта, както следва

$$
R = \sqrt{(X_M - X_0)^2 + (Y_M - Y_0)^2 + (Z_M - Z_0)^2}. \tag{5}
$$

Израз (5) определя дължината на вектора на посоката до точката от обекта. Традиционно, за да го намерите, се използва двойка изображения с взаимно припокриване.

Въз основа на тази теория могат да бъдат създадени два вида изображения: аналитични и цифрови. Първият изглед е показан в Таблица 1, където елементите на изображението са разстоянията, измерени от скенера [1, 3]. По-целесъобразно е използването на аналитични виртуални изображения за решаване на изчислителни проблеми, т.е. външна ориентация на сканирания, настройка на скан-триангулачни конструкции, внедряване на автоматични алгоритми за изграждане на триизмерни модели и др. В днешно време този тип от виртуални изображения може да се използва само за решаване на първите два проблема от изброените по-горе.

**Таблица 1 - Пример за аналитично виртуално изображение на контролни точки**

| номер на точка | x, mm | y, mm | R, m |
|---|---|---|---|
| Tar 4.5 | 42,184 | –8,069 | 18,367 |
| Tar 4.6 | 48,343 | –8,176 | 18,520 |
| Tar 5.1 | –82,631 | 1,378 | 39,343 |
| Tar 5.2 | –81,466 | 1,437 | 40,550 |
| Tar 5.3 | –40,328 | 2,775 | 60,800 |
| Tar 5.4 | –37,899 | 2,722 | 60,815 |
| Tar 5.5 | 5,081 | 1,900 | 58,258 |
| Tar 5.6 | 7,813 | 1,812 | 58,024 |
| Tar 5.7 | 24,393 | –2,034 | 34,408 |
| Tar 5.8 | 24,140 | –2,222 | 32,550 |

# 3 Заключение

Благодарение на бързото развитие на техническите средства, съвременното дистанционно наблюдение е в състояние да предостави на различни научни и промишлени структури пространствено-времеви данни за теренни обекти, инженерни конструкции и релеф [5, 7]. Такива данни са необходими за решаване на екологични, управленски и различни инженерни проблеми, както и за автоматизиран анализ при управлението на територии на базата на триизмерна геоинформационна поддръжка.

**ЛИТЕРАТУРА:**


[1] Диманова Д, "Алгоритъм на програма за моделиране честотата на природни бедствия". НК MATTEX 2014, ШУ "Епископ Константин Преславски" 20-22 ноември 2014, Шумен, ISSN: 1314-3921. pp. 172-176.

[2] Добрев, С., (2020). Изследване на бреговата ивица на водоеми с фотограметрични методи. MATTEX 2020, 24-26 ОКТОМВРИ 2020 г., ISSN: 1314-3921.

[3] Иванов С. ”Картографски приложения от дистанционни методи”. MATTEX 2020 - сборник научни трудове. Университетско издателство ”Еп. К. Преславски”. Шумен 2020. ISSN 1314-3921. стр. 262-265.

[4] Иванов, И., Проблемът кадастър и регулация – изменение на кадастралната карта чрез използване на графични материали, MATTEX 2022: Сборник научни трудове, Том 2, Университетско издателство “Епископ Константин Преславски“, Шумен, 2022, ISSN: 1314-3921, стр. 258 - 264.

[5] Пламен Михайлов, Божидар Стоянов, Евгени Стойков, „Заснемане на шуменската крепост с безпилотно летателно средство и орторектифициране – оценка на точността“ сп. "Геодезия, Картография, Земеустройдтво", Брой 5-6/2017 г., год. LVII, Издание на Съюза на геодезистите и земеустроителите в България - ФНТС, 9-13 стр., ISSN 0324-1610.

[6] Хасан, С., Ниязи-Юсуф, М., „Източници на йонизиращи лъчения“, Сборник доклади от Международна научна конференция „Радиационната безопасност в съвременния свят“ 15-17 ноември 2023 година, Велико Търново, Том 2, Издателски комплекс на НВУ „Васил Левски“, ISSN 2738-7607 Print, ISSN 2603-4689 CD, DOI: 10.34660/INF.2023.92.38.028, стр. 73-78

[7] Янчев К., Кирилова К., Наземно лазерно сканиране. Шумен: Научна конференция с международно участие MATTEX 2022. Сборник научни трудове, Том 2, Шумен, ISSN: 1314-3921, стр. 226-230.

# ACOUSTIC FIELD AND PHYSICAL CHARACTERISTICS OF SEA WATER*

**EVGENI G. STOYKOV**

***ABSTRACT:*** *Depth determination is a major task of the hydrographer, who must have specific knowledge of the environment, underwater acoustics, available depth measurement devices, additional measurement sensors, and the correct procedures to achieve internationally recommended standards of accuracy and range.*

***KEYWORDS:*** *acoustic field, temperature, salinity*

***DOI: https://doi.org/10.46687/MUQR3097***

# АКУСТИЧНО ПОЛЕ И ФИЗИЧЕСКИ ХАРАКТЕРИСТИКИ НА МОРСКАТА ВОДА

**ЕВГЕНИ Г. СТОЙКОВ**

***АБСТРАКТ:*** *Определянето на дълбочината е основна задача на хидрографа, който трябва да има специфични познания за средата, подводната акустика, наличните устройства за измерване на дълбочината, допълнителни сензори за измерване и правилните процедури за постигане на международно препоръчаните стандарти за точност и обхват.*

## 1 Въведение

През последното десетилетие хидрографското проучване претърпява концептуална промяна в технологията и методологията за измерване на дълбочината. Многофункционалните ехолоти (MBES – Multibeam echo sounders) и въздушните лазерни системи (ALS – Airborne laser sounding systems) вече осигуряват почти пълно покритие на морското дъно и измерване на дълбочината. Високата плътност на данните доведоха до огромни батиметрични и много допълнителни данни.

## 2 Акустично поле

Акустичните вълни се състоят от фини вариации на полето на налягане във водата. Частиците на морската вода се движат надлъжно, напред и назад, в посока на разпространението на вълната, като произвеждат съседни области на компресия и разширение.

Интензивността на акустичната вълна *I* е количеството енергия за секунда, пресичащо единична площ.

$$I = \frac{p_e^2}{\rho . c} \quad (1)$$

където $\rho$ е плътността на водата, $c$ е скоростта на звука във водата и $pe$ е ефективното акустично налягане, получено от амплитудата на пиково налягане, $P$:

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

(2) $$p_e = \frac{P}{\sqrt{2}}.$$

Интензитетът на акустичните вълни се изчислява, като се използва средно акустично налягане, а не мигновени стойности. Акустичното налягане и интензитетът, дължащи се на голямото им вариране на обхвата, обикновено се изразяват в логаритмични скали, отнасящи се до нивата на налягане и интензивност, като децибелната скала е най-често срещаната логаритмична скала. Нивото на акустичната интензивност *IL* се определя чрез:

(3) $$IL = 10.\log_{10}\frac{I}{I_{ref}},$$

където $I_{ref}$ е референтната интензивност.
Нивото на акустичната интензивност може да се изрази и чрез:

(4) $$IL = 20.\log_{10}\frac{p_e}{p_{ref}},$$

където $p_{ref}$ е референтното налягане [1, 3].

## 3 Физически характеристики на морската вода

**Температурата** на морската повърхност варира в зависимост от географското положение на земята, сезона на годината и времето на деня [2]. Разпределението на температурното поле е сложно и не може да се предвиди с достатъчна точност за хидрографски изследвания. Такава непредсказуемост изисква цялостно разпределение на профилите на скоростта на звука, както във времето, така и в пространството, за да се поддържа представителна извадка на профилите на скоростта на звука за зоната на изследване. Измерването на дълбочината е доста чувствително към измененията на профила на скоростта на звука. Промяната в температурата от един градус Целзий се превръща в приблизително 4,5 m/s промяна на скоростта на звука. Изменението на температурата е основен фактор за промяната на скоростта на звука между повърхността и долната граница на термоклина, след което налягането става с основно влияние. Термоклин се нарича още слоят на прекъсване или термичен слой. Термоклинът съответства на вертикален отрицателен температурен градиент в някои слоеве на водния стълб, който е значително по-голям от градиентите над и под него [4].

**Соленост**та е мярка за количеството разтворени соли и други минерали в морската вода. Солеността е масата в грамове на всички твърди минерални разтворени вещества в 1 kg морска вода, при условие че бромът е заместен с еквивалентно количество хлор, карбонатите са приведени към окиси, а органичните вещества са изгорени при температура 480°C. Количествено солеността се изразява в g/kg, т. е. в промили – S (‰). Поради голямото съдържание на хлорни аниони в морската вода на практика солеността се определя според хлорността ‰ – съдържанието в грамове на хлора и брома в 1 кг морска вода и преизчисляване на еквивалентното съдържание на хлора.

Солеността се определя по емпиричната формула на Кнудсен, Форх, Сьоренсен: S‰ = 0,030 + 1,8050 Cl‰. За Черно море емпиричната формула за определяне на солеността е:

S‰ = 0,1856 + 1,7948 Cl‰. От 1963 г. емпиричната формула за солеността е преобразувана по предложение на група експерти по океаноложки таблици и стандарти при ЮНЕСКО във вида S‰ = 1,80655 Cl‰.

Средната соленост на световния океан е около 35 ‰, но тя варира в различните морета: Балтийско – 11 ‰, Каспийско – 13 ‰, Азовско – 14 ‰, Черно море – 18 ‰, Средиземно море – 38 ‰, Червено море – 42 ‰, Аралско – 100 ‰, Мъртво – 310 ‰ и др. Химическият състав на черноморските води има някои специфични особености. Поради големия речен сток (353 км³/год) солеността на Черно море е почти два пъти по-ниска от тази на Световния океан.

Скоростта на изменение на скоростта на звука е приблизително 1,3 m/s за 1 ‰ промяна в солеността. Солеността може да се определи и като се използва наблюдаваната електрическа проводимост.

**Налягането** също оказва значително влияние върху изменението на скоростта на звука. Налягането е функция на дълбочината и промяната на скоростта на звука е приблизително 1,6 m/s за всеки 10 атмосфери, т.е. приблизително на всеки 100 метра дълбочина. Налягането оказва голямо влияние върху скоростта на звука в дълбоките води.

**Плътността** на водата зависи от споменатите вече параметри, т.е. температура, соленост и налягане. Петдесет процента от океанските води имат плътност между 1027,7 и 1027,9 kg/m$^3$. Най-голямо влияние върху плътността има сгъстяването с увеличаване на дълбочината. Вода с плътност 1028 kg/m$^3$ на повърхността би имала плътност от 1051 kg/m$^3$ на дълбочина 5000 метра [5].

# 4 Заключение

Морската вода е средата, в която обикновено се извършват хидрографски измервания, поради което познаването на физическите свойства на морската вода и разпространението на акустичните вълни е важно условие.

**ЛИТЕРАТУРА:**

[1] International Hydrographic Organization, Manual on Hydrography, Publication C-13, May 2005, (Corrections to February 2011), Chapter 1, 2 and 3.

[2] Pickard, G. and W. Emery, “Descriptive Physical Oceanography – An Introduction, 5th edition” Pergamon Press, Oxford, 1990.

[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] Кирилова, К., Янчев, К. „Отчитане на атмосферното влияние при планиране на геодезически дейности“. Шумен: Университетско издателство „Епископ Константин Преславски“, Годишник на ШУ, Технически науки. Том XI E, 2021, стр. 44-49, ISSN: 1311-834X.

[5] Добрев С., Анализ на геодезическите методи за изследване на деформациите на хидротехнически обекти. Научна конференция с международно участие MATTEX 2018, Шумен, стр. 147-156, ISSN: 1314-3921

# STRATEGY EXECUTION FOR ALLOCATION OF TERRITORIES FOR LONG-TERM DEVELOPMENT*

**RUMYANA K. TODOROVA, KRASIMIRA K. KIRILOVA**

***ABSTRACT:*** *The report presents a developed concept for the creation of a planning zone for carrying out a strategy in the territorial and spatial development of part of the "St. Nikola", the city of Varna, ensuring the most favorable conditions for "living", working", "leisure" and "service" for the people living in this neighborhood, in compliance with the requirements of Art. 104, para. 1 of the Spatial development act.*

***KEYWORDS:*** *detailed layout plan-regulation and development plan, investment design, research*

***DOI: https://doi.org/10.46687/STSI5472***

# ПРОВЕЖДАНЕ НА СТРАТЕГИЯ ЗА ОБОСОБЯВАНЕ НА ТЕРИТОРИИ ЗА ДАЛЕКОПЕРСПЕКТИВНО РАЗВИТИЕ

**РУМЯНА К. ТОДОРОВА, КРАСИМИРА К. КИРИЛОВА**

***АБСТРАКТ:*** *Доклада представя разработена концепция за създаване на устройствена зона за провеждане на собствена стратегия при териториалното и пространствено изграждане на част от квартал „Св. Никола“, гр. Варна, като се осигурят възможно най-благоприятните условия за „живеене“, труд“, „отдих“ и „обслужване“ на хората, живеещи в този квартал, като се спази изискването на чл. 104, ал. 1 от ЗУТ.*

## 1 Въведение

Високите темпове на строителство, почиващи на силното търсене на жилищни и нежилищни площи, налагат анализ на нови възможности за реализация на инвестиционни намерения. При изчерпване на потенциалните близкоперспективни разширения и възможности за рециклиране на вече урбанизирани територии, в рамките на времевия интервал на действие на прогнозите, заложени в Общите устройствен планове се налага обособяването на територии за далекоперспективно развитие. Тези територии попадат в различни видове устройствени зони – жилищни, за обществено обслужване, смесени многофункционални, производствени и т.н., съобразени с действащите подробни устройствени планове и трябва да осигуряват условия за развитие на основните функционални системи „Обитаване“, „Труд“, „Отдих“, „Обществено обслужване“, „Транспортно-комуникационна инфраструктура“, „Друга техническа инфраструктура“, „Културно-историческо наследство“, като се основават на анализа на тяхното настоящо териториално проявление и състояние, респ. процесите и проблемите, свързани с управлението на устройствения процес и реализацията на инвестиционните инициативи.

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

# 2 Инвестиционно проектиране. Обект на инвестиционното проектиране

Доклада представя концепция за създаване на устройствена зона за провеждане на собствена стратегия при териториалното и пространствено изграждане на част от квартал „Св. Никола“, гр. Варна, осигурявайки възможно най-благоприятните условия за „живеене“, труд“, „отдих“ и „обслужване“ на хората, живеещи в този квартал, като се спази изискването на чл. 104, ал. 1 от ЗУТ. „*Предвижданията на ОУП, с които се определят общата структура и преобладаващото предназначение на територията, видът и предназначението на техническата инфраструктура и опазването на околната среда и обектите на културно-историческото наследство са задължителни при изготвяне на подробните устройствени планове.“[2].*

## 2.1. Прединвестиционни проучвания. Анализ на съществуващото положение [8]

Теренът притежава специфични качества. Сградата и другите обекти се разполагат с отчитане релефа на местността, който влияе върху композицията на обемите и пространствата [9].

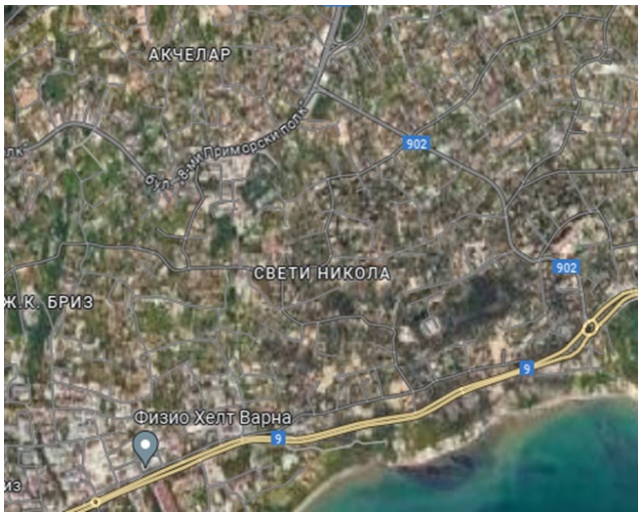
След посещение на квартала с цел натрупване на лични впечатления и наблюдения и след проучване на отделни компоненти на специализираната карта на изследваната територия, ще се спрем, преди всичко, на анализа на:

- **Природна среда**

Местност „Св. Никола“ е със статут на квартал на гр. Варна с решение на Общински съвет Варна от 2000 г. и е в строителните граници на града, съгласно Общия устройствен план (ОУП) на гр. Варна, одобрен със заповед № РД-02-14-2200/03.09.2012 г. на Министъра на МРРБ. Намира се на изток от гр. Варна, в посока на курортен комплекс “Златни пясъци“. Границте на разработваната територия са следните:

- от Север- бул. „Осми Приморски полк“
- от Изток- ул. Арх. Манол Йорданов“
- от Юг- ул. „Сирма войвода“
- от Запад- жк „Бриз“

Теренът е силно наклонен от север на юг към морето, като по западната му граница преминава дере в посока север-юг, което е естествено залесено и спомага оттичането на дъждовните води.

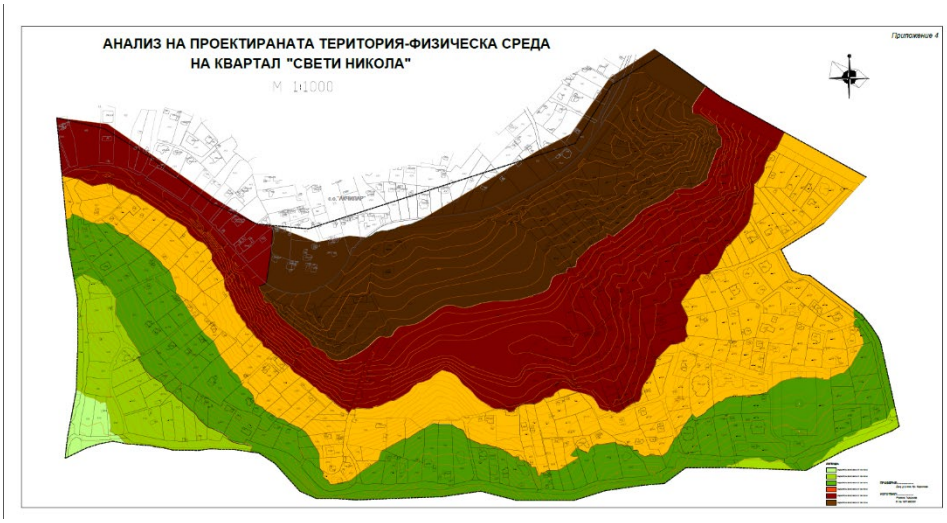



**Фиг. 1 Сателитна снимка на кв. „Св. Никола“.**

Изложението на квартала е изцяла южно, с невероятна морска панорама, която е осветена от слънцето почти през целия ден, което е предпоставка за все по-големия интерес за елитарно жилищно застрояване и причина за високите пазарни цени на имотите. Местоположението на квартала, в близост до морската градина, както и до морските плажове, невероятната морска панорама създава предпоставки и става причина все повече хора да изявяват желание да построят своя дом в него.

Растителността се състои изцяло от култивирана растителност – овощни дървета, декоративни храсти, както и зеленчукови насаждения.

Въз основа на извършения анализ на природната среда [1] се изработи аналитична структурна схема (Фиг. 2), като върху нея са отразени хоризонталите на цялата територия, превишенията, наклона на терена, изложението и др. Информацията и данните от тази схема се използват при проектирането на нови улици и техния наклон, ориентиране на новите сгради към посоката на ослънчаване, посоката на отвеждане на повърхностните води и др.




**Фиг. 2 Анализ на физическата среда на кв. „Св. Никола“**

- **Антропогенна среда**

Анализът на антропогенните елементи обхваща основните проектно-технически параметри на изследваната територия:

- **Градоустройствен статут**

През 1936 г. за квартала е разработен регулационен план, който е частично приложен. През 1977 г. е изработен кадастрален план по фотограметричен метод, а през 1990 г. със заповед на Министъра на Териториално и селищно устройство, получава статут на вилна зона.

През 1991 г. е разработен ПРЗ, за който след първо обявяване на заинтересованите собственици, процедурата за одобряване е прекратена.

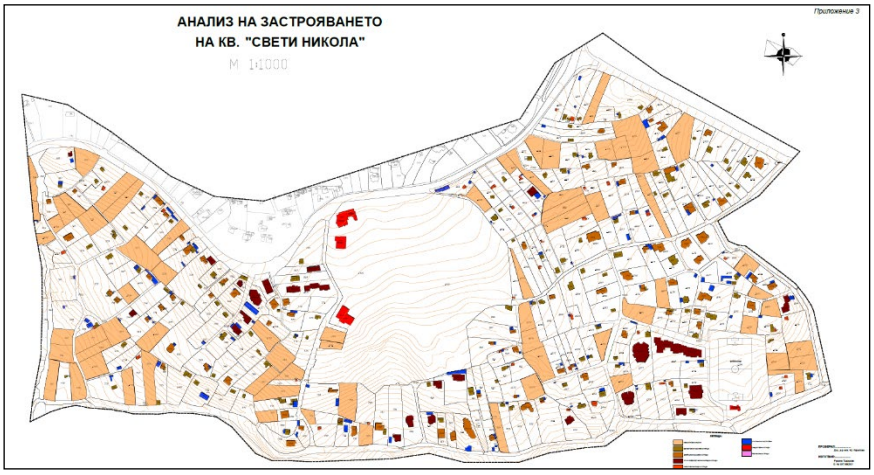
През 2008 г. е одобрен ПНИ-план на новообразуваните имоти.

Около 90% от общия брой на имотите са застроени с по една или повече сгради, включително и допълващо застрояване.

Завареното строителство е предимно вилно – с площ на сградите 35 кв.м.

Въз основа на извършения анализ на сградния фонд се изработи аналитична структурна схема на застрояването, в която с различни цветове са нанесени съществуващите едноетажни масивни сгради, жилищни сгради на два, три и повече етажа,

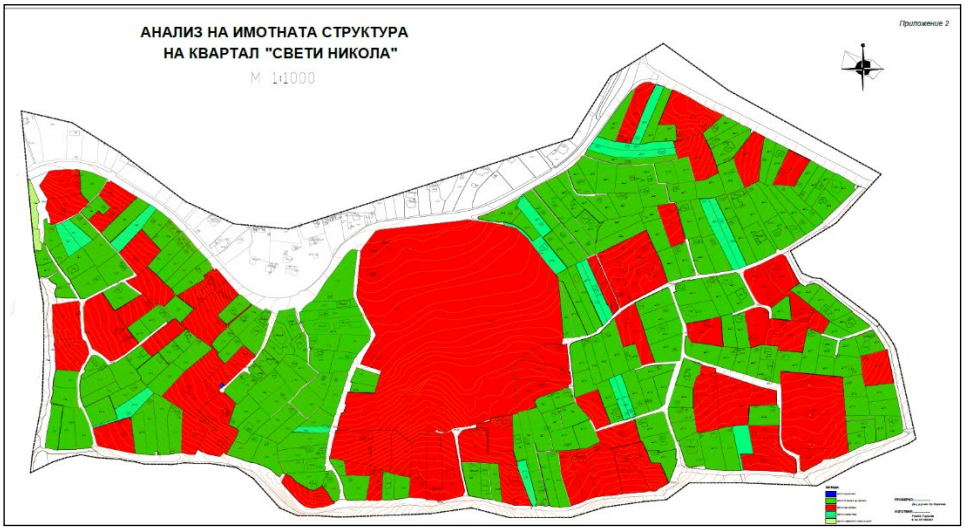
паянтовите сгради и сгради на допълващото застрояване-гаражи, стопански постройки, сгради за отглеждане на животни и съхранение на инвентар, земеделска продукция и др., както и незастроените имоти. Тази информация се използва при определяне местоположението на зоните за жилищно обитаване, зоната за комплексното обществено обслужване, училища, детски градини, зони за отдих, зоните за комплексно жилищно застрояване и др. (фиг. 3).




**Фиг. 3 Анализ на застрояването на кв. „Св. Никола“**

За да се даде информация за големината, формата и местоположението на имотите в квартала, имотите се квалифицираха в пет групи:

- имоти с площ под минимално допустимата;
- имоти с целесъобразна площ, неподлежащи на допълнително разделяне;
- имоти с площ, позволяваща разделяне;
- имоти с малко лице;
- имоти с неблагоприятна форма на разделяне, като в резултат се изработи аналитична схема на имотната структура (фиг. 4). Тези данни са база за определяне на границите на урегулираните поземлени имоти;




**Фиг. 4 Анализ на имотната структура на кв. „Св. Никола“**

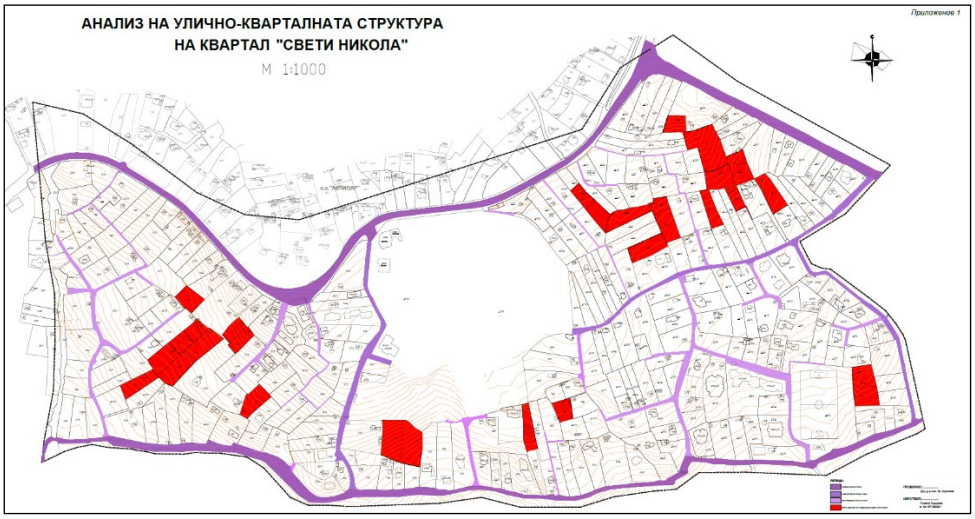
- **Благоустрояване**

Вътрешната улична мрежа не е развита добре. Улиците са малки, с непостоянни ширини от 3-4 м., частично благоустроени с асфалт, бетон или макадамова настилка. Благоустрояването е извършено със средства на собствениците. Много голяма част от имотите се обслужват от пътеки с ширина от 1-1,5 м, като 28 имота нямат достъп и преминаването до тях се извършва през чужди имоти.

Обслужването от градския транспорт се осъществява единствено по главния път с направление Варна-кв. „Виница“, с две автобусни спирки.

Водоснабдяването, електроснабдяването и канализацията са частични и изградени с частни средства.

С оглед на извършения анализ на уличната мрежа [7] се изработи аналитична структурна схема (фиг. 5), върху която са отбелязани главните и второстепенни съществуващи на място улици. Обследвани са кои имоти нямат достъп до улица, като тази информация използваме при проектирането на новите улици, за да им се осигури достъп, съгласно чл. 14, ал. 4 от ЗУТ [2].




**Фиг. 5 Анализ на улично-кварталната структура на кв. „Св. Никола“**

- **Обществено обслужване**

На територията на квартала има изградени: здравен пункт, читалище, магазин и сграда за административно-техническо обслужване към кметството на район „Приморски“ към Община Варна. Липсват заведения за обществено хранене, детска градина, училище и зони за спорт и отдих и почивка. Все повече млади семейства избират квартала за постоянно обитаване, поради което има остра необходимост от детски ясли и детса градина, както и училище за по-големите деца.

### 2.2. Проектно решение

Теренът притежава специфични качества. Сградата и другите обекти се разполагат с отчитане релефа на местността, който влияе върху композицията на обемите и пространствата.

След посещение на квартала с цел натрупване на лични впечатления и наблюдения и след проучване на отделни компоненти на специализираната карта на изследваната територия, ще се спрем, преди всичко, на анализа на:

Предмет на нашето по-нататъшно разглеждане е разработката на концептуалните структурни схеми за бъдещето функционално и пространствено зониране и развитие на част от кв. „Св. Никола“. След систематизиране на всички данни от изготвените аналитични структурни схеми, се пристъпи към изработването на две концептуални схеми създаващи условия за избор на най-целесъобразните възможности за развитие на изследваната територия [4].

Таблица 1 представя възможностите за разполагане на функционалните зони в концептуална схема Вариант 1.

***Таблица 1. Анализ на концептуална схема Вариант 1***

| Първи вариант | Зона обществено обслужване | Комплексно жил. строителство | Зона за спорт | Зона за отдих | Промишлена зона |
|---|---|---|---|---|---|
| Местоположение | В ПИ 1250, общ. собственост | Върху имоти, частна собственост | Върху имоти, частна собственост | В ПИ 1250, общ. собственост | В ПИ 1196, общ. Собственост |
| Възможност за нарастване | В рамките на ПИ 1250 | ограничена от финансова рамка | В рамките на отчуждените ПИ | В рамките на ПИ 1250 | Ограничена |
| Отдалеченост от централната зона | Част от зоната | В близост | В близост | Част от зоната | Отдалечена |
| Финасово-иконом. Показатели | без отчуждителни процедури | финансови с-ва за отчуждаване | финансови с-ва за отчуждаване | без отчуждителни процедури | без отчуждителни процедури |

Таблица 2 представя възможностите за разполагане на функционалните зони в концептуална схема Вариант 2.

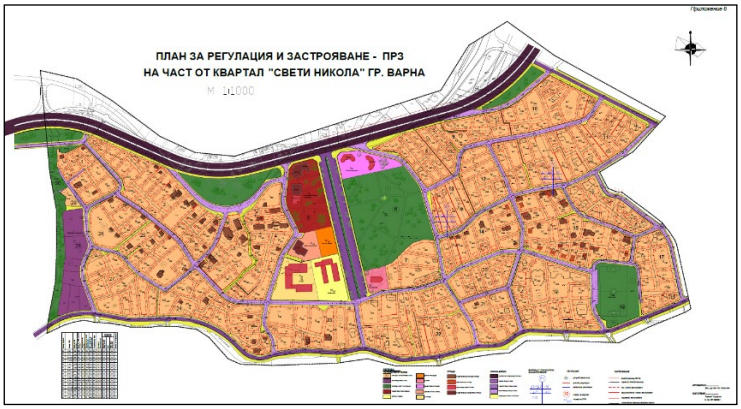
***Таблица 2. Анализ на концептуална схема Вариант 2***

| Втори вариант | Зона обществено обслужване | Комплексно жил. строителство | Зона за спорт | Зона за отдих | Промишлена зона |
|---|---|---|---|---|---|
| Местоположение | В ПИ 1250, общ. собственост | Няма | В ПИ 1250, общ. собственост | В ПИ 1250, общ. собственост | Върху имоти, частна собственост |
| Възможност за нарастване | В рамките на ПИ 1250 | Няма | В рамките на ПИ 1196 | В рамките на ПИ 1250 | Ограничена върху 3 бр. ПИ |
| Отдалеченост от централната зона | Част от зоната | Няма | В близост | Част от зоната | Отдалечена |
| Финасово-иконом. Показатели | без отчуждителни процедури | Няма | Съществуващ спортен терен | без отчуждителни процедури | Производства с частна инициатива |

От направения анализ е видно, че за реализирането на първия вариант ще са необходими големи финансови средства за отчуждаването на имотите, попадащи в зоната за комплексно жилищно строителство и спортния терен.

### 2.3. Инвестиционно проектиране

Въз основа на избрания вариант на концептуалната схема се разработи общата планова структура на кв. „Св. Никола“, гр. Варна [3, 5, 6]. Този етап конкретизира, допълни и прецизира предпочетената концептуална схема и включи следните основни етапи: Улична мрежа и улична регулация; Дворищна регулация; Застрояване на жилищните и обществените парцели; Зони за отдих и спорт;




**Фиг. 6 ПУП-ПРЗ на част от кв. „Св. Никола“**

# 3 Заключение

За изработването на план за регулация и застрояване, с обособени функционални зони, правилно проектирана улична мрежа и инфраструктура, функционална жилищна среда и осигуряване на условия за обитаване, отдих и обслужване е необходим голям екип от специалисти – урбанисти, архитекти, геодезисти, пътни инженери, социолози, климатолози, геолози и още мн. други, като положителния резултат е сбор от усилията, интелекта и продължителната работа на всеки член от екипа.

Експерименталната част на доклада представлява една обоснована стратегия за развитието на вилна зона на част от кв. „Св. Никола“, обл. Варна за задоволяване на рекреационни, промишлени и други специфични нужди. Така планирана и проектирана, територията на част от кв. „Св. Никола“, обл. Варна дава пълна свобода на живеещите в нея.

**ЛИТЕРАТУРА:**

[1] Диманова Д, "Алгоритъм на програма за моделиране честотата на природни бедствия". НК МАТТЕХ 2014, ШУ "Епископ Константин Преславски" 20-22 ноември 2014, Шумен, ISSN: 1314-3921. pp. 172-176.

[2] ЗУТ, обнародван ДВ,бр.1/2001г. с последващите изменения

[3] Ковачев, А. Градоустройство. Част I - Селищни елементи. София, Авангард Прима. 2019, ISBN 978-619-239-248-2

[4] Ковачев, А. Градоустройство. Част II - Функционални зони. София, Авангард Прима. 2019, ISBN 978-619-239-249-9

[5] НАРЕДБА № 7 за правила и нормативи за устройство на отделните видове територии и устройствени зони. ДВ, бр. 3 от 2004 г.

[6] Наредба № 8 за обема и съдържанието на устройствените планове ДВ, бр. 22 от 2014 г.

[7] Наредба № РД-02-20-2 за планиране и проектиране на комуникационно-транспортни системи на урбанизираните територии. Обн. ДВ бр.86 от 2004, посл. изм. ДВ бр.98 от 2018.

[8] Търсанков, Й., В. Иванов. Проект за малко селище – ръководство за проектиране. София, УАСГ, 2000.

[9] Янчев, К. Приложения на географските информационни системи в прогнозиране на условията на аерокосмическите изследвания. Шумен: Университетско издателство \"Епископ Константин Преславски\", Годишник на ШУ \"Еп. К. Преславски\" Технически науки. Том XI E, 2021, стр. 35-40, ISSN: 1311-834X.

# THE TRIGONOMETRICAL LEVELING IN THE DESIGN AND CONSTRUCTION OF LINEAR OBJECTS*

**IVAN D. IVANOV**

***ABSTRACT:*** *The design and construction activities of linear objects are related to achieving high accuracy in terms of determining the elevation position of characteristic points. By default, geodetic activities for this type of objects are associated with carrying out geometric leveling in order to achieve the necessary vertical accuracy. This paper examines the problems, feasibility and achievable accuracy of using the trigonometric leveling method to precisely determine the elevations of feature points in the design and construction of linear objects.*

***KEYWORDS:*** *trigonometric leveling, linear objects*

***DOI: https://doi.org/10.46687/RSAD3642***

# ТРИГОНОМЕТРИЧНАТА НИВЕЛАЦИЯ В ПРОЕКТИРАНЕТО И СТРОИТЕЛСТВОТО НА ЛИНЕЙНИ ОБЕКТИ

**ИВАН Д. ИВАНОВ**

***АБСТРАКТ:*** *Дейностите по проектиране и строителство на линейни обекти са свързани с постигане на висока точност по отношение на определяне височинното положение на характерни точки. По подразбиране, геодезическите дейности при този тип обекти, се свързва с провеждане на геометрична нивелация с цел постигане на необходимата вертикална точност. Настоящият доклад разглежда проблемите, възможността и достижимата точност при използване на методът на тригонометрична нивелация за прецизно определяне на височините на характерни точки при проектирането и строителството на линейни обекти.*

## 1 Въведение

Когато говорим за геодезически дейности е редно първо да разгледаме нормативната уредба, касаеща изследваната област, понеже за много от геодезическите дейности съществуват различни норми, образци, указания и др. За настоящата дейност, касаеща измерването линейните обекти (визираме главно пътища и ЖП линии), няма конкретни указания и норми, издадени от Агенция по геодезия, картография и кадастър. За дейностите по проектиране пътищата има издадена Наредба № РД-02-20-2 от 28 август 2018 г. [4], която третира геодезическите дейности при проектиране на пътища. В чл. 279, ал. 3, т. 5 се конкретизира единствения метод за определяне на височините на подробните точки, а именно - геометрична нивелация.

Отношение към изпълнението на строителството на линейните обекти има Техническа спецификация на АПИ от 2014 г. [5]. В нея никъде не се упоменава необходима точност и метод за измерване, но в своя раздел „1400. ОПИСАНИЕ, РАЗВИТИЕ И КОНТРОЛ НА СТРОИТЕЛНИТЕ РАБОТИ“ все пак задължава изпълнителя да провери опорния полигон и съществуващия терен.

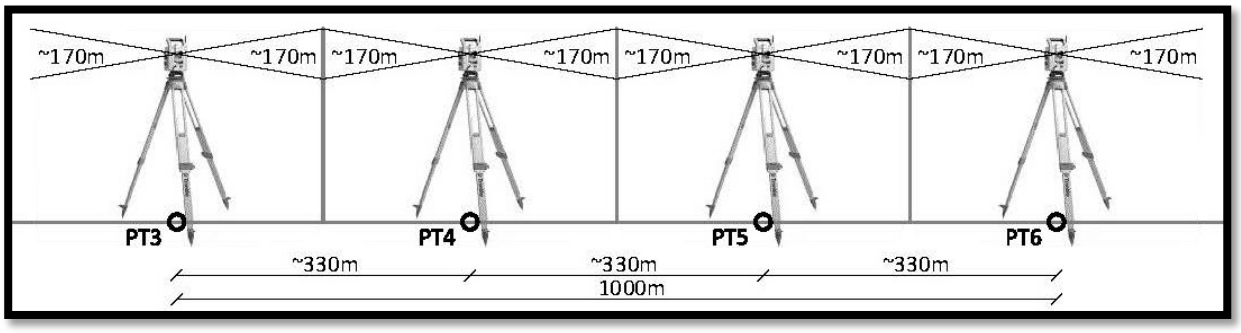
Макар нормативната уредба да не урежда методи, принципи и изисквана точност за геодезическите дейности при проектиране и изпълнение на линейните строителни обекти,

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

документи относими към тръжната документация на почти всички обществени поръчки дават индивидуални дефиниции и изисквания за тези дейности. Например в една техническа спецификация за открита обществена поръчка с цел изготвяне на технически проект за рехабилитация на III клас общински път се поставя изискване за максимална несвръзка между даденото и измереното превишение, изчислена по формулата: Fn =± 15√s [mm], където "s" е дължината на нивелачния ход в километри, а в друга за същия клас път - Fn =± 10√s [mm]. От друга страна се наблюдават и разлики в изискванията за методът на измерване като в единия случай има задължително използване на методът на геометричната нивелация, а в другия няма специфични изисквания към използвания метод. Общото е, че и в двата случая освен че няма нормативна регулация, няма и мотивирана обосновка зад тези поставени „изисквания".

## 2 Теоретична постановка

Погледнато теоретично, съгласно изискванията на нормативните актове и техническите спецификации, работна геодезическа основа за линейните обекти се изгражда с гъстота минимум 3 работни точки на 1km и съответно 2 нивелачни репера на 1km. Определянето на надморските височини на РГО на такива разстояния чрез тригонометрична нивелация с цел постигане на милиметрова точност е почти невъзможно, затова приемаме, че надморските височини на РГО са определени посредством геометрична нивелация. Предвид това може да приемем, че максималната дължина на визурите на площната тригонометрична нивелация в настоящото изследване, ще бъдат ≤170m (Фиг.1).



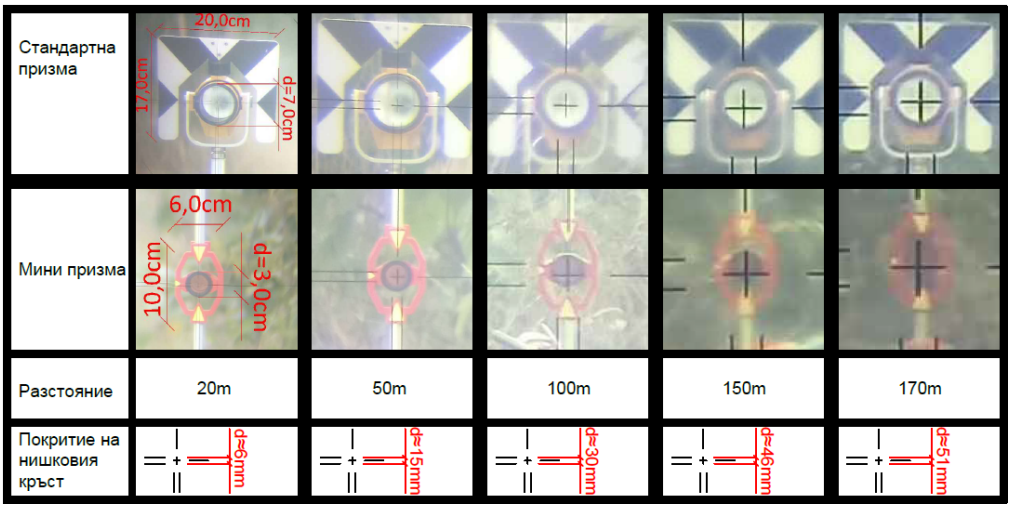

**Фиг. 1.** Максимално разстояние на визурите на площната тригонометрична нивелация

Следващия фактор са параметрите на измервателната техника, или иначе казано – ъгловата точност и точността на далекомера. В наши дни, всяка средностатистическа тотална станция (със съвсем малки изключения) притежава ъглова точност минимум 5" и точност на далекомера ≤3mm + 3ppm за измерване към отражател (призма). Тук по-голяма тежест се придава на ъгловата точност на инструмента като за горецитираната точност може да приемем индексна грешка в рамките на 20-30$^{cc}$. Вариация от 20-30$^{cc}$ за разстояние от 170m се равнява на грешка от порядъка на 5-8mm, пропорционално на измереното разстояние, което не е за подценяване и определя значението на инструменталната точност на измервателната техника.

Грешката в отчета по вертикалния кръг зависи и от още нещо, а именно – големината на наклона. Отклонения в отчета от 20-30$^{cc}$, в зависимост от наклона, предизвикват различна по големина грешка в изчисленото превишение. Например при отчет по вертикалния кръг 130$^{g}$ (респ. 70$^{g}$) и хоризонтално разстояние от 170m, колебание от 30$^{cc}$ повлиява изчисленото превишение със стойности ±10.1mm, докато при хоризонтален отчет

(близък до $100^g$), $30^{cc}$ предизвиква колебания от ±8.0mm. Съгласно [4], максималния надлъжен наклон, който можем да очакваме при провеждане на нивелация на пътища, е 9%. Отчитайки и разликата между височината на инструмента и сигнала, която в повечето случаи не превишава 50cm, измерените зенитни ъгли следва да са в границите между 94-$106^g$. За разстояние от 170 метра и приета грешка от $30^{cc}$, разликата между изчисленото превишение спрямо зенитен ъгъл $\pm 6^g$ и хоризонта ще бъде съответно 8.0mm и 8.1mm, с което може да заключим, че влиянието на наклона върху настоящите измервания е пренебрежимо малко.

При провеждане на тригонометрична нивелация, влияние указва и още един фактор, който често е пренебрегван при предварителна оценка на търсената точност, а именно покритието на нишковия кръст върху сигнала в съответствие с отдалечаването. Известно е, че с цел постигане на по-висока височинна точност, тригонометричната нивелация трябва да се извършва чрез отражател тип „мини призма“. Причините са две – този тип комплект призми имат фиксирани височини при сглобка на отделните елементи, а втората причина е в по-малкия диаметър на отражателя като така се постига по-прецизно насочване в центъра на сигнала, което е най-важната предпоставка за правилно определяне на превишението. За целта е проведено изследване при визиране на различни разстояния, резултатите от което са показани във Фиг.2. Използвана е тотална станция с увеличение X30, което е стандартно за повечето модели на пазара.




**Фиг. 2.** Илюстрация на визури на различни разстояние и съответното покритие на нишковия кръст

Резултатите показват, че при разстояние от 100m, нишковия кръст покрива диаметъра на стандартните мини призми (30mm), което е **критично при насочване в центъра на сигнала**. При разстояния по-големи от 100m, насочването към стандартна призма (70mm), снабдена с отражателна марка, изглежда по-надеждно, но постигането на милиметрова точност при тези условия се доближава повече до настъпване на случайна грешка, от колкото до професионализма и опита на оператора.

## 3 Източници на грешки и тяхното влияние

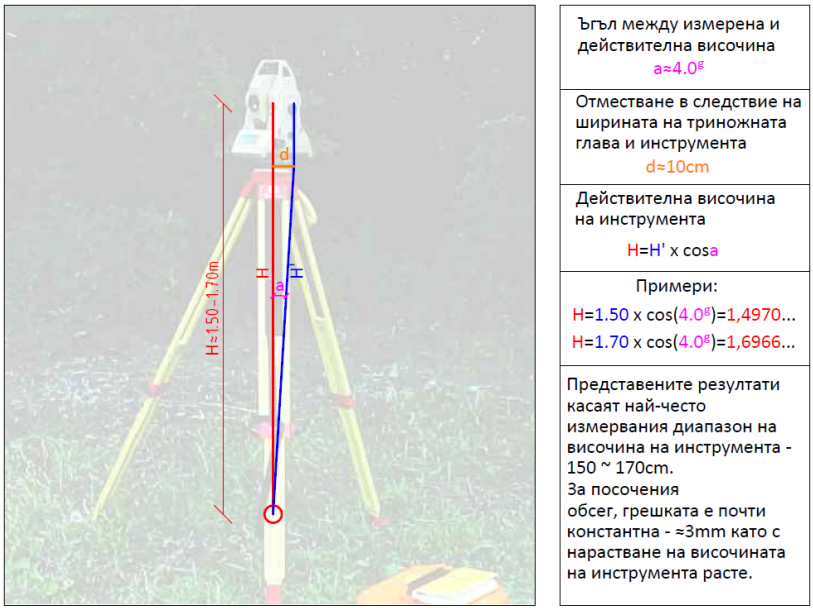
Тригонометричната нивелация е доказала своята ефективност и точност при сравнително не много сложна методика за измерване и изчисление. Наред с еволюцията технологиите и приборостроенето, съвременните тотални станции позволяват постигане

милиметрова височинна точност при проява на прецизност и спазване на определени правила. От това следва, че в основата за постигане на точността стоят уменията на наблюдателя (респективно и на фигуранта) и отчитането на влиянието на външната среда. Тези условности се подразделят в различни видове грешки, класифицирани като систематични, случайни и груби грешки.

**Грубите грешки** се характеризират със стойности, които се различават значително от очакваните. В почти всички случаи, те се появяват в резултат на действие на оператора, респективно фигуранта. Предвид напредването на технологиите и почти пълната автоматизация на записите и резултатите от измерванията, тези грешки са сведени на практика до минимум. Като най-характерен пример за груба грешка при площна тригонометрична нивелация, е грешно измерване и въвеждане на височина на инструмент и сигнал, ексцентрично измерване към сигнала (не в центъра) и грешно въвеждане на константата на отражателя. Тези грешки биха могли да се елиминират от оператори с достатъчно практически опит.

**Систематичните грешки** се допускат при всяко измерване като основните причини за тяхната поява са влиянието на външните фактори и неподходяща методика. Характерно за тези грешки е, че знакът и големината им са относително постоянни и се подчиняват на определен закон. Отстраняването на систематичните грешки се прави чрез използване на подходящ начин на измерване и/или въвеждане на поправки. Част от систематичните грешки обаче се подчиняват на твърде сложни закони и тяхното влияние не може да бъде елиминирано, особено в масовите измервания [3].

Като пример за систематична грешка в методиката при провеждане на тригонометрична нивелация можем да посочим измерването на височината на инструмента (Фиг.3).




**Фиг. 3.** Влияние на грешката в следствие ексцентрично измерване на височината на инструмента

Тази грешка е лесно отстранима при въвеждането на подходяща поправка за измерената височина, а може да бъде и напълно избегната при измерване от свободна станция (геодезическа засечка).

Влиянието на външните фактори поражда систематични грешки, които се подчиняват на по-сложни закони, съответно тяхното влияние се елиминира по-трудно. Като примери може да посочим влиянието на височината на квазигеоида над елипсоида, влиянието на височините на точките върху превишението, влияние на зенитния ъгъл върху рефракционната част на превишението, влияние на действителното гравитационно поле на Земята върху превишението и др. За всички тези фактори е установено, че за разстояния до 1-2km влиянието на тези фактори е разлика в превишението <1mm [2]. Основен източник на систематични грешки при тригонометричната нивелация, породени от външните условия, остават влиянието на кривината на Земята и вертикалната рефракция. Определянето на коефициентът на вертикална рефракция е сложен процес, което налага извършването на по-задълбочени изследвания, изразяващи се в извеждането му за отделни райони и периоди от денонощието. Въпреки това можем да направим препоръка, че оптималното време за измерване на вертикални ъгли е при най-малка динамика на температурата на въздуха и постилащата повърхност, при максимално възможно отдалечение на визирния лъч от терена [1].

За нашия експеримент ще приемем средния коефициент на вертикалната рефракция на светлината за нашата страна, а именно k=0.106. Съвместното влияние на кривината на Земята и вертикалната рефракция може да бъде определено по формулата:

(1) $$f = \frac{1-k}{2R} S^2$$

където R е средния радиус на Земята, а S е измереното разстояние.

От тази формула следва, че натрупване на грешка от 1mm се постига при визури >120 m и съответна грешката расте квадрата на разстоянието.

**Случайните грешки** се характеризират с различна големина и знак дори при относително постоянни условия. Има много причини за тези грешки, които действат често и за кратко време. Най-характерното свойство за тези грешки е, че с увеличаване на броя на измерванията, случайните грешки взаимно се компенсират, в резултат на което окончателната грешка е по-малка от грешката на отделното измерване. Разбира се за целите на настоящото изследване това правило не може да бъде приложено, така че те не могат да бъдат елиминирани. Единствения фактор за тяхното минимизиране е използването на изправна техника и натрупаният опит на оператора (респ. и на фигуранта).

# 4 Анализ и оценка на приложението на тригонометричната нивелация

Вземайки в предвид всички изброени грешки и фактори, влияещи върху точността на площнтата тригонометричната нивелация, може да обобщим, че милиметрова точност може да се гарантира при предварително изградено РГО, височинно определено посредством геометрична нивелация с необходимата точност, и измервания с дължина на визурите до 100m. Така ще се елиминира напълно влиянието на кривината на Земята и земната рефракция, а същевременно ще се намали и ефектът от покритието на нишковия кръст върху отражателя. Основно влияние върху грешката в измереното превишение ще се отдаде основно на ъгловата точност на инструмента като при горецитираната точност от 20-30$^{cc}$, ще се получат възможни вариации в границите на 3.1-4.7mm.

Останалите условия и фактори, както и до голяма степен допуснатите грешки в ъгловите отчети, зависят изцяло от опита и професионализма на оператора. При достатъчно добри професионални умения, операторът може да елиминира грешките от измерване на височината на инструмента, на сигнала, същевременно да минимизира грешките при

отчитане на вертикалния ъгъл и ексцентричното измерване към сигнала в следствие покритието на нишковия кръст, за които съществува опасност дори при така заложените условия, а именно – РГО с надморски височини, определени чрез геометрична нивелация и дължина на визурите до 100m.

За разлика от съвременната геометрична нивелация с дигитални нивелири и другите съвременни методи за определяне на надморски височини (респ. събиране на геопространствена информация), тригонометричната нивелация се влияе най-силно от субективния (човешкия) фактор. Делът на допусканите случайни грешки остава най-голям при провеждане на тригонометрична нивелация. Отделно е трудно да се постигне реална оценка на точността, защото при изравнение на площната тригонометричната нивелация дори да получим малки поправки при измерване към известните (изходните) работни точки, всяко отделно измерване самостоятелно се подчинява на гореупоменатите грешки и фактори.

# 5 Заключение

Настоящият доклад разглежда проблемите и възможностите за използване на метода на тригонометрична нивелация с цел постигане на милиметрова точност, необходима за дейностите по проектиране и строителство на линейни обекти. Данните и резултатите в нея имат чисто информативен и обзорен прочит на проблемите при горецитираните дейности.

Макар значителния дял на възможностите за допускане на грешки, методът на тригонометрична нивелация може да постига милиметрова точност при съблюдаване на предварително въведени акуратни условности. Това измества фокусът в изискването за определяне на надморските височини в посока търсена точност, а не в задължителен метод, защото съвременните технологии предлагат и други начини за постигане на милиметрова точност освен методът на геометричната нивелация.

Не на последно място трябва да се отчете и значителната част на планинската територия в България. Линейните обекти в тези територии обикновено са под формата на проходи, осеяни със множество хоризонтални криви и гориста растителност. Тази предпоставка доста често изключва възможността за използването на GNSS и други дистанционни методи като методът на тахиметрията може да осигури както хоризонталното, така и вертикалното заснемане на подробните точки с необходимата точност. Това от друга страна спестява допълнителното провеждане на височинно измерване (най-често геометрична нивелация) с цел определяне на надморските височини на подробните точки.

**ЛИТЕРАТУРА:**

[1] Александров, Б. Експериментално определяне на стойността на коефициента на вертикална рефракция за района на УОБ ”Веринско“, сп. ”Геомедия”, 2013, бр. 5, стр.36-41 ISSN-1313-3365.

[2] Вълчинов, В. Земна рефракция и геодезическите измервания. София. 2023. ISBN 978-619-92537-0-0.

[3] Маждраков, М., Иванова, Ил. Геодезия. 2014. Шумен, Издателство на ШУ „Епископ Константин Преславски“.

[4] Наредба № РД-02-20-2 от 28 август 2018г.за проектиране на пътища.

[5] Техническа спецификация – АПИ. 2014.

# CONTENTS OF THE CADASTRAL MAP*

**MIREM E. NIYAZI-YUSUF**

***ABSTRACT:*** *Pursuant to the Law on the Cadastre and Property Register, the cadastre is a set of basic data on the location, borders and sizes of real estate on the territory of the Republic of Bulgaria, which are collected, presented, kept up-to-date and stored in accordance with the procedure established by this law. In addition to the basic data, the cadastre also includes data on the right of ownership and data on other real rights on real estate, data on state borders, borders of administrative-territorial units, land borders and borders of territories with the same permanent purpose. The data are plotted on a cadastral map and recorded in cadastral registers.*

***KEYWORDS:*** *cadastre, cadastral data, map*

***DOI: https://doi.org/10.46687/FRPW9487***

# СЪДЪРЖАНИЕ НА КАДАСТРАЛНАТА КАРТА

**МИРЕМ Е. НИЯЗИ-ЮСУФ**

***АБСТРАКТ:*** *Съгласно Закона за кадастъра и имотния регистър, кадастърът е съвкупност от основни данни за местоположението, границите и размерите на недвижимите имоти на територията на Република България, които са набирани, представяни, поддържани в актуално състояние и съхранявани по установен от този закон ред. Освен основните данни, кадастърът обхваща и данни за правото на собственост и данни за другите вещни права върху недвижимите имоти, данни за държавните граници, границите на административно-териториалните единици, землищните граници и границите на територии с еднакво трайно предназначение. Данните се нанасят върху кадастрална карта и се записват в кадастрални регистри.*

Съгласно чл. 5 от Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри, кадастралната карта съдържа данни за:

1. държавните граници;
2. границите и наименованията на областите;
3. границите и наименованията на общините;
4. границите и наименованията на населените места и на районите на градове по чл. 10 от Закона за административно-териториалното устройство на Република България (ЗАТУРБ);
5. границите и номерата на кадастралните райони;
6. границите и номерата на поземлените имоти;
7. границите и/или очертанията и номерата на сградите и на съоръженията на техническата инфраструктура, в които има самостоятелни обекти;
8. очертанията на самостоятелни обекти в сгради и в съоръжения на техническата инфраструктура;
9. очертанията и номерата на зоните на ограничения;

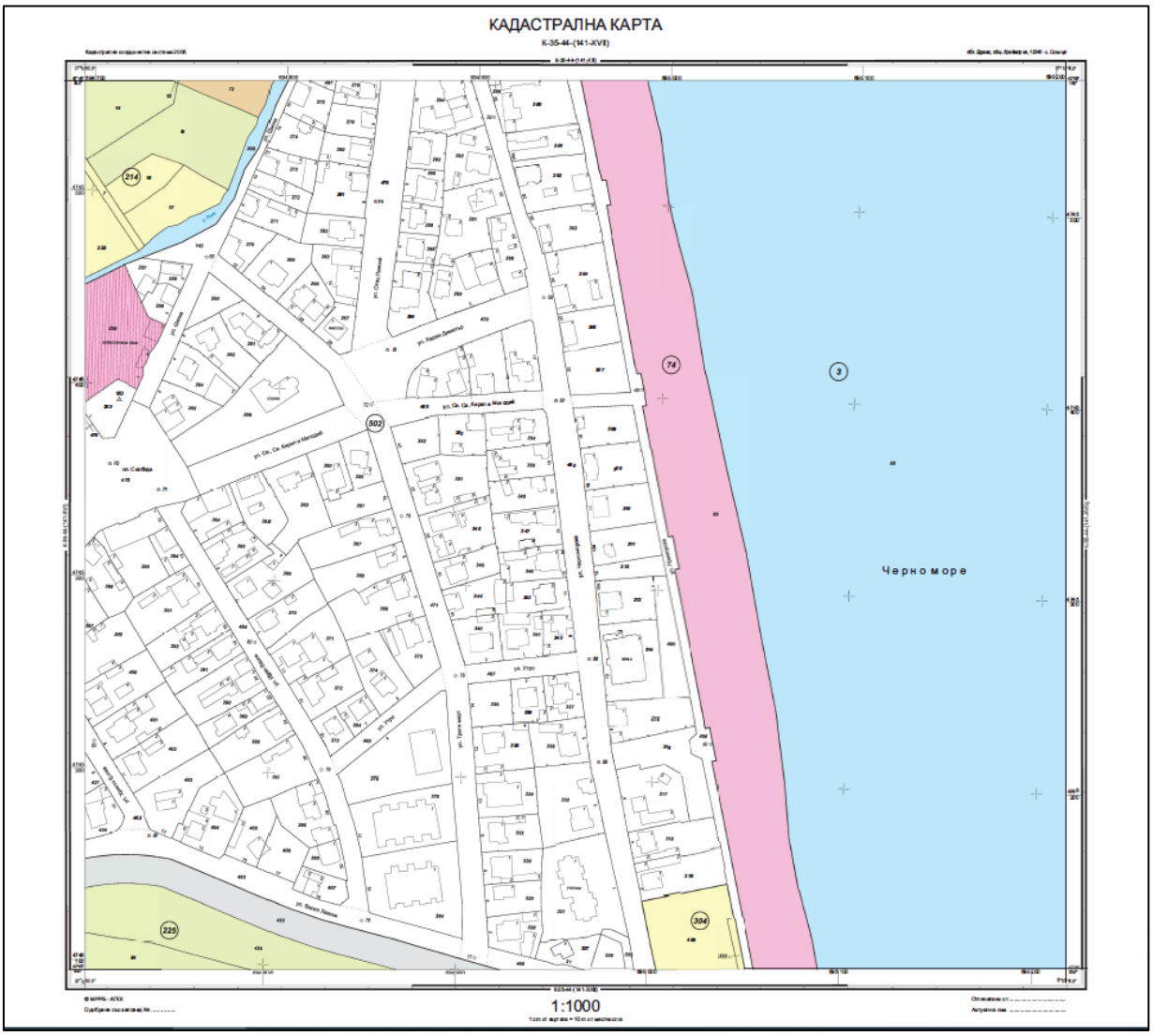
* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

10. територииите с еднакво трайно предназначение и територииите по чл. 13, ал. 4 от [3];

11. подробните точки, определящи границите и очертанията;

12. точките от геодезическата основа и техните номера;

13. наименованията на местности, улици, площади, булеварди, квартали, жилищни комплекси; природни и исторически забележителности; водни течения и водни площи; пристанища, пътища, железопътни линии и гари; музеи, училища и други обществени сгради, както и номерата от административните адреси на поземлените имоти.




**Фиг. 1.** Кадастрална карта в М 1:1000 [3]

Изобразяването на държавната сухоземна граница и държавната речна граница в кадастралната карта се осъществява в съответствие с установеното им местоположение с международни договори.

Държавната морска граница и границата на вътрешните водни пътища се нанасят в кадастралната карта по данни от Главна дирекция "Гранична полиция" съгласно Закона за

морските пространства, вътрешните водни пътища и пристанищата на Република България (ЗМПВВППРБ).

Границите и наименованията на областите, общините и населените места се изобразяват в кадастралната карта така, както са определени по реда на ЗАТУРБ.

Землищните граници се изобразяват в кадастралната карта така, както са отразени в плановете и картите, одобрени по реда на Закона за собствеността и ползването на земеделските земи (ЗСПЗЗ).

Съгласно чл. 11, ал. 3 от [3] При определянето на землищна граница се спазват следните изисквания:

1. землищната граница да минава при възможност по реки, дерета или по едната страна на пътища, железопътни линии, по структурни линии на терена, други трайно съществуващи обекти на терена, както и да има минимален брой чупки;
2. землищната граница да минава по граници на поземлени имоти.

Районите по чл. 10 ЗАТУРБ и територията на населените места и се разделят на кадастрални райони. Границите на кадастралния район съвпадат с границите на поземлените имоти. Кадастралният район се ограничава от граница на селищната територия на населеното място, землищна граница на извънселищната територия на населеното място, граници на райони на градове по чл. 10 ЗАТУРБ и граници на поземлени имоти - пътища, железопътни линии, улици, реки и други трайно съществуващи линейни обекти. Кадастралният район може да обхваща и територии с различно трайно предназначение. [3]

Когато кадастралната карта се създава с данни от карти на възстановената собственост границите на масивите се приемат за граници на кадастрални райони. Територията, попадаща в масив с номер 0 (нула), се присъединява към съседни кадастрални райони.

Териториите с еднакво трайно предназначение, границите на които се изобразяват в кадастралната карта, са:

1. урбанизирани територии (селищната територия на населеното място и селищни образувания и индустриални паркове извън границите на населените места и селищните образувания) - определени с устройствен план съгласно Закона за устройство на територията (ЗУТ), съответно със застроителен и регулационен план или околовръстен полигон съгласно отменения Закон за териториално и селищно устройство (ЗТСУ), или са такива по начин на трайно (фактическо) ползване, доколкото то не противоречи на закон - в територии без устройствени планове;

2. територии на транспорта - определени съгласно Закона за пътищата (ЗП), Закона за железопътния транспорт (ЗЖПТ), Закона за гражданското въздухоплаване (ЗГВ) и ЗМПВВППРБ;

3. земеделски територии - определени с планове и карти, одобрени по реда на ЗСПЗЗ;

4. горски територии - определени с планове и карти, одобрени по реда на Закона за възстановяване на собствеността върху горите и земите от горския фонд (ЗВСГЗГФ) и ЗСПЗЗ и Закона за горите (ЗГ);

5. територии, заети от води и водни обекти - определени съгласно Закона за водите (ЗВ) и ЗМПВВППРБ;

6. защитени територии - определени съгласно Закона за защитените територии (ЗЗТ) и Закона за културното наследство (ЗКН);

7. нарушени територии - определени съгласно ЗУТ. [3]

За установяване на границите на поземлените имоти в урбанизираните територии се анализират на данните от:

1. геодезически измервания на означените на място граници в съответствие с правото на собственост;

2. одобрена кадастрална карта;

3. 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. регулационни планове, одобрени по реда на ЗУТ или на отменените ЗТСУ и Закона за планово изграждане на населените места (ЗПИНМ) - за имотите с приложена регулация, границите на които не са материализирани;

5. геодезически измервания на съществуващите на място материализирани граници, когато не са означени по реда на чл. 14, ал. 1, т. 1 от [3];

6. карти, планове и друга документация, предоставени от ведомства и общини по реда на чл. 30 от [3];

7. документите по чл. 41, ал. 2 и 3 ЗКИР.

В зависимост от състоянието им върху терена, границите на поземлените имоти се определят като:

1. трайно материализирани - изобразяват се съгласно формата по чл. 12, т. 5 ЗКИР;

2. нетрайно материализирани - изобразяват се съгласно формата по чл. 12, т. 5 ЗКИР;

3. нематериализирани - изобразяват се съгласно формата по чл. 12, т. 5 ЗКИР.

За установяване на границите и/или очертанията на сгради и на съоръжения на техническата инфраструктура се анализират данните от:

1. геодезически измервания на съществуващите на място надземни сгради и съоръжения на техническата инфраструктура;

2. планове и карти, посочени в чл. 41, ал. 1, т. 1 и 3 ЗКИР.

За установяване на очертанията на подземни сгради и съоръжения на техническата инфраструктура се анализират данните от:

1. геодезически измервания на видимите надземни части и подземни части преди засипването им;

2. екзекутивни чертежи или проекти за изграждането на сградите и съоръженията;

3. планове и карти, посочени в чл. 41, ал. 1, т. 1 и 3 ЗКИР.

Самостоятелен обект в сграда или в съоръжение на техническата инфраструктура се изобразява чрез неговото очертание в хоризонталния разрез на сградата или на съоръжението на техническата инфраструктура на съответния етаж. Когато самостоятелният обект е разположен на няколко етажа, се изобразяват очертанията му на всеки етаж. Ниво в самостоятелен обект, което не съвпада с етаж от сградата, няма графично изображение. Броят на нивата на самостоятелния обект се надписват. [3,7]

Очертание на самостоятелен обект в сграда или в съоръжение на техническата инфраструктура се определя приоритетно от:

1. одобрен инвестиционен проект;

2. граници, описани в документ за собственост и измервания на място.

Номерацията на самостоятелните обекти - жилища в сградата, се извършва по входове и започва от най-ниския жилищен етаж, като по възможност се запазват административните им номера. Самостоятелните обекти, които не са жилища, получават номер след последния номер за жилище. Самостоятелните обекти в съоръженията на техническата инфраструктура се номерират с единна номерация за цялото съоръжение, като се започва от северозападния край на първия подземен етаж или на първия надземен етаж със самостоятелни обекти. [3]

**ЛИТЕРАТУРА:**

[1] Закон за кадастър и имотен регистър. ДВ бр. 34, 2000

[2] Закон за собствеността. ДВ бр. 92, 1951

[3] 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

[4] 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.

[5] Наредба № 19 от 28.12.2001 г. за контрол и приемане на кадастралната карта и кадастралните регистри. ДВ, бр. 2, 2002

[6] 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.

[7] Стойков Е., 2021 г. „Морска информационна система“, Годишник: Технически науки. Том XI E, Шумен, Университетско издателство „Епископ Константин Преславски“, ISSN: 1311-834X, стр.25 - 29.

[8] http://www.cadastre.bg/ - Агенция по геодезия, картография и кадастър

# STANDARDS FOR EXECUTION, CONTROL AND ACCEPTANCE OF CONSTRUCTION AND INSTALLATION WORKS IN BRIDGE CONSTRUCTION IN BULGARIA*

**ANI A. STEFANOVA**

***ABSTRACT:*** *The article examines the regulatory framework in Bulgaria for control and acceptance of construction and assembly works. An analysis and systematization of the construction and assembly tolerances concerning the erection of prefabricated and monolithic bridge construction has been made. The required accuracies of the setting out in position and height have been derived.*

***KEYWORDS:*** *regulatory framework, construction and assembly tolerances, accuracy, setting out of bridges*

***DOI: https://doi.org/10.46687/FTED9155***

# НОРМИ ЗА ИЗПЪЛНЕНИЕ, КОНТРОЛ И ПРИЕМАНЕ НА СТРОИТЕЛНО-МОНТАЖНИ РАБОТИ В МОСТОВОТО СТРОИТЕЛСТВО В БЪЛГАРИЯ

**АНИ А. СТЕФАНОВА**

***АБСТРАКТ:*** *В доклада е разгледана действащата у нас нормативна уредба за контрол и приемане на строително-монтажните работи. Извършен е анализ и систематизиране на строително-монтажните допуски, свързани със строителството на сглобяеми и монолитни мостови конструкции. Изведени са необходимите точности на геодезическите трасировъчни работи по положение и височина.*

## 1 Въведение

При прегледа на съществуващата българска нормативна уредба е установено, че строително-монтажните допуски (СМД) са публикувани в различни наредби, правилници и бюлетини, издавани през различни периоди от време. **Те** са разделени не по видове строителни обекти, а по типове строителство, което има положителни качества, поради обстоятелството, че допуските са събрани в сравнително малко на брой нормативни документи. Основното неудобство обаче, се крие във факта, че при изпълнение на строително-монтажни работи (СМР) на определен вид строителен обект е необходимо изрично да се посочат кои СМД ще се използват при контрол и приемане на СМР, тъй като някои от тях са сравнително еднакви.

Въз основа на казаното по-горе авторът стига до заключение, че съществува необходимост от анализ, оценка и систематизиране на строително-монтажните допуски по основни видове СМР извършвани при различните видове строителство.

Техническата спецификация (ТС) на Агенция „Пътна инфраструктура“ е пример за такъв подход [7]. **Тя** представлява комплект от инструкции за строителство на пътища и пътни съоръжения и съдържа съответните утвърдени технически изисквания и условия за материалите и строително-монтажните работи **при** пътни обекти, в това число и мостове.

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

Съществен недостатък на тази спецификация е обстоятелството, че публикуваните допуски са директно заимствани от оригиналните нормативни документи и не са адаптирани към различните етапи от строителството: фундаменти, устои и стълбове, носещи конструкции, в зависимост от техния тип.

Общ недостатък на Техническата спецификация и нормативната уредба за контрол и приемане на СМР, е липсата на изисквания за точност към геодезическите измервания. В някои литературни източници [6] са цитирани такива допуски за точност, но най-често те са взети от остарели вече руски източници, поради което се нуждаят от преоценка и актуализиране. Поради тази причина авторът смята, че е необходимо да се разработят изисквания за точност на геодезическите работи извършвани при различните видове строителство, които да съответстват на строителните допуски, регламентирани в съвременните български нормативни документи за изпълнение, контрол и приемане на СМР. Добър пример за това са руските „Строителни норми и правила“ (СНиП), в някои от които са дадени и изискванията за точност на геодезическите измервания.

В България се използват следните нормативни документи при изпълнение, контрол и приемане на СМР при строителството на различни видове сгради и съоръжения:

- **ПИПСМР – Раздел „Специални промишлени фундаменти - фундаменти под машини“, БСА, бр. 7-8 от 1977г.**
- **Правилник за приемане на земната основа и фундаментите (БСА, кн. 6 от 1985г.).**
- **Правилник за приемане на стоманобетонни конструкции (БСА 10/68; доп. БСА, 8/78; изм. БСА 1/82).**
- **Външни мрежи и съоръжения за водоснабдяване, канализация и топлоснабдяване, ПИПСМР (БСА, кн. 4 от 1984г., попр., БСА, кн. 3-4 от 1985г.).**
- **ПИПСМР – Раздел „Топлопроводи и газопроводи“ (БСА, кн. 8 от 1969г., попр., БСА, кн. 12 от 1982г., изм., БСА, кн. 4 от 1984г. със заповед № РД-14-02-1286 от 07.03.1984г.).**
- **ПИПСМР – Раздел „Съоръжения за телефони, телеграфни и радио (ТТР) съобщения (БСА, кн. 10 от 1968г., изм., БСА, кн. 9 от 1979г.)**
- **ПИПСМР – Раздел „Железопътни линии“ (БСА, кн. 7-8 от 1968г.).**
- **ПИПСМР – Раздел „Електрификация на железопътни линии“ (БСА, кн. 9 от 1968г.).**
- **ПИПСМР – Раздел „Пътища и улици“ (БСА, кн. 3 от 1978г.)**
- **ПИПСМР – Раздел „Мостове и водостоци“ (БСА, кн. 3-4 от 1969г.).**
- **ПИПСМР – Раздел „Пристанищно строителство“ (БСА, кн. 2 от 1970г).**
- **ПИПСМР – Раздел „Хидротехнически съоръжения“ (БСА, кн. 3-4 от 1969г.).**
- **Правила за приемане на хидромелиоративни системи и съоръжения (БСА, кн. 12 от 1987г.).**
- **ПИПСМР – Раздел „Охладителни кули, комини, силози и бункери“ (БСА, кн. 9 от 1968г.).**
- **Наредба № 3 за контрол и приемане на бетонни и стоманобетонни конструкции [1] (ДВ, бр. 97/1994г., БСА, 2/1995г., изм. ДВ, бр. 53/1999г.)**
- **Правила за приемане на паркове и градини (БСА, кн. 8 от 1987г.).**
- **Правилник за приемане на електромонтажни работи (БСА, кн. 12 от 1984г.)**

**Изброените нормативни документи освен поотделно са публикувани и заедно в два сборника:**

- **Правила за извършване и приемане на строителни и монтажни работи (ПИПСМР)– Сгради, СЕК, 2008;**
- **Правила за извършване и приемане на строителни и монтажни работи (ПИПСМР) – Съоръжения, СЕК, 2007 [3].**

Както бе споменато по-горе СМД допуски дадени в тях, не са систематизирани по основни видове СМР. Някои от тях са или сходни или много общо формулирани, което води до неоднозначност и неясноти при тяхното използване.

## 2 Допустими отклонения при строителството на мостове

Във връзка с казаното по-горе, авторът на доклада е извършил анализ, оценка и систематизиране на строително-монтажните допуски от изброените източници, в резултат на което е синтезирал извадка (таблици: 1, 2, 3, 4 и 5), ориентирана към извършване на основните видове СМР при строителството на мостове, в зависимост от начина на фундиране, материала, вида и начина на изграждане на носещата конструкция – стоманобетонна, изпълнена монолитно или чрез монтаж на готови елементи или монтаж на метални ферми. При съставянето й авторът се е консултирал с колеги от УАСГ и специалисти от практиката.

Систематизираната извадката на строително-монтажните допуски, отнасящи се до строителството на монолитни и сглобяеми конструкции на мостове включва:

**Таблица 1**

**Допустими отклонения при изграждане на фундаменти на устои и междинни опори (изпълнение на пилотни фундаменти, шпунтови огради, анкери, кладенци и кесони) [2], [4], [7]**

| № по ред | Наименование на отклонението | Допустимо отклонение |
|---|---|---|
| 1 | **Допустими отклонения от проектното положение на забивните и набивни пилоти в план в зависимост от вида и разположението на пилотите:** | |
| | 1.1. Забивни пилоти с квадратно и правоъгълно сечение, кухи и кръгли забивни пилоти с диаметър по-малък от 0.50 m | |
| | а) при еднородно разположение на пилотите | |
| | - напречно на оста на пилотния ред | 0,20 d * |
| | - надлъжно на оста на пилотния ред | 0,30 d |
| | б) за група пилоти и ивици с разполагане на пилотите в два или три реда: | |
| | - за крайни пилоти | 0,20 d |
| | - за пилотния ред напречно на оста | 0,30 d |
| | в) за единични пилоти | 5 cm |
| | г) за пилоти - стълбове | 3 cm |
| | 1.2. Кухи кръгли пилоти с диаметър от 0.50 до 0.80 m и забивни пилоти с диаметър по-голям от 0.50 m | |

| | | |
|---|---|---|
| | а) при езично разположение на пилотите – напреч-но на реда | 10 cm |
| | б) при ивично разположение на пилотите - надлъжно на реда и при групово разположение на пилотите | 15 cm |
| | в) за единични кухи кръгли пилоти за колони | 8 cm |
| | 1.3. Пилоти и кухи пилоти, забити чрез кондуктори | Отклонението на осите на монтирания и закре-пен кондуктор от про-ектното положение на ниво горен ръб кондук-тор трябва да бъде в акватория до 0.025H, където H е дълбочината на водата на мястото на монтира-ния кондуктор и ± 25 mm при сухи корита. |
| 2 | **Допустимо отклонение от котата на главата на пилота в зависимост от типа на пилотния фунда-мент:** | |
| | 2.1. Фундаменти с монолитен ростверк | ± 3 cm |
| | 2.2. Фундаменти със сглобяем ростверк - плоча | ± 1 cm |
| | 2.3. Фундаменти без ростверк с монтажна шапка | ± 5 cm |
| | 2.4. Пилот - стълбове | от 0 до 3 cm |
| 3 | **Отклонение на шпунтовия ред от проектното положение в план в зависимост от вида на шпунта** | |
| | 3.1. Дървен шпунт на кота глава шпунт | Дебелината на шпунта |
| | 3.2. Дървен шпунтов ред без прегради (подкоси) | 300 mm |
| | 3.3. Стоманобетонен шпунт на кота терен | 100 mm |
| | 3.4. Стоманобетонен шпунт при забиване на плава-що устройство: | |
| | а) на кота горен ръб на шпунта | до 300 mm |
| | б) на кота терен | 150 mm |
| | 3.5. Стоманобетонен шпунт при забиване от кота горен ръб на шпунта | 150 mm |
| 4 | **Отклонение в размерите на положението на кладенците и кесоните:** | |
| | 4.1. В размерите на напречното сечение: | |
| | - по дължина и ширина | 0.5% но не повече от 12 cm |
| | - по радиуси | 0.5% но не повече от 6 cm |
| | - по диагонали | 1% |
| | 4.2. По дебелина на стените: | |
| | - бетонни и бутобетонни | ± 30 mm |

| | | |
|---|---|---|
| | - стоманобетонни | ± 30 mm |
| | 4.3. Хоризонтални отмествания | 0.01 от дълбочината на спускане |
| | 4.4. Тангенс на ъгъла на отклоняване на вертикалата | 0.01 |
| 5 | **Допустими отклонения във фундаментите:** | |
| | 5.1. Изместване на осите на фундаментите спрямо геодезическите оси на разбивката | ± 10 mm |
| | 5.2. Изместване на котата на горната повърхност | -10 mm |
| | 5.3. Отклонение на наклона на горната повърхност | 1/1000 |
| | 5.4. Отклонение на плоскостите и линиите на тяхното пресичане спрямо вертикалата или от проектния наклон по цялата височина на конструкцията на фундамента | ± 20 mm |
| | 5.5. Отместване на геометричните оси на конструкцията на фундамента | ± 15 mm |

***d – диаметър на кръгъл, страна на квадратен или по-малката страна на правоъгълен пилот.**

Допълнение към т.1 от горната таблица:

- Броят на пилотите или кухите пилоти с максимално допустими отклонения не трябва да надвишава: при ивично разположение 25% от общия брой пилоти, а при изпълнение на пилоти-стълбове - 5%.
- Не се допуска наклонът на забивните пилоти (освен стоящите) да надвишава проектния с повече от 2%, а при набивните – 1%.

**Таблица 2**

**Допустими отклонения при изграждане на устои, опори (стълбове) и носещи елементи, изпълнени като монолитни или сглобяеми бетонни и стоманобетонни конструкции [2], [7]**

| **№ по ред** | **Наименование на отклонението** | **Допустимо отклонение в mm** |
|---|---|---|
| 1 | **При бетонни и стоманобетонни опори:** | |
| | 1.1. Отклонения от вертикалата или от проектния наклон на кофражите и на пресечните им линии: | |
| | - на 1 m височина | 5 |
| | - на цялата височина на конструкциите за: | |
| | а) стени и колони с височина до 5 m вкл. | 10 |
| | б) стени и колони с височина над 5 m | 15 |
| | в) колони, свързани с греди | 10 |
| | 1.2. Отклонения във вътрешните размери на кофрираните напречни сечения на колони, стени | 5 |
| | 1.3. Разместване на осите на колоните в долното сечение по отношение на осите на разбивката | 5 |
| | 1.4. Разместване на осите на колоните в горното сечение по отношение на осите на разбивката при височина на колоната: | |
| | а) до 8 m | 20 |
| | б) от 8 до 16 m | 25 |
| | в) от 16 до 25 m | 32 |

| | | |
|---|---|---|
| | г) от 25 до 40 m<br><br>д) над 40 m<br><br>1.5. Отклонение на плоскостите и линиите на тяхното пресичане спрямо вертикалата или от проектния наклон по цялата височина на конструкцията:<br>- за стени и колони, поддържащи сглобяеми гредови конструкции | 40<br>задължително се определя от проектанта<br><br><br><br>±10 |
| 2 | **При стоманени опори:**<br>2.1. Повърхност на фундамента и ниво на предварително поставени опорни метални части:<br>- по ниво<br>- по наклон<br>2.2. Горна повърхност на опорната плоча<br>- по ниво<br>- по наклон | <br><br><br>± 5<br>1/1000<br><br>± 1.5<br>1/1500 |

**Таблица 3**

**Сглобяеми бетонни и стоманобетонни конструкции (гредови, конзолен монтаж) [2]**

| **№ по ред** | **Наименование на отклонението** | **Допустимо отклонение в mm** |
|---|---|---|
| 1 | **Греди, ферми и панели**<br>1.1. Изместване на осите на елементите спрямо трасировъчните оси на опорните конструкции | <br>± 5 |
| | 1.2. Отклонение на котите при опорните плоскости | ± 20 |
| | 1.3. Отклонение на оста на горния пояс (фланш) от правата линия | ± 25 |
| | 1.4. Разлика във височината на два съседни подови панела при панели с дължина:<br>а) до 4 м<br>б) над 4 м | <br>5<br>10 |
| | 1.5. Разместване в план на подови и покривни панели спрямо проектното положение на опорните повърхности | 13 |
| | 1.6. Разлика във височината на два покривни панела, мерена по горния им надлъжен ръб, при панели с дължина:<br>а) до 6 м<br>б) над 6 м | <br>15<br>25 |
| | 1.7. Разлика във височинните коти на опорните повърхности | ± 10 |
| | 1.8. Разлика във височината на два съседни подови или покривни панела, мерена под или над панелите | 4 |

***Забележка:*** Допустимите отклонения от точки 1.4, 1.5, 1.6, 1.7 и 1.8 (табл. 3) се прилагат за гредови мостове, при които носещата конструкция върху тях, се изгражда чрез сглобяеми стоманобетонни панели.

**Таблица 4**

**Монолитни бетонни и стоманобетонни носещи конструкции, включително конзолно бетониране**

| **№ по ред** | **Наименование на отклонението** | **Допустимо отклонение в mm** |
|---|---|---|
| 1 | Местни отклонения от проектната повърхност на елемента при проверка на конструкция с рейка с дължина 2 м, освен опорните повърхности | ±5 |
| 2 | Отклонение в дължината при светлия отвор на елемента | ±20 |
| 3 | Отклонение в размерите на напречното сечение на елемента | от +6 до -3 |
| 4 | Отклонение в котите на повърхностите и на закладните детайли, служещи за опори на метални или сглобяеми стоманобетонни колони и други сглобяеми елементи | -5 |
| 5 | Отместване на геометричните оси на конструкцията - за греди и дъги | ±10 |

***Забележка*:** Всички точки от горната таблица се отнасят както за монолитните, така и за сглобяемите бетонни и стоманобетонни конструкции.

**Таблица 5**

**Сглобяеми стоманени конструкции**

| **№ по ред** | **Наименование на отклонението** | **Допустимо отклонение в mm** |
|---|---|---|
| 1 | **Ферми, греди, ригели, столици** | |
| | 1.1. Отклонение в нивото на опорните възли на ферми и ригели | ± 20 |
| | 1.2. Отклонение на горния пояс (в средата на отвора) от вертикалната плоскост, минаваща пред центровете на опорите | 1/500 от височината на конструкцията |
| | 1.3. Отклонение в разстоянието между осите на фермите, мерено по горния пояс | 15 |
| | 1.4. Отклонение в разстоянието между столиците | 10 |

## 3 Обосновка на точността на плановите и височинни мостови геодезически мрежи и трасировъчни работи

Авторът е извършил обосновка на точността на плановите и височинни мостови геодезически мрежи използвани при строителството на мостове, въз основа на строително-монтажните допуски, регламентирани в българската нормативна уредба.

На базата на част от допустимите отклонения, включени в систематизираната извадка, с използване на закона за предаване на грешките и в частност – теорията на размерните

вериги, са определени изискванията за точност на геодезическите измервания, извършвани при трасиране, контрол и приемане на СМР.

Една от най-важните задачи при обосновката на точността на геодезическите измервания е да се определи точността на геодезическите мрежи и точността на трасиране. Точността на геодезическите мрежи за нуждите на мостовото строителство е необходимо да удовлетворява изискванията за точност на всички видове СМР, извършвани на обекта.

За обосновката на точността на плановата мостова геодезическа мрежа, в качеството на изходен параметър, авторът предлага използването на допустимото отклонение в „дължината или светлия отвор на елемента“ (т.2 от табл. 4), което тук се асоциира с допустимото отклонение на статичния светъл отвор на мост.

Споменатото допустимо отклонение е представено като резултат от натрупване на съответните отклонения при изпълнение на предходните СМР (1):

$$(m_{\text{св.отв.}}^{\text{доп}})^2 = 2\left(m_{\text{тр.}}^{\text{доп}}\right)^2 + 2\left(m_{\text{израб.+верт.}}^{\text{доп}}\right)^2, \quad (1)$$

където: $m_{\text{св.отв.}}^{\text{доп}}$- допустима грешка на определяне на светлия отвор на моста ($m_{\text{св.отв.}}^{\text{доп}} = \pm 20mm$ - табл. 4); $m_{\text{тр.}}^{\text{доп}}$- допустима грешка в положението на центровете на опорните повърхности на фундаментите при трасирането; $m_{\text{израб.+верт.}}^{\text{доп}}$ - сумарна допустима грешка от изработването на стълбовете.

При обосновката на точността на височинната мостова геодезическа мрежа се цели да се определят допустимите грешки в котите на временните и постоянни репери като функция на СМД. От стойностите в табл. 4, в качеството на изходна величина, се използва допустимото отклонение в „котите на повърхностите и на закладните детайли, служещи за опори на метални или сглобяеми стоманобетонни колони и други сглобяеми елементи“ - $m_{H_i}^{\text{доп}}$ (2):

$$\left(m_{H_i}^{\text{доп}}\right)^2 = \left(m_{H_{\text{ВНР}_i}}^{\text{доп}}\right)^2 + \left(m_{\text{тр}}^{\text{доп}}\right)^2 + \left(m_{\text{бет.р.}}^{\text{доп}}\right)^2, \quad (2)$$

където: $m_{H_i}^{\text{доп}}$ - допустима грешка в котата на горната повърхност на коя да е мостова опора; $m_{H_{\text{ВНР}_i}}^{\text{доп}}$- допустима грешка в котата на всеки един временен нивелачен репер; $m_{\text{тр}}^{\text{доп}}$ - допустима грешка от трасирането; $m_{\text{бет.р.}}^{\text{доп}}$ - допустима грешка от бетоновите работи.

Обосновката на точността на плановите и височинни мостови геодезически мрежи и трасировъчни работи не е включена в настоящия доклад, поради големия обем от информация, но е подробно описана в дисертацията на автора [5]. По-долу са представени само основни изводи и препоръки изведени въз основа на извършената обосновка на точността.

При обосновката на точността на плановите мостови геодезически мрежи и плановите трасировъчни работи са определени:

- Допустимите грешки в положението на изходните точки от плановите мостови геодезически мрежи:
  - ✓ при използване на принципа на равните влияния - $m_{\text{изх}}^{\text{доп}} = \pm 9.5mm$
  - ✓ при използване на принципа на пренебрежимо малкото влияние - $m_{\text{изх}}^{\text{доп}} = \pm 4.5mm$.
- Допустимата грешка в положението на центровете на опорните повърхности на фундаментите при трасирането - $m_{\text{тр.}}^{\text{доп}} = \pm 13.4mm$ и допустимата грешка от трасировъчните операции $m_{\text{тр.оп.}}^{\text{доп}}$:
  - ✓ при използване на принципа на равните влияния - $m_{\text{тр.оп.}}^{\text{доп}} = \pm 9.5mm$

- ✓ при използване на принципа на пренебрежимо малкото влияние - $m_{\text{тр.оп.}}^{\text{доп}} = \pm 12.6mm$.

От анализа на изведените стойности на допустимите грешки, се препоръчва използването на първия принцип (принципа на равните влияния), тъй като при втория - допустимата точност в положението на изходните точки от плановата мостова инженерно-геодезическа мрежа (ПМИГМ) е двойно по-висока, което е по-трудно постижимо, а допустимата грешка от трасировъчните операции не се увеличава значително – само с около 25%. При условие, че проектираната ПМИГМ ще се използва и при изследване на деформациите на мостовата конструкция, то изискваната точност трябва да бъде тази, определена при принципа на пренебрежимо малкото влияние, а именно $m_{\text{изх}}^{\text{доп}} = \pm 4.5mm$.

При обосновката на точността на височинните мостови геодезически мрежи и височинните трасировъчни работи са определени:

- ➢ Допустимите грешки в котите на временните и постоянни репери като функция на строително-монтажните допуски, регламентирани в българската нормативна уредба, съответно:
  - ✓ за временните репери $m_{H_{\text{ВНР}_i}}^{\text{доп}} = \pm 4.7mm$
  - ✓ за постоянните репери:
    - $m_{H_{\text{ИНР}}}^{\text{доп}} = \pm 3.3mm$ (при прилагане на принципа на равните влияния
    - $m_{H_{\text{ИНР}}}^{\text{доп}} = \pm 1.6mm$ (при използване на принципа на пренебрежимо малкото влияние).
- ➢ Допустимата грешка от трасирането $m_{\text{тр}}^{\text{доп}} = \pm 1.4mm$ и допустимата грешка в измереното превишение между изходния и временен нивелачен репер $m_{\Delta h_{\text{ИНР,ВНР}_i}}^{\text{доп}}$:
  - ✓ при използване на принципа на равните влияния - $m_{\Delta h_{\text{ИНР,ВНР}_i}}^{\text{доп}} = \pm 3.3\text{mm}$
  - ✓ при използване на принципа на пренебрежимо малкото влияние - $m_{\Delta h_{\text{ИНР,ВНР}_i}}^{\text{доп}} = \pm 4.4\text{mm}$.

Препоръчва се използването на принципа на равните влияния, тъй като при използването на принципа на пренебрежимо малкото влияние – допустимата точност в котата на изходния нивелачен репер е двойно по-висока, което е по-трудно за реализиране, а допустимата грешка в измереното превишение между изходния и временния нивелачен репер се увеличава само с 25 %.

# 4 Заключение

В настоящия доклад е извършен анализ, оценка и систематизиране на строително-монтажните допуски от нормативната уредба в Република България, отнасящи се до строителството на монолитни и сглобяеми конструкции на мостове. Направена е обоснована е точността на плановите и височинни геодезически мрежи, използвани при строителството на мостове, въз основа на строително-монтажните допуски, регламентирани в българската нормативна уредба.

**ЛИТЕРАТУРА:**

[1] Наредба № 3 за контрол и приемане на бетонни и стоманобетонни конструкции. обн. ДВ. бр. 97 от 25 ноември 1994. изм. бр. 53 от 11 юни 1999.

[2] Правила за извършване и приемане на строителни и монтажни работи – Сгради. СЕК. 2008.

[3] Правила за извършване и приемане на строителни и монтажни работи – Съоръжения. СЕК. 2007.

[4] Правилник за извършване и приемане на строителни и монтажни работи. С. Техника. 1977.

[5] Стефанова, А., Проблеми на геодезическото осигуряване при строителството на мостове, София, УАСГ, Дисертация, 2019

[6] Стойчев, Д., Г. Милев, А. Гълъбов. Геодезически работи в строителството. Техника. 1983.

[7] Техническа спецификация, Агенция „Пътна инфраструктура" при МРР. С. 2014.

# USE OF REMOTE METHODS FOR ASSESSMENT AND ECOLOGICAL MONITORING OF AGROECOSYSTEMS IN MOUNTAIN REGIONS*

**KRISTINA K. YANCHEVA**

***ABSTRACT:*** *The report examines the use of remote sensing methods for assessment and ecological monitoring of agroecosystems in mountainous regions. The main emphasis is on modern technologies, such as satellite images, drones and geographic information systems (GIS), which allow continuous monitoring of environmental conditions in these hard-to-reach territories. The advantages of remote monitoring for tracking soil erosion, water resources, biodiversity and climate change are discussed, emphasizing its importance for the sustainable management of agroecosystems. The report also analyzes the main challenges in the implementation of these technologies and outlines the prospects for their future development, in view of the increasing climate changes and the need for environmental protection.*

***KEYWORDS:*** *agroecosystems, mountain regions, geographic information systems [GIS], ecological monitorin*

***DOI: https://doi.org/10.46687/HTTH1043***

# ИЗПОЛЗВАНЕ НА ДИСТАНЦИОННИТЕ МЕТОДИ ЗА ОЦЕНКА И ЕКОЛОГИЧЕН МОНИТОРИНГ НА АГРОЕКОСИСТЕМИТЕ В ПЛАНИНСКИТЕ РАЙОНИ

**КРИСТИНА К. ЯНЧЕВА**

***АБСТРАКТ:*** *Докладът разглежда използването на дистанционни методи за оценка и екологичен мониторинг на агроекосистемите в планинските райони. Основният акцент е върху съвременните технологии, като сателитни изображения, дронове и географски информационни системи (ГИС), които позволяват непрекъснато наблюдение на екологичните условия в тези труднодостъпни територии. Изследват се предимствата на дистанционния мониторинг за проследяване на почвена ерозия, водни ресурси, биоразнообразие и климатични промени, като се подчертава значението му за устойчивото управление на агроекосистемите, Извършен е анализ на основните предизвикателства при прилагането на тези технологии, като са очертани перспективите за бъдещото им развитие, с оглед на нарастващите климатични промени и нуждата от опазване на околната среда.*

## 1 Въведение

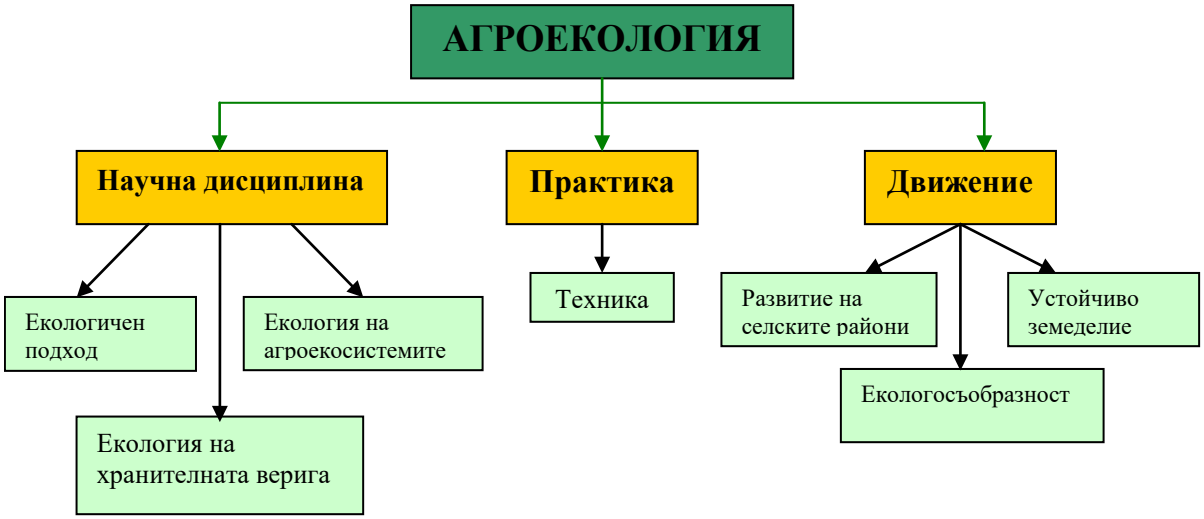
Агроекосистемите в планинските райони са изключително уязвими на екологични промени и човешка дейност. Климатичните условия, релефът и ограничените ресурси правят тези райони особено податливи на ерозия, загуба на биоразнообразие и деградация на почвите. В същото време, те играят важна роля в местната икономика, осигурявайки продукция от селското стопанство, особено в устойчивите практики. За ефективното управление и опазване на тези екосистеми е необходимо да се извършва непрекъснат екологичен мониторинг, а един от най-съвременните методи за това е използването на дистанционни технологии (Remote Sensing, RS).

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

## 2 Значение на агроекосистемите в планинските райони. Предмет на Агроекологията

Понастоящем терминът „Агроекология” означава:

- научна дисциплина;
- земеделски практики;
- социално/политическо движение;




**Фиг. 1.** Многообразие на настоящите видове значения на агроекологията

В по-тесен смисъл агроекологията е наука, която изучава екологичния феномен в **агроекосистемите**. Агроекологията разглежда екологичните взаимовръзки в една агрофитоценоза и нейната задача е да осветли формите, динамиката и функционирането на тези взаимовръзки.

Агроекосистемите са създадени от изменени в резултат на човешката дейност природни екосистеми (гори, естествени ливади и пасища), които частично са се запазили и все още съществуват между земеделските площи. В този смисъл, агроекосистемите представляват урбанизирани екосистеми, които по структура и функции са по-близки до природните, в сравнение с градските екосистеми и по-добре от тях се вписват в ландшафта. [4]

Агроекосистемите в планинските региони се характеризират с висока екологична и агрономическа стойност. Те често включват култури и пасища, които се използват за традиционно земеделие и отглеждане на животни. Тези райони също играят важна роля за опазване на водните ресурси, предотвратяване на почвената ерозия и съхранение на въглерод. [1]

Тъй като условията на живот и земеделие в планинските региони са значително различни от тези в равнинните области, тяхното управление изисква специфични подходи. Неправилното използване на земята може да доведе до сериозни екологични последици, като влошаване на водните ресурси и загуба на почви. [7]

## 3 Дистанционни методи за мониторинг.

Дистанционните методи за мониторинг на агроекосистемите включват използване на сателитни изображения, дронове, географски информационни системи (GIS) и други технологии, които позволяват събиране и анализ на данни за околната среда от разстояние.

Тези технологии предлагат редица предимства, включително мащабност, висока прецизност и възможност за редовен мониторинг.

### 3.1. Сателитни изображения

Сателитните технологии са едни от най-използваните в дистанционния мониторинг на агроекосистеми. С тяхна помощ може да се наблюдава растежът на културите, влагата в почвата, промените в растителното покритие и разпространението на вредители. Използването на различни сателити, като Landsat, Sentinel и MODIS, позволява наблюдението на промените във времето и пространството с висока прецизност.

Сателитите могат да осигурят данни за различни спектрални диапазони, включително видимата светлина, инфрачервената светлина и топлинното излъчване, които са полезни за оценка на здравословното състояние на растенията и почвените условия. [10]

### 3.2. Дронове

Дроновете, или безпилотни летателни апарати (БЛА), са мощен инструмент за мониторинг на малки и средни по мащаб агроекосистеми [3]. Те позволяват по-подробен анализ на местните условия в сравнение със сателитите, тъй като могат да летят на по-ниска височина и да заснемат с по-голяма резолюция. Дроновете се използват за картографиране на терена, проследяване на състоянието на почвите и културите, както и за откриване на проблеми с водоснабдяването или наличие на вредители.

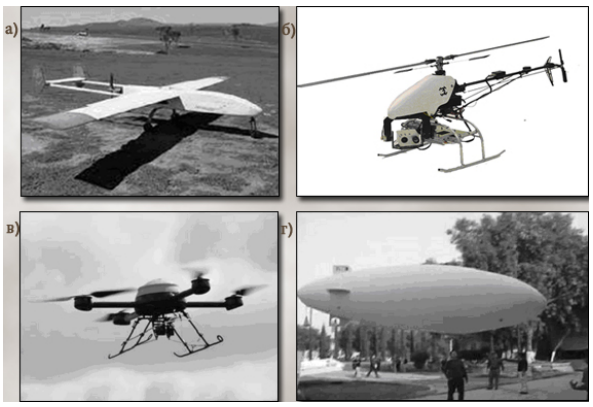
Терминът „Безпилотен Летателен Апарат" - БЛА (заимстван от Unmanned Air Vehicle или Unmanned Air System) следва да се използва само за онези летателни апарати, които носят определена научна или изследователска апаратура, чрез която се събира информация за решаването на определени, важни за обществото задачи.

Говорейки за професионално/научно използване на такава техника, следва да се прилага термина „Безпилотна летателна система (БЛС)". Обединяваща три основни подсистеми:

*Първата подсистема* на БЛС е летателният апарат, който в зависимост от конструктивното решение може да бъде:

- Апарат с „фиксирано крило" (с дърпащ или тласкащ вариант на пропелера);
- Апарат с „ротиращо крило" (с разновидност от 1 до 8 ротиращи крила);
- Апарат, по-лек от въздуха (по примера на дирижабъл);

Освен изброените варианти се правят опити за конструиране на летателни апарати, използващи принципа на „махащи крила", наподобяващи движението на крилата на птиците.




**Фиг. 2.** Варианти на летателният сегмент на БЛА: а) фиксирано крило (тласкащ пропелер); б) ротиращо (централно разположено) крило; в) ротиращо (тип „дрон") крило; г) тип дирижабъл

Задвижването на пропелера или ротиращото крило се осъществява от електрически двигател, двигател с вътрешно горене, горивна клетка или реактивен двигател. [11]

*Втората подсистема* на БЛС е навигационната система, позволяваща извършването на самостоятелен (или подпомаган) контролиран полет по предварително зададен маршрут или маршрут, конструиран в момента на полет.

*Третата подсистема* на БЛС е съставена от различни уреди и инструменти за заснемане, регистриране и измерване, на параметри за оценка на пространствените размери, позиция или състояние на различни обекти и явления.[6];[8]

### 3.3. Географски информационни системи (ГИС)

ГИС е система за събиране, съхранение и анализ на географски данни, която може да интегрира информация от различни дистанционни източници, като сателити и дронове, за създаване на пространствени карти. Тези карти са от голямо значение за управлението на агроекосистемите, тъй като позволяват детайлно моделиране на екологичните условия в даден район. [2]

## 4 Приложение на дистанционните методи в планинските райони.

Планинските райони представляват сериозно предизвикателство за традиционните методи на мониторинг поради труднодостъпните терени и изменчивите климатични условия. Дистанционните технологии обаче позволяват извършването на прецизни оценки на състоянието на агроекосистемите, включително:

- Оценка на почвена ерозия: Чрез анализ на топографските и хидрологичните данни от дистанционни технологии могат да се идентифицират участъци с повишен риск от ерозия и да се предприемат мерки за предотвратяване на деградацията. [2]
- Мониторинг на водните ресурси: Дистанционните технологии позволяват ефективно проследяване на наличието и качеството на водните ресурси, които са ключови за поддържането на агроекосистемите в планинските райони.
- Оценка на климатични промени: Планинските райони са чувствителни на климатични колебания, които могат да влияят на растежа на растенията и на качеството на почвите. С дистанционните методи може да се наблюдават дългосрочни промени в климата и да се предприемат адаптационни мерки.
- Биоразнообразие и растително покритие: С помощта на дистанционните технологии се извършва наблюдение на растителните видове, тяхната плътност и динамиката на техните изменения. Това е важно за запазването на биоразнообразието в планинските агроекосистеми.[2]

## 5 Предизвикателства и бъдещи перспективи.

Въпреки множеството предимства, дистанционните методи за мониторинг на агроекосистемите в планинските райони не са без предизвикателства. Трудностите включват:

- Технически ограничения: Въпреки напредъка на технологиите, метеорологичните условия, като облачност или лошо време, могат да затруднят събирането на качествени данни чрез сателити и дронове.
- Финансови разходи: Инвестицията в оборудване, софтуер и обучение на персонал за работа с дистанционните методи може да бъде висока, особено за малки стопанства в планински райони.

В бъдеще, с развитието на по-усъвършенствани технологии и методи за обработка на данни, дистанционният мониторинг ще стане още по-достъпен и ефективен. Очаква се

разработването на по-добри алгоритми за анализ на големи обеми от данни и по-прецизни модели за предсказване на екологичните промени.[5];[9]

# 6 Заключение

Използването на дистанционните технологии за мониторинг на агроекосистемите в планинските райони предлага възможности за ефективно и устойчиво управление на тези чувствителни екосистеми. Те позволяват непрекъснато наблюдение на екологичните условия, като подпомагат вземането на информирани решения за земеделието и опазването на околната среда. Развитието на тези технологии ще има ключово значение за справянето с предизвикателствата на климатичните промени и деградацията на околната среда в бъдеще.

**ЛИТЕРАТУРА:**

[1] Андреев, К. (2021). Интегрирано използване на дистанционни методи и ГИС за мониторинг на агроекосистеми в България. Списание по земеделие и екология, 12(4), 35-47.

[2] Боев, Н. (2019). Приложение на географски информационни системи за оценка на екологичното състояние на агроекосистеми. София: Университетско издателство.

[3] Янчев К., Кирилова К. Оценка на възможността за практическо използване на безпилотна летателна система при триизмерно моделиране на теренна повърхнина. Научна конференция с международно участие MATTEX 2020, Сборник научни трудове, Том 2, Шумен, ISSN: 1314-3921, стр. 247-254

[4] Jones, H. G., & Vaughan, R. A. (2010). Remote Sensing of Vegetation: Principles, Techniques, and Applications. Oxford University Press.

[5] FAO. (2021). Mountain Agriculture: Opportunities for Green Solutions. Food and Agriculture Organization of the United Nations. Достъпно на: http://www.fao.org

[6] European Space Agency (ESA). (2020). Sentinel-2 for Agriculture. Достъпно на: https://www.esa.int

[7] Zhang, C., & Kovacs, J. M. (2012). The application of small UAVs for precision agriculture: A review. Precision Agriculture, 13(6), 693-712.

[8] NASA Earth Observatory. (2021). Remote Sensing for Agricultural Monitoring. Достъпно на: https://earthobservatory.nasa.gov

[9] Moran, M. S., et al. (1997). Opportunities and limitations for image-based remote sensing in precision crop management. Remote Sensing of Environment, 61(3), 319-346.

[10] Симов, П. (2020). Използване на сателитни данни за мониторинг на планински агроекосистеми. В: Годишник на Аграрния университет, 65(1), 89-102.

[11] Gavrilaş, I. (2021). The impact of climate changes on mountain agriculture and the use of GIS technology in sustainable development. Environmental Monitoring and Assessment, 193(6), 399.

# THE FUTURE OF GEODESY*

**VANESA G. GEORGIEVA, EVGENI G. STOYKOV**

***ABSTRACT:*** *Geodesy is a science that deals with the measuring and representing the Earth and its shape, size, gravitational field and the position of objects on its surface. It plays a key role in various fields such as cartography, construction, navigation and land use.*

***KEYWORDS:*** *geodes, GNSS, measuring, navigation, cartography*

***DOI: https://doi.org/10.46687/OQCA4962***

# БЪДЕЩЕТО НА ГЕОДЕЗИЯТА

**ВАНЕСА Г. ГЕОРГИЕВА, ЕВГЕНИ Г. СТОЙКОВ**

***АБСТРАКТ:*** *Геодезията е наука, която се занимава с измерването и представянето на Земята и нейната форма, размер, гравитационно поле и позицията на обекти на повърхността ѝ. Тя играе ключова роля в различни области, като картография, строителство, навигация и земеползване.*

## 1 Въведение

С напредъка на технологиите и иновациите, бъдещето на геодезията обещава да бъде динамично и интензивно. Възможностите за интегриране на нови методи, като дронове, сателитни технологии и геоинформационни системи, ще разширят обхвата на геодезичните приложения.

Този доклад ще разгледа как тези нововъведения ще повлияят на различни области, включително строителството, екологията и градското планиране, и как геодезията ще продължи да се развива в отговор на нарастващите нужди на съвременното общество.

## 2 История

За баща на науката геодезия се смята Ератостен (276 г. пр.н.е. – 194 г. пр.н.е., в гр. Cyrene днешен Shahhat, в Либия) Фиг. 1, който е бил третият директор на библиотеката в Александрия и е астрономът, измерил за първи път размерите на Земята.

Думата геодезия (γεωδαισία – geodaisia) има гръцки произход и в превод на български означава „разделяне на Земята". Следователно, науката е пряко свързана с човешката дейност и по-конкретно с използването на земята за земеделие, животновъдство, различни производства или строителство.

Смята се, че още в древните Асировавилония и Египет геодезическите измервания са били редовна практика. Тя била свързана главно с възстановяването на границите на земите на отделните владетели след годишните приливи и отливи на река Нил.

Геодезията се разделя на няколко основни дяла:

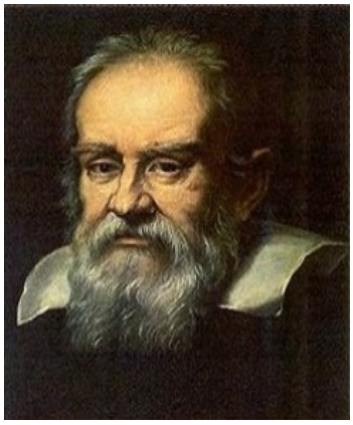
- Висша геодезия, която се занимава с глобални измервания на Земята (обикновено с размери над 500 м 2 ), като се взема предвид кривината на Земната повърхност.

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи"

- Практическа (инженерна) геодезия, при която се измерват по-малки по площ и специфични части и региони на Земята, като кривината може да се пренебрегне, тъй като тя не оказва практическо значение

- Космическа геодезия, чиято задача е определянето на разстоянията между отдалечени една от друга точки на Земната повърхност и изучаване на промяната във формата на Земята с времето (с помощта на сателитни изследвания).

- Физическа геодезия – изследва физичните свойства на гравитационното поле на Земята и Геопотенциала от гледна точка на тяхното приложение в геодезията.- Картографията (идва от гръцката дума: Χάρτης- харта, чартах - означаваща папирус и „графос” – чертая) в началото е била част от геодезията, но с възникването на необходимостта от различни по вид и свойства карти, тя се обособява като отделна наука. Има за основна цел създаването, изучаването и разработването на карти.



**Фиг. 1.** Портрет на Ератостен

Картите са съществували още от дълбока древност (Фиг. 2), като дори и първобитните хора са използвали някакъв примитивен вид карти.



А)



Б)

**Фиг. 2.** Древни карти:
А) План на град, изработен на глинена плочка, Месопотамия, XV в. пр.н.е.
Б) Египетски рай, „тръстиково поле”, изработена от смола (2500 в. пр.н.е.)

В съвременността картите са тематични, като освен такива изобразяващи релефа съществуват и други показващи различни аспекти от съвременния ни живот.

В бъдещето може да се очаква картите да бъдат много по-интерактивни и динамични с интеграцията на технологии като ГНСС, дронове и 3D моделиране. Също така може да включват реалновременни данни за географски характеристики, климатични условия и дори информация за инфраструктурата.

С развитието на дроновете и безпилотните летателни апарати, геодезията получава нови инструменти за събиране на данни. Дроновете могат да извършват бързи и точни измервания на труднодостъпни райони, което значително подобрява ефективността на геодезичните проекти. Освен това, сателитните технологии, включително системи за глобално позициониране (ГНСС), предоставят висока прецизност и възможности за наблюдение на промените в земната повърхност.

Геоинформационните системи играят важна роля в анализа и визуализацията на геодезичните данни. Те позволяват интегрирането на различни видове информация, което улеснява вземането на решения в области като градско планиране, управление на природни ресурси и екологични изследвания. Бъдещето на ГИС ще бъде свързано с развитието на изкуствения интелект и машинното обучение, които ще подобрят обработката на данни и предсказването на тенденции.

Геодезията намира приложения в множество области, включително строителството, транспорта и опазването на околната среда. С увеличаването на населението и урбанизацията, геодезичните данни стават все по-важни за устойчивото развитие на градовете. Геодезистите ще играят ключова роля в проектирането на инфраструктура и управление на земята, като осигуряват точни измервания и анализи.

# 3 Заключение

Бъдещето на геодезията е обещаващо, благодарение на напредъка в технологиите и новите приложения, които се появяват. Съчетаването на традиционните методи с иновации като дронове и ГИС ще доведе до нови възможности за изследване и управление на Земята. Геодезията ще продължи да бъде важен инструмент за справяне с предизвикателствата на съвременния свят и за подпомагане на устойчивото развитие.

**ЛИТЕРАТУРА:**

[1] http://web.uni-plovdiv.bg/exner/Geodesy_Cartography_GPS/GKGPS_lectures_2012.pdf

[2] https://treto-gd.com/mathematicians/index.html

# RADIOCOMMUNICATION TECHNOLOGY IN GEODESY*

**STEFAN D. DOBREV**

***ABSTRACT:*** *Radiocommunications yield us many benefits, one of each is casting corrections on UHF radio band for receiving accurate position from one GNSS receiver to another.*

***KEYWORDS:*** *radiocommunications, UHF radio, GNSS measurements in RTK mode, Satel easy pro, Leica*

***DOI: https://doi.org/10.46687/YJFJ5894***

# РАДИОКОМУНИКАЦИОННИ ТЕХНОЛОГИИ В ГЕОДЕЗИЯТА

**СТЕФАН Д. ДОБРЕВ**

***АБСТРАКТ:*** *Радиокомуникациите ни дават различни възможности, една от които е да предаваме навигационни корекции чрез УВЧ за получаване на точно позициониране от един ГНСС приемник към друг.*

## 1 Въведение

В Геодезията, глобалните навигационни спътникови системи (ГНСС) намират приложение в широк набор от дейности, като определяне на точки от геодезически мрежи с местно предназначение (ГММП), приравнени към тях или отговарящи на по-високи изисквания, от работна геодезическа основа (РГО) и приравнените към тях, извършване на геодезически снимки, трасиране на проектни точки и др.

За извършване на измервания чрез ГНСС методи е необходимо да се извършват едновременни измервания на една базова станция и една определяема точка, при което:

1. измерванията на базовите станции са непрекъснати и продължават през цялото време, докато се осъществяват измервания на определяеми точки;

2. измерванията на определяемите точки са с продължителност, специфична за прилагания ГНСС метод и вида на извършваната работа, съгласно чл. 28, 31, 35 и 39.

(3) При прилагане на ГНСС методи в реално време базовите станции съвпадат с изходни точки [5].

Измерванията в реално време – Real-time kinematic (RTK), е ГНСС метод за високоточно определяне на координатите на точки. Тази технология намира приложение в голям спектър от задачи, не само в Геодезията, но и в навигацията. В този доклад, ще разгледаме какво потребителско оборудване е необходимо за определяне на точки в реално време според чл. 21, ал. 4 от Инструкция № РД-02-20-25 ОТ 20 СЕПТЕМВРИ 2011 Г. ЗА ОПРЕДЕЛЯНЕ НА ГЕОДЕЗИЧЕСКИ ТОЧКИ С ПОМОЩТА НА ГЛОБАЛНИ НАВИГАЦИОННИ СПЪТНИКОВИ СИСТЕМИ- В сила от 11.10.2011 г. Издадена от Министерството на регионалното развитие и благоустройството Обн. ДВ. бр.79 от 11 Октомври 2011г.:

Чл.21. Потребителското ГНСС оборудване отговаря на следните основни изисквания:

1. позволява центрирането върху геодезически точки;

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

2. при прилагане на методи с последваща обработка записва в паметта си първичните данни по чл. 9, ал. 2, а при наличие на вградено или външно устройство за управление - също и индивидуални данни за измерените точки;

3. при прилагане на методи в реално време подвижната апаратура приема по радиото, чрез клетъчни или спътникови комуникации базови или корекционни данни от източниците по чл. 15, ал. 1;

4. при прилагане на ГНСС методи в реално време в случаите по чл. 4, т. 2 базовата апаратура предава по радиото, чрез клетъчни или спътникови комуникации базови или корекционни данни. [5]



**Фиг. 1.** Два броя приемници на Leica, единия базов (в ляво), а другият подвижен (в дясно)

## 2 ГНСС оборудване за извършване на измервания в реално време

Необходимото потребителското ГНСС оборудване, за извършване на измервания в реално време (RTK) се състои от минимум два броя ГНСС приемници, който трябва да имат съответната хардуерна и софтуерна възможност за предаване на корекции чрез радио връзка. Има различни видове модели приемници, в някои има вграден радио модул за излъчване и приемане на корекции, други разполагат само с вграден модем, който позволява използването на външно радио.

За разлика от метода Network RTK, при връзката с радио е необходимо да се използват различни по тип антени и адаптери за предаване и приемане на сигнала.




**Фиг. 2.** Антени и адаптери на Leica

Според изискванията на гореспоменатата инструкция, базовият приемник, трябва да има възможността да се центрира върху геодезически точки. Това обуславя използването на глава с оптичен или механичен отвес, което от своя страна изисква използването на тринога. Подвижния приемник (роувър), се монтира на подходящ за ГНСС измервания щок – виж фигура 3.




**Фиг. 3.** Потребителското ГНСС оборудване от два приемника, за извършване на измервания в реално време (RTK)

От фигура 3 се вижда, че за извършване на ГНСС измервания с потребителска базова станция в реално време, освен двата приемника са необходими: един щок, един брой тринога за базовия приемник (за предпочитане – дървена), един брой тринога за поставяне на излъчвателната антена (може да се ползва и щок с дву или триподна стойка). В случай че базовия приемник няма вградено излъчвателно радио, е необходимо да се използва външно такова. За външното радио е необходимо и допълнително захранване.

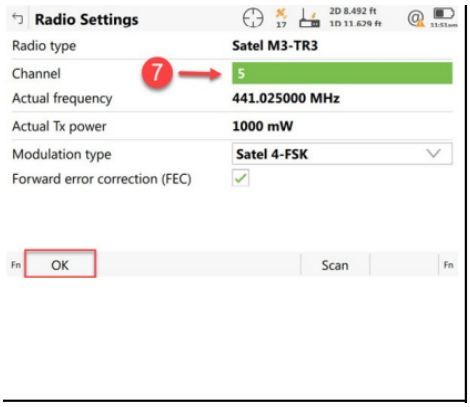
Препоръки при стартиране на базовата станция с радио SATEL EASYPRO 35W, за покриване на 8 km базова линия на предаване(фигура 3):

1. Повдигнете антената на базовия приемник на височина от 3-5 m.
2. Използвайте антена поне 5dB.
3. Проверете окабеляването на базата с радиото, захранването и всички антени. Препоръчителната е подмяната на кабелите и конекторите на всеки 3-4 години.
4. Уверете се, че захранването което използвате е акумулаторна батерия - 12V, с поне 50 AH.
5. Заредете батерията напълно, нощта преди полските измервания. Индикацията на външното радио трябва да отчита 12.8-13.1V.
6. Поставете базата на открито място, без препятствия на поне 13° от хоризонта и на поне 25 m от линия с високо напрежение, ако е възможно.




**Фиг. 4.** Външно радио TRIMTALK с външно захранване за излъчване на корекции реално време (RTK)

След изпълнението на горе описаните препоръки, базовият приемник може да бъде стартиран и да се измерят или въведат координатите на базовата точка. Това става чрез софтуера на фирмата производител на приемниците, в някои случаи може да се ползва и друг софтуер. Важен момент тук е избора на носеща честота (канал – виж фигура 5) за корекциите от базовия приемник към подвижния. Двата приемника трябва да са на един и същ канал с еднакви настройки, и трябва да се избере подходящ канал, спрямо законодателството на съответната държава, в която се извършват измерванията.




**Фиг. 5.** Избор на канал и носеща честота

На територията на Европейски съюз и Република България, важат законови разпоредби за използването на различни радио-честотни диапазони, в т.ч. и потребителските базови станции, трябва да заемат законово определен диапазон от радиочестотната лента. Към Подзаконови актове по Закона за електронните съобщения са описани и Правила за свободно използване на радиочестотния спектър. В Приложение 1 - Радиочестотен спектър, който се използва от радио съоръжения и електронни съобщителни мрежи са регламентирани различните приложения и честоти на потребителските и комерсиални радиопредаватели.

За нуждите на геодезията радиопредавателите вградени в приемниците и външните радиа, могат да се причислят към подвижните, ръчно преносими устройства (PMR446, към които спадат и уоки-токитата), които трябва да излъчват в диапазона от 446.0 – 446.2 MHz, това са честоти и канали за свободно ползване /без лиценз.

**Таблица 4**

| | № | Параметър | Описание | Коментар |
|---|---|---|---|---|
| Нормативна част | 1 | *Радиослужба* | Подвижна | |
| | 2 | *Приложение* | PMR446 | PMR446 са ръчно преносими устройства (не се използват базови станции или ретранслатори) и при тях се използват вградени антени само с цел да се постигне максимално споделяне и да се сведат до минимум радиосмущенията. Тези устройства функционират в режим на равноправен достъп на къси разстояния и не се използват нито като част от инфраструктурна мрежа, нито като ретранслатори. |
| | 3 | *Радиочестотна лента* | 446.0-446.2 MHz | |
| | 4 | *Разпределение на каналите* | | |
| | 5 | *Модулация/Широчина на заеманата честотна лента* | | |
| | 6 | *Посока/Разделяне* | | |
| | 7 | *Предавателна мощност/Плътност на мощността* | 500 mW e.r.p. | |
| | 8 | *Достъп до канала и правила за заемането му* | Трябва да се използват методи за достъп до спектъра и ограничаване на радиосмущенията, осигуряващи подходящо ниво на работните показатели, така че да са спазени съществените изисквания на Директива 2014/53/ЕС. Ако в хармонизираните стандарти или части от тях, които са били посочени в публикации в Официален вестник на Европейския съюз съгласно Директива 2014/53/ЕС, са описани съответни методи, трябва да се осигури ниво на работните показатели, което е най-малко еквивалентно на осигуряваното от | |

5

**Фиг. 6.** Таблица 4 от Приложение 1 - Радиочестотен спектър, който се използва от радиосъоръжения и електронни съобщителни мрежи

За спазването на тези правила следи Комисията за Регулиране на Съобщенията (КРС) и нарушаването на правилата, може да доведе до глоба за ползвателите на съответната апаратура.

**ЛИТЕРАТУРА:**


[1] Stoykov, Evgeni. 2018 г., „Technology of satellite measurements when creating a GPS network“, Годишник: Технически науки. Том VIII Е. Шумен: Университетско издателство "Епископ Константин Преславски", 153 - 156 стр. ISSN: 1311-834X.

[2] Ivanov S. „Principles of GNSS“. Journal scientific and applied research. Volume 20. Шумен 2021. Университетско издателство „Еп. К. Преславски“. ISSN: 1314-6289. Стр. 27 - 32.Adati, T., Miyazawa, T., On paracontact Riemann manifolds. TRU Math. 13 (2) (1977), 27-39.

[3] K. Yanchev "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.

[4] Д. Петров, Беджева М. “Statistic models of the filling in of a waste depot” (загл. на български: Статистически модели на запълването на депо за битови отпадъци), MATTEX 2018, Сборник научни трудове, том 2, част 2, Университетско издателство „Еп. К. Преславски“ 2018, стр. 60-67, ISSN: 1314-3921.

[5] ИНСТРУКЦИЯ № РД-02-20-25 ОТ 20 СЕПТЕМВРИ 2011 Г. ЗА ОПРЕДЕЛЯНЕ НА ГЕОДЕЗИЧЕСКИ ТОЧКИ С ПОМОЩТА НА ГЛОБАЛНИ НАВИГАЦИОННИ СПЪТНИКОВИ СИСТЕМИ- В сила от 11.10.2011 г. Издадена от Министерството на регионалното развитие и благоустройството Обн. ДВ. бр.79 от 11 Октомври 2011г.

# SPECTRAL REFLECTANCE CHARACTERISTICS OF THE MAIN CLASSES OF NATURAL OBJECTS IN REMOTE SENSING OF THE EARTH'S SURFACE*

**NAYLYAN M. SALIEVA**

***ABSTRACT:*** *Remote sensing is widely used in various fields of human activity and plays an important role in providing objective information for the study and analysis of the real state of many objects and parts of the earth's surface. That is why it is necessary to explore different approaches for their implementation, such as spectrometric methods, which are based on the spectral characteristics of the observed objects. The differences in the values of the measured electromagnetic energy registered by the sensor are used to study the properties of the observed object, without contact with it and without disturbing its integrity.*

***KEYWORDS:*** *remote sensing, spectral reflectance characteristics, natural objects, electromagnetic radiation*

***DOI: https://doi.org/10.46687/FHQC6700***

# СПЕКТРАЛНИ ОТРАЖАТЕЛНИ ХАРАКТЕРИСТИКИ НА ОСНОВНИТЕ КЛАСОВЕ ПРИРОДНИ ОБЕКТИ ПРИ ДИСТАНЦИОННИ ИЗСЛЕДВАНИЯ НА ЗЕМНАТА ПОВЪРХНОСТ

**НАЙЛЯН М. САЛИЕВА**

***АБСТРАКТ:*** *Дистанционните изследвания се използват широко в различни области на човешката дейност и играят важна роля за осигуряването на обективна информация за изучаването и анализирането на реалното състояние на множество обекти и части от земната повърхност. Именно затова се налага да бъдат разучени различни подходи за тяхното провеждане, като например спектрометричните методи, които се основават на спектралните характеристики на наблюдаваните обекти. Разликите в регистрираните от сензора стойности на измерваната електромагнитна енергия се използват за изучаване на свойствата на наблюдавания обект, без контакт с него и без да се нарушава неговата цялост.*

## 1 Въведение

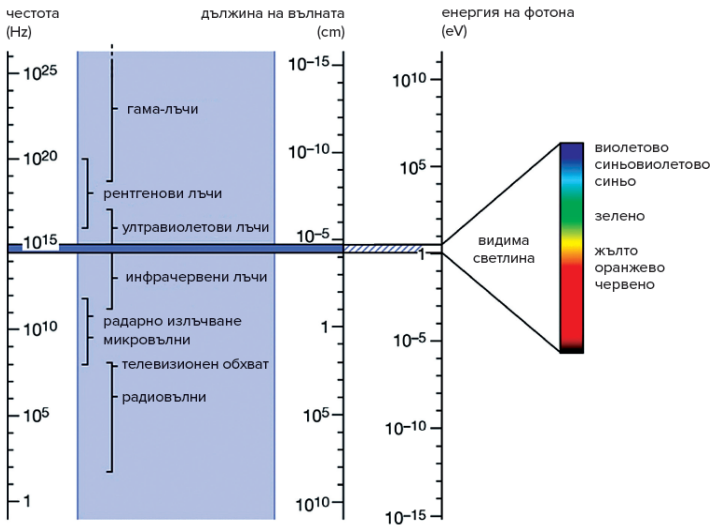
Дистанционните изследвания са наука и метод за получаване на информация за различни обекти, области и явления чрез анализ на изображения и данни, без пряк контакт с изучаваните обекти, като се използват датчици, разположени на въздушни или космически носители, които регистрират електромагнитната енергия от различни диапазони на електромагнитния спектър. Физическата основа на тези изследвания е свързана със способността на материални тела да поглъщат и отразяват по различен начин достигащата до тях електромагнитна енергия и чрез тяхното анализиране се получава информация за изследваните обекти.

## 2 Физически основи на дистанционните изследвания

Дистанционните изследвания се свързват по-конкретно с измерването на взаимодействия между земната повърхност и електромагнитната енергия [1], като се

* Докладът е финансиран по проект № РД-08-122/01.02.2024 г. „Изследване на възможностите за неинвазивно проучване на културно-историческото наследство с геодезични методи“

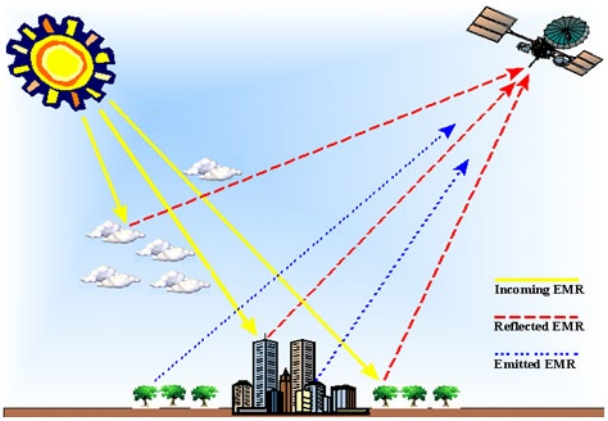
регистрира отразеното или собственото електромагнитно излъчване на изучаваните обекти. Под електромагнитна енергия е прието да се разбира енергията, излъчена в диапазона с дължина на вълната от $10^{-10}$ мкм (космическите лъчи) до $10^{10}$ мкм (радиовълните), а диапазонът, който обхваща дължини на вълните от гама-излъчването до радиовълните, да се нарича електромагнитен спектър [3], показан на фиг. 2. Човешкото око възприема само малка част от електромагнитния спектър, наречена „видима“.




**Фиг. 1.** Електромагнитен спектър [4]

Количеството на енергията, излъчвана от даден обект зависи от следните основни фактори:

- абсолютната му температура;
- излъчвателната му способност;
- дължината на вълната [2].




**Фиг. 2.** Взаимодействия между земната повърхност и електромагнитната енергия

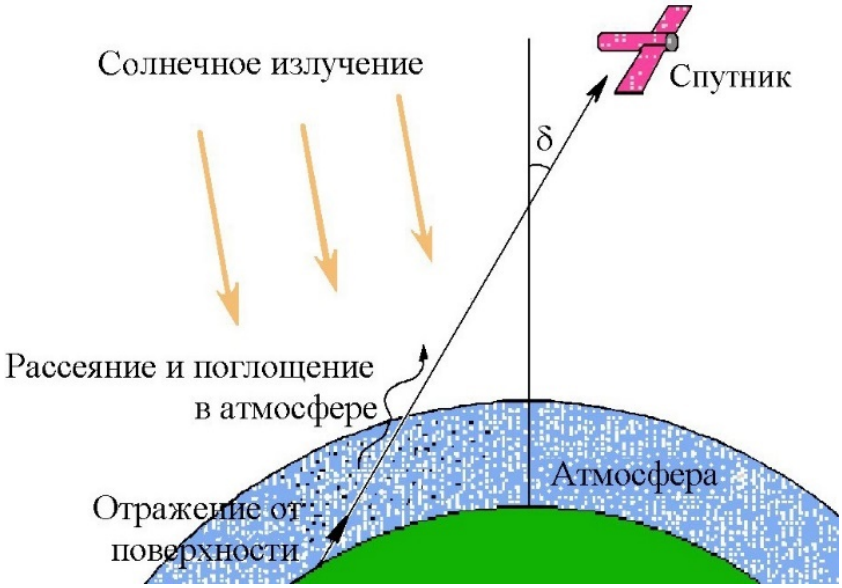
Съществуват три основни източника на електромагнитна енергия, оказващи влияние при дистанционно изследване на обектите:

- излъчването на Слънцето;
- собственото излъчване на Земята;
- изкуственото излъчване.

Един от основните фактори, определящи качеството и ефективността на дадена система за дистанционно изследване на земната повърхност, е спектралната разделителна способност [7]. Именно тя характеризира способността на системите за ДИ да регистрират данни в определени участъци от електромагнитния спектър (с конкретни стойности на дължината на вълната). Колкото е по-високо спектралното разрешение на даден сензор, толкова са повече на брой и са по-тесни по размер диапазоните от електромагнитния спектър, в които той може да регистрира данни, и по този начин да предостави по-богата и по-специфична информация за заснетите обекти [6]. Ето защо при оценката на спектралното разрешение на всеки конкретен сензор се разглеждат две характеристики: количество на каналите му (диапазоните) и ширината на тези канали.

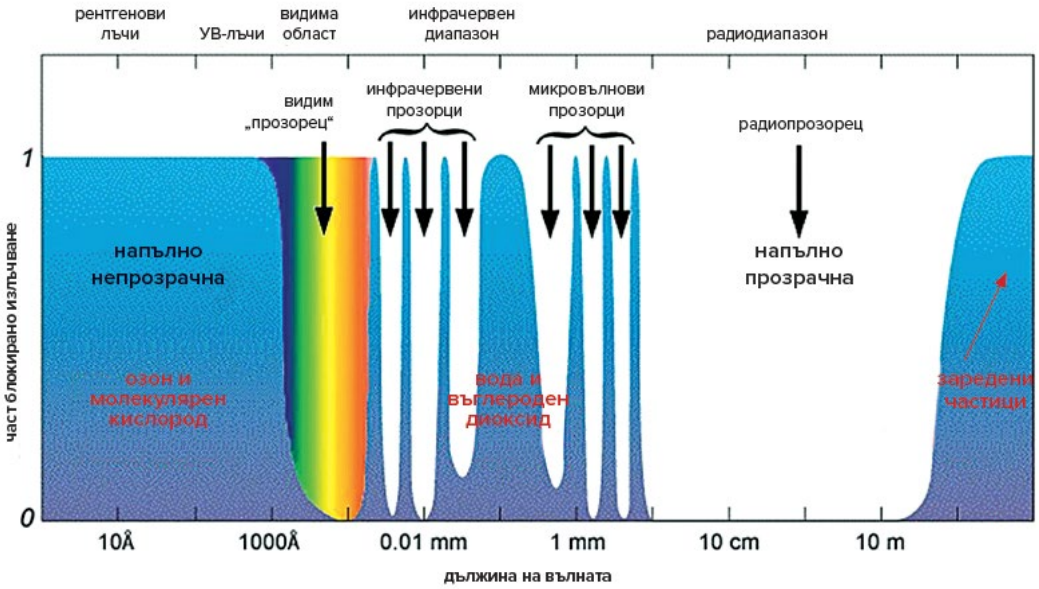
## 3 Въздействия на атмосферата върху електромагнитното излъчване

Въздействията на атмосферата върху електромагнитното излъчване са два основни типа – поглъщане и разсейване, представляващи основните физически процеси, които оказват съществено влияние върху възможността за наблюдение на изследваните обектите.




**Фиг. 3.** Въздействията на атмосферата върху електромагнитното излъчване - Закон на Бугер [4]

Поглъщането на светлината представлява физическо явление на преобразуване на част или цялата електромагнитната енергия във вътрешна (най-често топлинна) или в друга форма на енергия, което води до намаляване на светлинния поток или до пълното му изчезване при неговото разпространение в различните среди и вещества. Тези диапазони от електромагнитния спектър, които лежат извън интервалите на поглъщане, се наричат “прозорци на прозрачност“ на атмосферата (фиг. 4). Само тези „пролуки“ могат се използват за целите на дистанционното изследване, защото само в тях пропускането на атмосферата е достатъчно добро и електромагнитното излъчване може да бъде регистрирано със съответни сензори.




**Фиг. 4.** Прозорци на прозрачност на атмосферата

Тъй като атмосферата се състои от различни газове, водни пари и механични частици, които при съприкосновение с електромагнитните вълни поглъщат електромагнитното излъчване, почти половината от електромагнитните вълни не достигат до земната повърхност. Най-голяма способност за поглъщане на слънчевата енергия притежават озона – $O_3$, въглеродния двуокис – $CO_2$ и водните пари – $H_2O$. Отразената енергия преминава обратно през атмосферата и отново претърпява изменения както на своето спектрално разпределение, така и на интензивността си. След това, излъчването достига до датчика за дистанционно изследване, където то се измерва и се регистрира във вид на конкретни данни.

Разсейването на електромагнитните вълни представлява промяна в посоката им на разпространение, дължаща се на тяхното взаимодействие с молекулите на различните газове и механични частици, съдържащи се в атмосферата. Големината на разсейването зависи от множество фактори като:

- дължината на електромагнитните вълни;
- концентрацията на газове в атмосферата;
- размера на механичните частици;
- разстоянието, което електромагнитните вълни изминават през атмосферата [3].

## 4 Спектрални характеристики на основните класове природни обекти

При взаимодействието на електромагнитните вълни с различните обекти, разположени върху земната повърхност, се осъществява трансформация на енергията на фотоните. То бива три основни типа: поглъщане, отражение и пропускане.

В резултат на това взаимодействие, попадащата върху обектите от земната повърхност енергия Ei се разделя на три основни съставящи:

- отразена енергия ER, съдържаща се в отразените от обектите електромагнитни вълни;

- погълнатата (абсорбирана) енергия EA, която се поглъща от обектите;
- пропусната енергия ET, преминавща през самите обекти.

Съгласно закона за запазване на енергията, връзката между тях може да се изрази със следната формула:

$$EJ(\lambda) = ER,J(\lambda) + EA,J(\lambda) + ET,J(\lambda) \quad (1)$$

Където: λ е конкретната дължина на вълната;

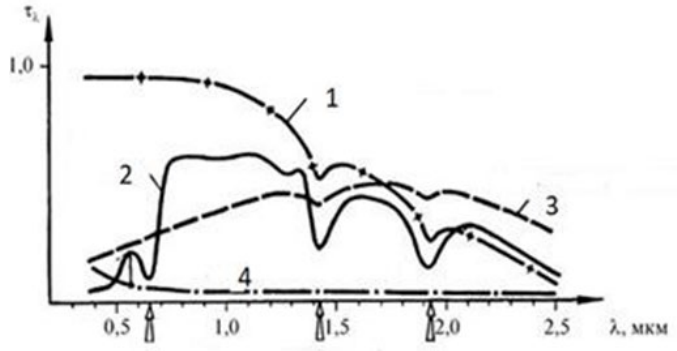
J е даден тип (клас) обекти от земната повърхност.

ER,J(λ) се явява основен демаскиращ признак на обектите при тяхното дистанционно изследване [3].

Отражателната способност на обектите се изразява чрез спектралната плътност на енергийната яркост и може да се измерва със сензорите за дистанционни изследвания. Много е важно е да се разбира, че именно начинът на отражението и поглъщането от обектите на електромагнитна енергия определя стойността на своеобразен вид „сигнал“, който може да бъде регистриран и трансформиран в определена количествена форма. Получените резултатни величини се представят в дискретни цифрови значения, съответстващи на характеристиките на отражателната способност. Тези величини се наричат спектрални коефициенти на яркостта или спектрални яркости. [3] Величината ρλ се нарича спектрална отразяваща способност и играе изключително важна роля в дистанционно изследване.

$$\rho_\lambda = \frac{\text{енергия на отразено излъчване с дължина } \lambda}{\text{енергия на падащо излъчване с дължина } \lambda} * 100 = \frac{E_R(\lambda)}{E_i(\lambda)} * 100 \quad (2)$$

Различните обекти в зависимост от своята физическа природа (структура, химичен състав и др.) и в зависимост от условията (температура, влажност и др.), и дължината на вълната на електромагнитната енергия имат и различни способности за отражение, поглъщане и пропускане на енергията. Тяло, което е способно напълно да погълне падащото върху него електромагнитно излъчване, а след това отново да го излъчи се нарича абсолютно черно тяло. За него както излъчващата способност (e), така и поглъщащата способност (a) са равни на единица. Произволно тяло, температурата на което е по-голяма от абсолютната нула (0 градуса по Келвин), се явява източник на ЕМИ, тъй като неговите молекули се намират във възбудено състояние, което се различава от състоянието на пълен покой. [3] За ДИ най-голямо значение имат следните специфични характеристики на природните обекти*:* Отражателната им способност*;* Коефициентът на отражение; Направлението на отражение; Коефициентът на поглъщане. Проникващата способност е количество електромагнитна енергия, преминаващо през конкретно препятствие със зададена дебелина – атмосфера, почва, бетон, органична и неорганична материя и т.н. При така наречения дискриминантен анализ на природните образувания, въз основа на спектралните им отражателни характеристики се извършва изучаване на земната повърхност, като се използва свойството на различните повърхности и обекти да поглъщат и отразяват по различен специфичен начин падащата върху тях ЕМЕ. Въпреки огромното многообразие от обекти (в земните ландшафти), те могат да се разделят на следните основни класове – сняг, растителност, скали и почви, води, всеки от които се отличава със своя специфична крива на спектралната яркост (фиг. 5) [3].




**Фиг. 5.** Основните класове природни обекти според техните специфични криви на спектрална яркост (1-сняг, 2-растителност, 3-скали и почви, 4-води)

Основните класове природни обекти според техните специфични криви на спектрална яркост са:

*a. Спектрални характеристики на скали и почва – характеризират се с увеличаване на спектралната яркост при приближаване към червената зона на електромагнитния спектър*

Съставът и структурата на почвата влияят силно върху съдържанието на влага в нея и определят вида на отражателните характеристики. Железният окис влияе съществено на отражателната характеристика. Червеният цвят на много почви се обяснява с наличието в тях на нехидратирани железни окиси. Увеличеното съдържание на железни окиси води до значително намаляване на отражателната способност особено във видимия диапазон на спектъра. Намаляването на железните окиси води до повишаване на отражателната способност в диапазона от 0.5-1.1 μm, но на практика не влияе над 1.1 μm. Съдържанието и степента на разлагане на органичните вещества силно влияе на цвета на почвите. Цветът на почва е 5% съдържание на органични вещества е тъмнокафяв или черен, а с ниско съдържание - светлокафяв или сив. Влияние върху цвета оказва и дренирането на почвите и климатичните условия. В зони с тропически и умерено топъл климат дори и при по- ниско съдържание на органични вещества (3%) цветът е черен, а не кафяв. Текстурата на почвата предизвиква увеличение на отражателната способност при намаляване на размера на частиците (колкото е по-малка зърнистостта на почвата, по-висока е отражателната способност).

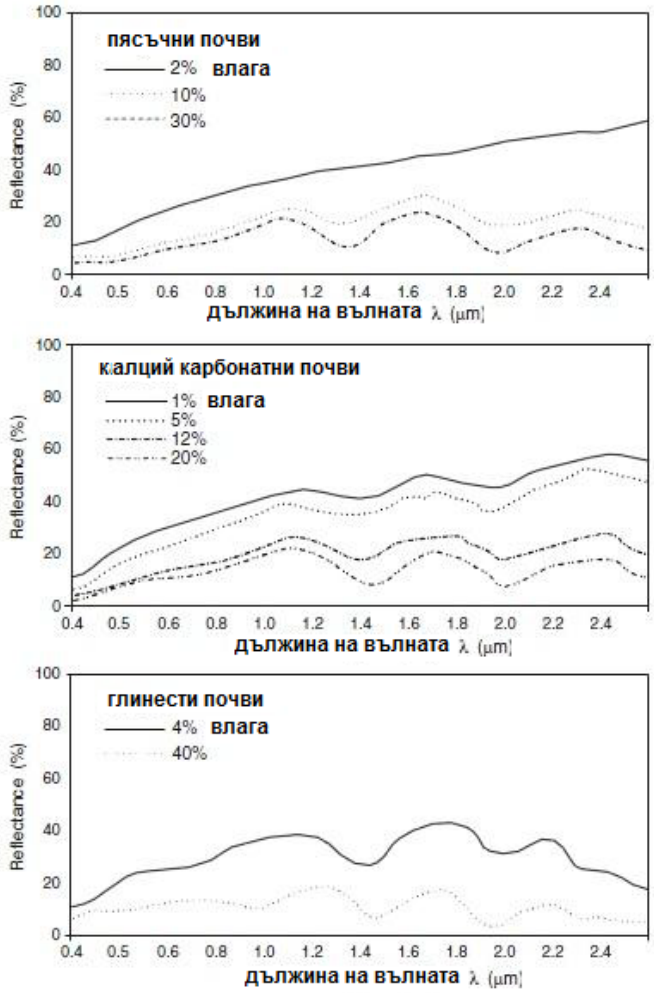
Основен фактор, който влияе върху вида на отражателните характеристики на скалите е видът на скалообразуващите ги минерали, т.е. минералният състав.

*b. Спектрални характеристики на растителната покривка*

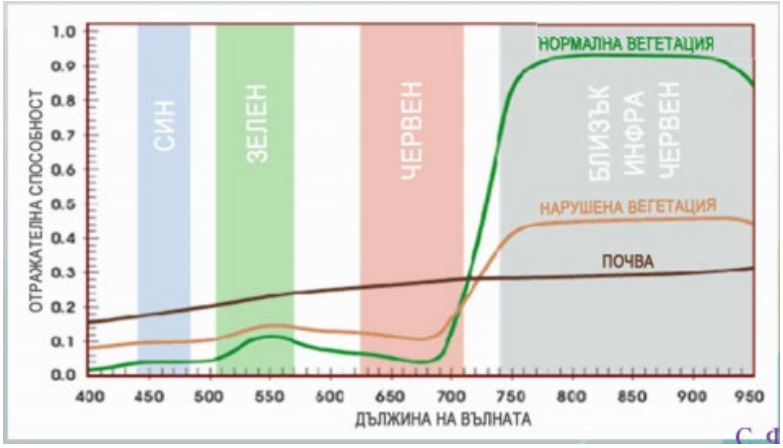
В спектралната отражателна характеристика на зелената растителност има два минимума в областта на синия и червен цвят, съответстващи на поглъщането на хлорофила (максимум в зеления цвят) и минимуми в областта на инфрачервена зона, дължащи се на поглъщането на водата. В близката инфрачервена зона отражателната способност силно се повишава поради слабото поглъщане на зеления лист. В средния инфрачервен диапазон е съществено влиянието на наличието на влага, тъй като съдържанието на влага в зелените листа е значително.

Кривите на отражателните характеристики на почвите не са така сложни както при растителността. Като цяло обща е зависимостта за увеличение на отражателната способност с увеличение на дължината на вълната, особено във видимия и близкия инфрачервен

диапазон на спектъра. Факторите, които влияят на отражателната способност са: влага, органични вещества, железни окиси, глина, прах,пясък, зърнистост на почвата [5].




**Фиг. 6.** Спектрална отражаваща способност на някои типове почви при различен процент на тяхната влажност




**Фиг. 7.** Спектрална отразяваща способност на растенията

*с. Спектрални характеристики на водата и снега*

За отражателните характеристики на водата основно влияние оказва водната повърхност, обусловена от природата на самата вода. Наличието и границите на водните маси лесно се установяват в близкия инфрачервен диапазон. Картографирането на снежната покривка става най-лесно в средния инфрачервен диапазон. Във видимия диапазон върху отражателната способност влияе съдържанието на органични и неорганични вещества. Обработката на спътникови данни показва, че надеждното разделяне на облаците от снега е невъзможно поради еднаквата отражателна способност в диапазона 0.5-1.1μm.

Отражателната способност на облаците и снега е така висока, че детекторите на Landsat се насищат. Тези образувания е възможно да се различат в диапазона 1.55-1.75 μm и съответно 2.1-235 μm. В тези диапазони отражателната способност на облажите е висока (те са с бял цвят), а на снега е ниска и той изглежда по-тъмен (дори черен) [5].

# 5 Заключение

Анализът на специфичните особености на отделните класове обекти да отразяват, поглъщат и излъчват ЕМЕ в различни спектрални зони е в основата на всички методи за ДИ и извличането на качествени характеристики от изображенията в дребни мащаби се базира именно на различната им отражателна способност. Посредством спектралните отражателни характеристики на природните обекти е възможно да се извършва изучаването на земната повърхност чрез ДИ.

**ЛИТЕРАТУРА:**

[1] Eastmand, J. Ronald. Guide to GIS and Image Processing, Volume 1, Clark University (2001).

[2] Толстохатько, Пеньков. Фотограмметрия и дистанционное зондирование. Харъков - ХНАГХ (2013).

[3] Здравчева Н., Дистанционни изследвания, лекционен курс, София (2021).

[4] Кашкин, В. Б, А. И. Сухинин, Цифровая обработка аэрокосмических изображений, Красноярск (2008).

[5] Малджански Пл., Фотограметрични технологии, лекционен курс, София (2017).

[6] Хасан, С., Ниязи-Юсуф, М., Източници на йонизиращи лъчения, Сборник доклади от Международна научна конференция „Радиационната безопасност в съвременния свят“, Велико Търново (2023).

[7] Niyazi-Yusuf, M., Inaccuracies in area objects transferred from the map of the restored property to the cadastral map, Journal scientific and applied research, Volume 23. Konstantin Preslavsky University Press, Shumen (2022).

# LOCATION SELECTION METHOD FOR THE INITIAL POINTS OF HORIZONTAL BRIDGE GEODETIC NETWORKS

**ANI A. STEFANOVA**

***ABSTRACT:*** *The article analyzes and evaluates the classical schemes and methods for designing horizontal bridge geodetic networks. A location selection method has been developed for the initial points of horizontal networks, aiming to provide the possibility to apply direct setting out methods via linear-angular measurements. Alternative methods for setting out the bridge piers are proposed.*

***KEYWORDS:*** *horizontal bridge geodetic networks, initial points, setting out methods, linear-angular measurements, bridge piers*

***DOI: https://doi.org/10.46687/MOIB2093***

## 1 Introduction

Bridge engineering-geodetic networks are a set of geodetic points with certain plan coordinates and heights usually located along the banks of the overcoming water obstacle or along the facility if the obstacle presents a dry valley.

Their purpose is to serve as a basis for horizontal and vertical survey, for the design and setting out of bridges and related facilities. They are used as grounds for making various control measurements during construction as well as for creating an executive survey and defining the bridge deformations.

From a thorough review of the specialized literature related to geodetic networks in bridge construction [1], [4], [6], [7], [8], it was found that there is a lack of specific recommendations regarding the design of the initial points necessary for setting out bridges with a length of over 500m, as well as a methodology for determining the locations of these points. For this reason, one of the main tasks of the author's research is the development of a method for determining the locations of the initial points as a function of the geometric parameters of the bridge and the required accuracy of setting out, with the output method of setting out – direct intersection.

## 2 Horizontal bridge geodetic networks

The shape and dimensions of horizontal bridge geodetic network are determined depending on the type and topographic features of the overcoming obstacle (dry valley or watercourse), the direction of the axis of the facility and the mutual location of the bridge piers. Specialized literature [1], [4], [6], [7], [8] recommends a number of schemes and methods for building horizontal networks, applied in the second half of the 20$^{th}$ century. Some of them are still used nowadays but they are implemented with modern technical tools, therefore they are the relevant topic in this article and serve as basis of the proposals for the design of horizontal bridge geodetic networks covered by the author further on.

### *Analysis and evaluation of classic schemes and methods for creating horizontal bridge geodetic networks*

When bridging dry valleys, mountain gorges, etc. with presence of multiple intermediate piers, the bridge network is constructed in the form of a chain of triangles and geodetic quadrilaterals covering the bridge piers so that it is possible to conduct setting out works from at least two, three and more setting out stations with the required accuracy (Figure1). This is the type

of bridge network developed for setting out the viaduct near the village of Yordankino, Bulgaria currently the village of Eleshnitsa (km. 6+900 away from Hemus highway).

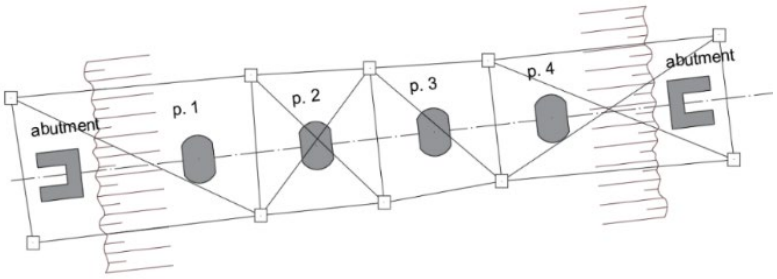



**Figure 1.** An example of a horizontal bridge network of triangles and geodetic quadrilaterals

In the bridge construction over dry valleys overcoming with a single span or in case of significant water currents, the specialized literature recommends the construction of networks of the type shown in Figure. 2 [7].

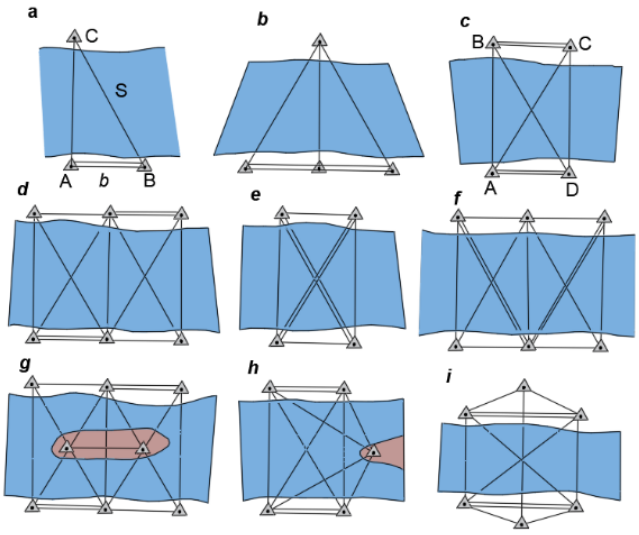



**Figure 2.** Schemes of horizontal bridge geodetic networks

In order to ensure a better network geometry, it is recommended [7] that the lengths of the short sides (located along the banks) must be chosen so that the angles in the network are not less than $30^g$.

When setting out bridges with a length of up to 200 m, it is suggested [7] that the network is built in the form of one triangle (Figure 2-a) while when constructing bridges with a length of 200-300 m - as two triangles (Figure 2-b). The bridge network is often built in the form of two geodetic quadrilaterals (Figure 2-d).

In the construction of bridges across wide water obstacles, part of the points of the bridge network should be located as close as possible to the places of the piers in order to create favorable conditions for their setting out with the required accuracy. For this purpose, the points are located on islands, if there are any or on piles located in the bridged water areas (Figure 2 – g, h, i).

Horizontal bridge networks can be constructed as angular (triangulation), longitudinal (trilateration), linear-angular networks, GNSS or a combination.

Until the mid-1970s, the bridge triangulation method was used as the main and only possible method for building horizontal networks (Figure 2). Generally, it is very labor-intensive because its peculiar high-precision angular and base measurements are carried out according to a special program during certain parts of the day and are strongly influenced by the atmospheric conditions, especially in cases of bridging large water obstacles.

With the advent of modern radio distance meter, triangulated networks have been replaced by linear and linear-angular constructions which is the so-called precise polygonometry, realized according to different schemes (Figure 4 and 5).

Linear-angular networks are most often constructed in the form of one or two geodetic quadrilaterals (Figure 3).

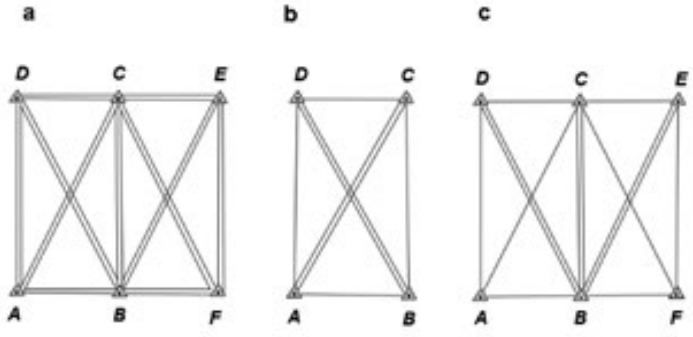



**Figure 3.** Linear-angular network schemes

If the surface of the area does not allow visibility between the points located along the coasts or the distances between them are too short, the linear-angular network can be built according to the scheme shown in Figure 4. In this case, measurements of directions between them are not provided since they are significantly less accurate than directions measured along the long sides.

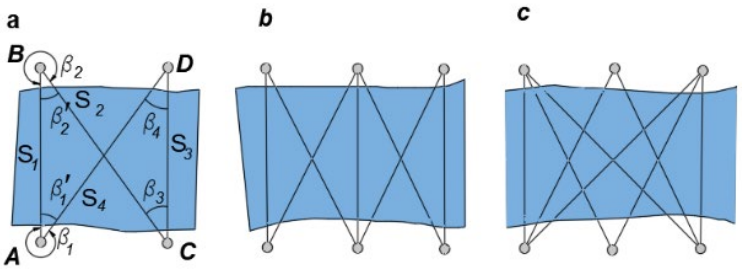



**Figure 4.** Linear-angular network schemes in case of lack of coast visibility

The method of precision polygonometry or the polygonometric method is used in the construction of the land piers and the shallow sections of the bridge transition. The simplest type of polygonal course is a rectilinear course that is laid directly along the axis of the bridge. These points can be stabilized near the locations of the pier construction (Figure 5).

Polygonometry is more convenient for setting out the supports where instead of a course made along the axis of the bridge, one or two more polygonometric courses are made (on the other side of the axis). The points of this polygonal course are materialized on the site of the additional tracing axis CD (Figure 5-a) or on two such axes CD and EF (Figure 5 - b and c) [7].

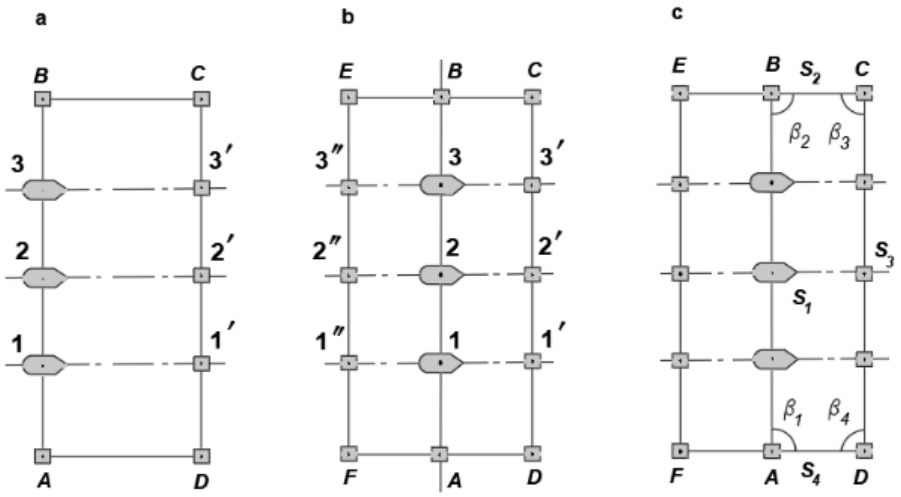



**Figure 5.** Bridge polygonometry schemes

Trilateration method (Figure 6) is less often used in the construction of horizontal bridge networks. However, there are cases in which the measurement of angles in the network is made difficult by the presence of fog alternating with strong refraction phenomena and measurements with radio distance meter, respectively trilateration constructions have been the only possible alternative for creating horizontal networks.

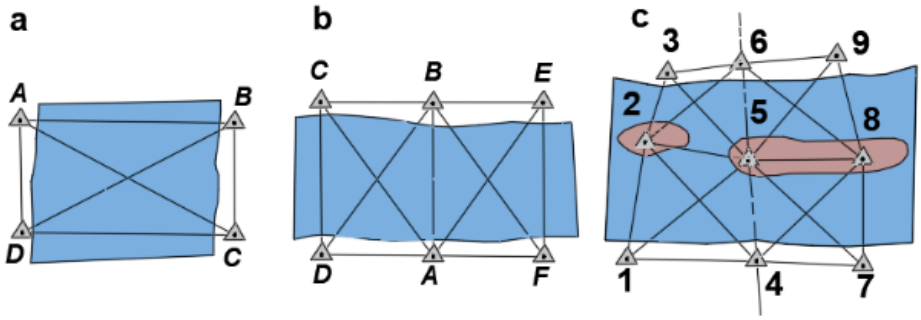



**Figure 6.** Trilateration schemes
a – geodetic quadrilateral; b- two geodetic quadrilaterals; c – quadrilaterals network

Despite the advent of highly accurate automated linear-angular measurement devices in the 1990s, the construction of high-precision linear-angular bridge networks is still labor intense and relatively slow as it involves waiting for suitable atmospheric conditions for angular measurements during the day and the involvement of significant support personnel.

With the development of GNSS technologies over the last 20 years, their use has significantly expanded in the field of engineering geodesy including bridge construction. Compared to classical linear-angular measurements, GNSS observations can be done during any time of the day without restrictions regarding the condition of the ground atmospheric layer and with significantly less burden on the observers. At the same time, the observations themselves are carried out by not highly-qualified operators. In this sense, GNSS as a means of creating engineering-geodetic networks is more promising and, in some cases – faster and cheaper in case that the required accuracy is ensured.

As seen in the statement above, the literature [1], [4], [6], [7], [8] lacks specific recommendations regarding the design of the initial points necessary for setting out non-class bridges as well as a methodology for location selection of these points. Therefore, one of the main tasks of the author's research is the development of a methodology for location selection of the initial points as a function of the required accuracy of setting out and the geometric parameters of the bridge with the output method of setting out - direct intersection.

# 3 Design of horizontal bridge geodetic networks when bridging wide water obstacles

The most important condition for the implementation of reliable horizontal geodetic assurance in bridge construction is the creation of a suitable network with a sufficient number of points appropriately located from the point of view of using practically all modern geodetic methods for setting out in plan. Therefore, when designing the network, it is necessary to take into account the following:

- the required setting out accuracy;
- the necessary accuracy in the point locations of the network;
- the bridge geometric parameters (facility length, span size, location of the piers and their height);
- providing the possibility to choose appropriate setting out methods and to determine their range (the maximum distance from the setting out station to the object been set out) while ensuring the required accuracy so as to provide setting out of the entire object.

Practically all known direct and indirect (reduction) setting out methods can be used in bridge construction. It is widely known that the direct methods which can achieve the required accuracy (direct right-angle intersection, linear intersection, polar method) are implemented using sufficiently accurate linear-angular measurements.

It is known that the precision in determining or setting out points using linear-angular measurements depends on the accuracy of the measured elements, the accuracy of the initial points and the mutual location of the newly determined and initial points (network geometry). In the specific case, this means that in order to achieve the accuracy of the coordinate determinations required in bridge construction, besides the use of precise tools, it is also necessary to create networks with a geometry suitable for using the direct or indirect setting out methods listed above.

***Method for designing the location of the initial points of horizontal bridge networks***

The author has developed a method for designing the locations of the initial points of horizontal networks which provides a suitable geometric shape, allowing direct setting out of the centers of bridge piers with the required accuracy using **linear-angular** measurements. Theoretical conclusions and settings are based on the formulas for evaluating the precision of a direct intersection. The developed method is described in detail in [9].

It is known that the accuracy in the position of a surveyed/set out point by the direct intersection method [1], [2], [3], [4], [5], [7] regardless of the errors of the initial points is determined by the following formulas:

$$M_P = \frac{m_\beta}{\rho}.\frac{b\sqrt{sin^2\,\beta_1+sin^2\,\beta_2}}{sin^2\,\gamma} = \frac{m_\beta}{\rho}.\Phi \tag{1}$$

$$M_P = \frac{m_\beta}{\rho}.\frac{\sqrt{S_{AP}^2+S_{BP}^2}}{sin\,\gamma} = \frac{m_\beta}{\rho}.\Phi, \tag{2}$$

where: $\beta_1$ и $\beta_2$ are the measured/set out angles at the given points; $\gamma=200-(\beta_1+\beta_2)$ – new point angle; $b$ – the distance between the given points; $S_{AP}$ and $S_{BP}$ – the lengths between the given and the new point; $m_\beta$ – mean squared error of measured/set out angle; $\Phi$ – geometrical factor.

It is obvious that the intersection accuracy is a function of the geometric factor $\Phi$ and the accuracy of the angular measurements. Research has established [6] that $\Phi$ has the smallest value if the triangle formed by the given and the new point is isosceles with a new point angle $\gamma=121.6200^g$.

Figure 7 shows an example of a part of horizontal bridge geodetic network where in order to simplify its geometry and the following conclusions, the value of the angle γ is assumed to be $100.0000^g$.

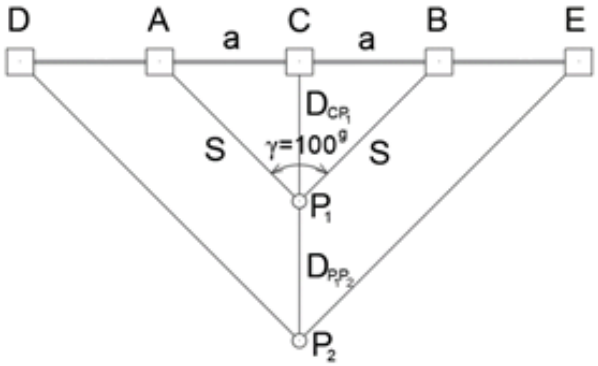



**Figure 7.** Part of horizontal bridge geodetic network

Point C of the above scheme is a point on the axis of the bridge (initial or final) where pt. $P_1$ and pt. $P_2$ are the centers of piers 1 and 2, with design intermediate distances $D_{CP1}$ and $D_{CP2}$, respectively. The locations of the network points (points A, B, D and E) are placed in a direction perpendicular to the axis of the bridge, assumed to be direct line in this case. Points A and B, designed as initial points for setting out the support $P_1$ are distant from pt. C where $S_{AC}=S_{CB}=a=D_{CP1}$ and points D and E (initial points for pt.$P_2$) where $S_{DC}=S_{CE}=S_{CP2}$.

It should be noted that designing a network with such assumed geometrical conditions is quite possible in practice due to the fact that in most cases the longitudinal axis of bridges is designed approximately perpendicular to the axis of the obstacle [6], [7], [8], respectively on the coastline.

Provided that $S_{AP_1} = S_{BP_1} = S$ and $\gamma=100^g$, from formulae (2) for geometrical factor $\Phi$:

$$\Phi = \left(\sqrt{S_{AP_1}^2 + S_{BP_1}^2}\right) / \sin\gamma = S\sqrt{2}. \quad (3)$$

Figure 7 shows that $S^2 = a^2 + D_{CP_1}^2$, considering that $D_{CP_1} = a$, after conversion it turns out that $S = a\sqrt{2}$. Hence, after substitution in (3) for the geometric factor $\Phi$, it turns out that $\Phi=2a$. Thus, obtained value for $\Phi$ after substitution in formula (2) for the setting out accuracy $M_P$ it follows that:

$$Mp = \frac{m_\beta \cdot 2a}{\rho} \quad (4)$$

From the above formulas, it follows that if a pier is to be set out distant from the starting or ending point of the bridge at a distance of, for example, 300m, then the distance between the initial

points should be 600m and the distance between the initial points and the point been set out - about 424m. At such large distances, problems can arise both in providing visibility between the initial points and in achieving the required angular setting out accuracy.

Therefore, network points along the banks of obstacles should be designed at smaller distances from each other so as to ensure the required setting out accuracy for all piers, including the most distant for a given angular setting out accuracy, achievable when measured in no more than one set of rounds.

Hence, the following task can be formulated:

To determine the locations of the initial points for direct point setting out (center of the bridge pier) using linear-angular measurements (bipolar intersection, straight-angle intersection), given the following output data:

- Allowable setting out error $M_P$
- Distance $D$ from the direction of the initial points to the one that have to be set out
- Allowable error of a setting out angle $m_\beta$ at measurement/setting out/ in one set of rounds.

The initial points are placed in a direction perpendicular to the axis of the bridge.

In fact, the solution of the problem comes to calculating the angle γ, hence the distance $S_{AB}$ = 2a (Figure 8) which helps to determine the locations of the initial points A and B.

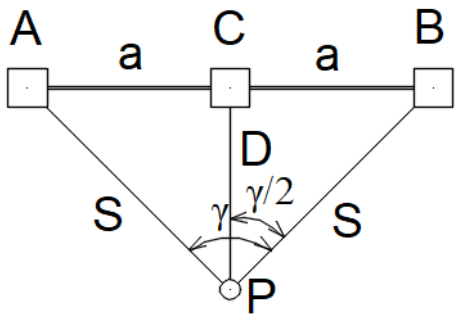



**Figure 8.** Part of horizontal bridge geodetic network

To derive the angle γ, it is based on formula (2) out of which the geometric factor $\Phi$ is expressed:

$$\Phi = \frac{Mp \cdot \rho}{m\beta} = \frac{\sqrt{S_{AP}^2 + S_{BP}^2}}{\sin\gamma} \tag{5}$$

Since in the case of Figure 8 it is seen that $S_{AP} = S_{BP} = S = D.sec(\gamma/2)$, the above formula is converted as follows:

$$\phi = \frac{M_p \cdot \rho}{m_\beta} = \frac{D \cdot sec\frac{\gamma}{2}\sqrt{2}}{\sin\gamma} \tag{6}$$

$$\text{or } \frac{Mp \cdot \rho}{m_\beta} = \frac{D\sqrt{2}}{\sin\gamma \cos\frac{\gamma}{2}}. \tag{7}$$

From formula (7), for the calculation of angle γ the following equation is obtained:

$$\sin\gamma \cos\frac{\gamma}{2} = \frac{m_\beta D\sqrt{2}}{M_P \cdot \rho} = c \tag{8}$$

$$\text{or } \sin\gamma \cos\frac{\gamma}{2} = c. \tag{9}$$

After some conversions, the above equation comes to solving a cubic equation. It can be solved with the so-called "Cardano's formula" but its use leads to complex numbers and in this sense its use for the purposes of the present task is unsuccessful. Therefore, a solution with real numbers is derived by Prof. Vladimir Todorov (University of Architecture, Civil Engineering and Geodesy, Section Mathematics) which is used here:

$$\gamma = 2\,arcsin\left(\frac{2}{\sqrt{3}}cos\left(\frac{1}{3}arccos\left(-\frac{3\sqrt{3}}{4}c\right)\right)\right). \quad (10)$$

Provided that: $\left|\frac{2}{\sqrt{3}}cos\left(\frac{1}{3}arccos\left(-\frac{3\sqrt{3}}{4}c\right)\right)\right| \leq 1$

and $\left|cos\left(\frac{1}{3}arccos\left(-\frac{3\sqrt{3}}{4}c\right)\right)\right| \leq \frac{\sqrt{3}}{2}$.

Using the determined angle γ, the distance is calculated $S_{AB} = 2a$ (Figure. 8):

$$S_{AB} = 2a = 2\sqrt{S^2 - D^2} = 2\sqrt{\frac{D^2}{cos^2\frac{\gamma}{2}} - D^2}. \quad (11)$$

Having in mind that pt. C (Figure 8) is known to us (a point from the axis of the bridge) and that the direction of the initial points is perpendicular to the axis of the bridge with the distance *"a"* derived by the above formula, the locations of the starting points A and B are determined.

Experimental calculations [9] prove that this method is also applicable in location selection of the initial points of horizontal networks when the bridge axis is rotated at an angle of obliquity of up to $50^g$ (Figure 9).

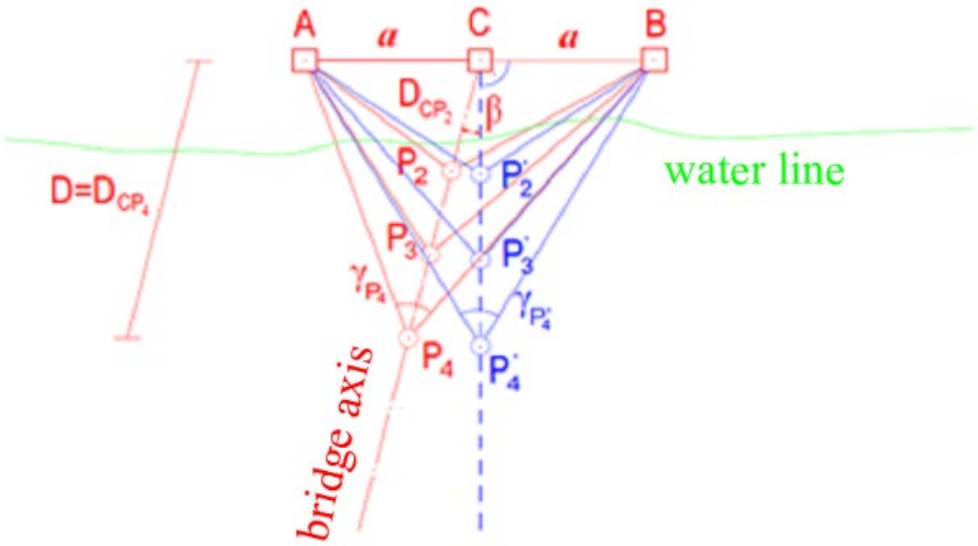



**Figure 9.** Horizontal networks with rotated bridge axis

## 4 Conclusion

The developed method for location selection of the initial points of horizontal bridge geodetic network provides a suitable geometric shape allowing direct setting out of the centers of bridge piers with the required accuracy using linear-angular measurements. This method proved to be also applicable for a bridge axis rotated at an angle of obliquity of up to 50g. The use of linear-angular measurements or their alternative GNSS observations is a matter of evaluation by the site geodesist given the specific conditions and time available. Considering this, it should be

taken into account that when using GNSS, the millimeter accuracy required in this case is achieved with observations in static mode lasting 2-3 hours. Therefore, in many cases it is more appropriate to set out the piers close to the abutments directly using linear-angular measurements.

**ЛИТЕРАТУРА:**

[1] Atanasov, S., L. Todorov, Geodesy 2. Technique. Sofia. 1991.

[2] Bakalov, P., V. Valchinov, R. Yaneva. Guideline for geodesy exercises. Techique. Sofia. 1991.

[3] Baran, P. I., V. I. Mickevich, Y. V. Polishtuk, S. G. Radov. Application of geodetic intersections, their generalized schemes and methods of machine decisions. Nedra. Moscow. 1986.

[4] Bolshyakov, V.D., G.P. LEVCHUK. Reference manual for engineering and geodetic works. Nedra. Moscow. 1980.

[5] Viduev, N., P. Baran. Geodetic survey work. Nedra. Moscow. 1973.

[6] Dimitrov, A. Engineering geodesy. Technique. Sofia. 1989.

[7] Kougia V., V. Gruzinov, O. Malkovsky, V. Petrov. Geodetic works in bridge construction. Nedra. Moscow. 1986.

[8] Levchuk, G. P. Applied Geodesy. Geodetic works in surveys and construction of engineering structures. Nedra. Moscow. 1983.

[9] Stefanova, A., Geodetic assurance problems in bridge construction. University of Architecture, Civil Engineering and Geodesy. Dissertation. Sofia. 2019.

# PROGNOSTICATION OF TOTAL GYROSCOPE ERROR INCREASE IN GUIDING GYROSCOPES*

**ANDREY I. BOGDANOV, TEODORA D. PEEVA**

***ABSTRACT:*** *Total gyroscope error is a major criterion characterizing the state of gyroscopic measurement systems. The prediction of its increase allows to use an objective criterion for the prediction of the remaining lifetime of the instrument.*

***KEYWORDS:*** *gyroscope; vibration spectrum*

***DOI: https://doi.org/10.46687/HZDO9716***

# ПРОГНОЗИРАНЕ НАРАСТВАНЕТО НА СУМАРНАТА ГРЕШКА ПРИ ЖИРОСКОПИЧНИ ИЗМЕРВАТЕЛНИ СРЕДСТВА

**АНДРЕЙ И. БОГДАНОВ, ТЕОДОРА Д. ПЕЕВА**

***АБСТРАКТ:*** *Общата грешка на жироскопа е основен критерий, характеризиращ състоянието на жироскопските измервателни системи. Прогнозирането на нейното нарастване позволява да се използва обективен критерии за прогнозиране на остатъчния ресурс на уреда.*

## 1 Въведение

Точността се явява един от основните критерий за оценка качеството на измервателните средства или информационно – измервателни системи, който определя съответствието между действителното и измереното значение на контролираните параметри. При жироскопичните измервателни средства проблем при определяне на сумарната грешка е това, че те са без скалови.

## 2 Изложение

При жироскопичните измервателни средства (ЖИС) точността се изразява в пропорционалност на изходния сигнал с ъгловото отклонение, което се преобразува от конкретното устройство. Отклонението от тази пропорционалност спрямо зададената в нормативно - техническата документация характеризира “неточността” или грешката на ЖИС. Тази грешка е следствие от множество външни и вътрешни причини пораждащи елементарни грешки, от действието на който се определя общата грешка на жироскопа.

Целта която си поставяме в настоящият доклад е да се прогнозира нарастването на сумарната грешка като функция на времето и да се определи с колко може да се удължи срока на техническа годност на уредите.

Така поставената цел изисква решаването на следните задачи:

1. Да се определи нарастването сумарната а грешка на жироскопа в целия диапазон на работа на уреда;

2. Да се определят апроксимационните функции за получените стойности на нарастване на сумарната грешка на жироскопа;

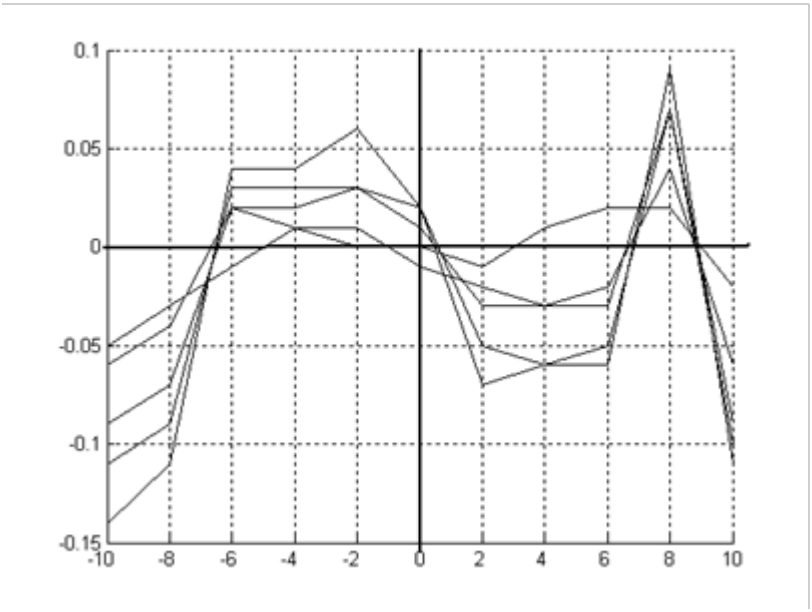
* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии“

3. Да се решат получените апроксимационни уравнения и прогнозиране възможността за удължаване срока за техническа годност на жироскопичните измервателни средства.

За да се определи нарастването на сумарната а грешка се измерва изходният сигнал при различни ъглови разсъгласувания в целия работен диапазон на уредите. Измерванията се извършват по схема и последователност описани в [1]. За получаване на многовариантност на решенията изследването се извършва с група от четири измервателни средства от един и същ тип.

За един от уредите нарастването на сумарната грешка при измервания извършвани през еди час работа на уреда в продължение на пет часа има вида показан на фиг.1

Съгласно [2] всяка техническа система има своя характерна крива на износване, като модела на това износване се избира като случаен процес, който има определена функционална връзка с времето, а техния стабилен характер се определя от параметри не зависещи от времето. За такива квазистационарни процеси най – разпространения модел на изследваните необратими изменения на параметрите има вида:




**Фиг. 1.** Нарастване на сумарната грешка при измерване през един час.

$$y_i(t) = \sum \alpha_{ij} \varphi_i(t) \qquad i = 0,1...n \qquad (1)$$

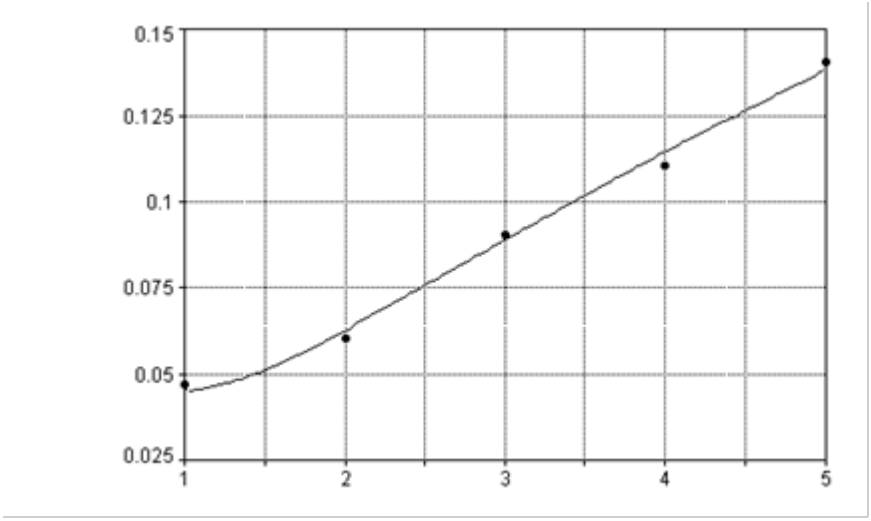
където $\alpha_{ij}$ е случайна величина;

$\{\varphi_i(t)\}_{i=0}^{m}$ - непрекъсната детерминирана функция на времето.

Това представяне може да се апроксимира, като за изследваните измервателни средства апроксимация на процесите на нарастване на грешките се представят чрез степенни, експоненциални или логаритмични функции на времето [3,4].

Графиките на нарастване на сумарната грешка при измерване в зададения интервал от време показват, че най – голяма е стойността на грешката в краищата на измервателния

обхват. Затова при извършване на апроксимацията се използват стойностите за –10 градуса. Апроксимационната крива за един от уредите има вида:




**Фиг. 2.** Апроксимация на резултатите от измерванията

Уравнението на получената крива има вида:

$$y = a + bt \qquad (2)$$

За оценката на коефициентите по метода на най – малките квадрати се получава:
$a = 0.035$; $b = 0.0626$.

Получените апроксимационни уравнения за останалите измервателни средства имат вида:

$$y = a + bt^{0.5} \qquad (3)$$

където: $a = 0.01582$; $b = 0.0481$.

$$y = a + b/t \qquad (4)$$

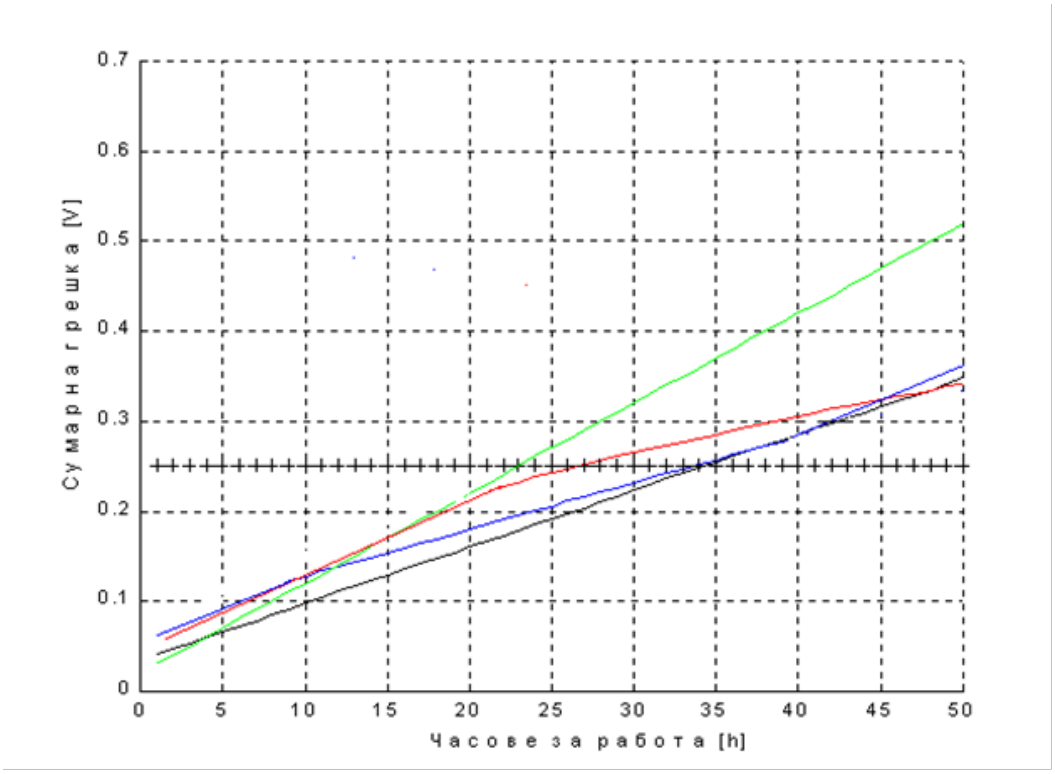
където: $a = 0.07641$; $b = 0.05163$.

$$y = a + bt \qquad (5)$$

където: $a = 0.02$; $b = 0.01$.

Решават се уравнения (2) до (5) при изменение на $t = 1...50$. Графичният вид на получените зависимости е представен на фигура (3):

За да се определи с колко може да се удължи срока на техническа годност на жироскопите за направление се определя след колко часа те биха достигнали максимално допустимата грешка която за изследваните уреди съгласно предписаното в техническата документация е 0.25V




**Фиг. 3.** Графичен вид на нарастването на сумарната грешка

## 3 Заключение

Представеният метод дава възможност за вземане на обосновано решение за удължаване срока за техническа годност на жироскопичните измервателни средства, като се използва обективен критерии какъвто е точността на измервателните средства. Използването на метода дава възможност да се прогнозира какъв е запасният ресурс на уредите.

**ЛИТЕРАТУРА:**

[1] Богданов А. И., Генов Б. Г., Метод за удължаване срока за техническа годност на жироскопични измервателни средства, Дефектоскопия 2002 – XVII Национална конференция по безразрушителен контрол с международно участие, Созопол 2002

[2] Силин В. Б., Заковряшин А. И., Автоматическое прогнозирование состояния аппаратуры управления и наблюдения, Энергия, Москва, 2013.

[3] Ригли У., Холистер У., Денхард У., Теория проектирование и испытания гироскопов, Мир, Москва, 2002.

[4] Абрамов О.В., Розенбаум А. Н., Прогнозирование состояния технических систем, Наука, Москва, 2009.

[5] Cota E. F., Negreiros M., Carro L., Lubaszewski M., A New Adaptive Analog Test and Diagnosis System. IEEE Instrumentation and Measurement. Vol. 49 №2 April 2000.

# ON RATIONAL DECISIONS IN THE CONTEXT OF INTRALOGISTICS*

**SVETLOZAR P. STOYANOV, ZHENYA P. GEORGIEVA, NIKOLAY H. YORDANOV**

***ABSTRACT:*** *The proposed statement assumes the conclusion that the satisfaction of a certain social need with a new technical object implies rational technical solutions, as well as the necessity of designing the interrelations between the participants in the creation and production of the products.*

***KEYWORDS:*** *intralogistics, rational technical solution*

***DOI: https://doi.org/10.46687/SMDS9678***

# ЗА РАЦИОНАЛНИТЕ РЕШЕНИЯ В КОНТЕКСТА НА ИНТРАЛОГИСТИКАТА

**СВЕТЛОЗАР П. СТОЯНОВ, ЖЕНЯ П. ГЕОРГИЕВА, НИКОЛАЙ Х. ЙОРДАНОВ**

***АБСТРАКТ:*** *Предложеното изложение допуска извода, че задоволяването на определена обществена потребност с нов технически обект предполага рационални технически решения, както необходимост от проектиране и на взаимовръзките между участниците в създаването и произвеждането на изделията.*

Обект на предложената тематика е задоволяването на определена обществена потребност с нов технически обект.

Предмет на разработката е рационалността на техническите решения.

Целта е представяне на резултата от развитието на инженерната наука, който предполага необходимостта от проектиране и на взаимовръзките между участниците в създаването и произвеждането на изделията.

Известно е, че интралогистиката се отнася систематично към вътрешнопроизводственото движение на материалните потоци и съответните процеси в производствените звена на индустриалното производствено предприятие. Има се предвид инженерният аспект на логистиката, а в тази посока и технологичният компонент на микросредата на ефективното логистично управление. Той представлява различните видове взаимодействие между суровини, незавършено производство и готовата продукция с машините и механизмите, като е главна логистична функция в производството [1, с. 16, с. 54 – 58; 7, с. 56, с. 57].

Следва да се отбележи, че именно частта от логистиката, свързана с проучването, проектирането, развитието, производството и приемането на материали се отнася към т.нар. производствена логистика. С нея е свързана инженерната логистика, която е направление, занимаващо се с управлението на процеса по осигуряване на ефективна подкрепа на индустриалните продукти през целия им жизнен цикъл [2, с. 15; 10, с. 12 (Бел. 2); 14].

В посока на казаното излизането наяве на технически обект, отличаващ се със свои специфични особености, се диктува от потребността за удовлетворяване на фиксирана социална необходимост, при регистриране и на още различни условия: дава се сметка за актуалното положение на технологията и организацията на производството; употреба на

* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии“

материали, съобразени с възможностите на по-голяма част от група хора; намаляване на разноските за производство; изделието да е екологично, а също и производството му. Възможно е формулирането и на още условия по отношение на отскорошно възприетият обект, като количеството и техният порядък на тежест, поставят в зависимост активните стремежи на конструктора с цел задоволяването им. В тази посока е необходимо пояснението за контроверсност на определени предпоставки, принуждавайки конструктора взетите от него решения да са резултат от изследване на съществено количество основни обстоятелства. По тази причина в инженерната практика в замяна на оптимално, дискусията е за рационално техническо решение, което се отличава с овеществяване и реален вид на концепцията. Такива решения са свързани с показатели за качеството и критерии, осигуряващи възможност на показателите да се даде оценка. По същество претенциите по отношение на техническите обекти имат възможност за трансформация в критерии за оценка на осъществимостта им [5, с. 7, с. 246 (Табл. 9.3) – 247 (Табл. 9.3 – продължение)].

Във всяка целенасочена човешка дейност на изследователите се налага да разглеждат множество варианти и да взимат определени решения. Изборът на най-доброто решение в определен смисъл е свързан с процес на търсене. Задачата за търсене на най-доброто решение се поставя както при изследване на съществуващите технологични обекти, така и в стадия на тяхното проектиране. Създаването на нови, по-евтини и по-надеждни технически системи, от една страна, и повишаването на ефективността и качеството на функционирането на съществуващите, от друга, днес е почти немислимо без организираните процеси на търсене на най-доброто решение, т.е. на оптимизацията. Това е целенасочена дейност за получаване на най-добър резултат в определен смисъл и при определени условия [3, с. 187; 11, с. 7; 12, с. 9].

От своя страна ефективността е вътрешна мярка за изпълнение, която дава представа доколко добре процесът преобразува входните ресурси в изходни. Колкото повече съотношението на изхода към входа се приближава до единица, толкова по-добра е ефективността на процеса. В тази посока измерването на ефективността се предопределя от наличието на няколко взаимодействащи си среди, т.е. физическа, икономическа и управленска, което дава основание да се оценяват следните видове ефективност:

- физическа ефективност – определя се като отношение между резултатите на изхода и входа, изразени в натурални измерители, а стремежът е тя да се доближава до единица за по-пълно оползотворяване на ресурсите, т.е.:

$$E_1 = \frac{O}{I} = \frac{P}{R} < 1 \tag{1}$$

където:

$E_1$ – физическа ефективност;

$O$ – изход;

$I$ – вход;

$P$ – продукт;

$R$ – ресурси;

- икономическа ефективност – това е отношение между стойностния израз на постигнатата полезност и стойността на употребените производствени ресурси, т.е. себестойността:

$$E_2 = \frac{U}{C} > 1 \tag{2}$$

където:

$E_2$ – икономическа ефективност;

$U$ – полезност;

$C$ – себестойност;

- обща ефективност – това е произведението от физическата ефективност и икономическата ефективност, т.е.:

$$E_3 = E_1.E_2 \quad (3)$$

където:

$E_3$ – обща ефективност;

$E_1$ – физическа ефективност;

$E_2$ – икономическа ефективност [13, с. 36 – 37].

Рационалните решения не зависят от миналия опит, като процесът на тяхното приемане включва избора на алтернатива, която ще донесе максимални ползи за организацията, т.е. има търсене на най-доброто решение. Следва да се отбележи, че рационалното решение се изгражда чрез избора на обективен аналитичен процес, а процедурата за вземане на такова решение включва седем последователни стъпки: идентифициране (определяне) на проблема; формулиране на ограничения и критерии за вземане на решения; идентифициране на алтернативи; оценка на алтернативите; избор на алтернатива или взимане на решение; изпълнение на решението или прилагане на решението; обратна връзка. Следните фактори влияят пряко върху процеса на вземане на решения и тяхната ефективност: лични оценки, ниво на риск, време и постоянно променяща се вътрешна и външна среда, информационни и поведенчески ограничения, негативни последствия и взаимосвързаност на решенията [4, с. 65 – 72; 9, с. 80].

Именно рационалността на техническото решение е базис за потребността от усъвършенстване на конструкцията на техническия обект, което е възможно за обосноваване измежду следните ракурси: промяна в условията на обществената поръчка; подновено подреждане на потребностите, предопределено от променящата се околна среда; предизвикателно изтъкване на преден план на индивидуални претенции с намерение за удовлетворяване на консуматорски дирения. В посока на казаното по квалификационен признак обликът на обектите може да бъде: според вида на обекта – изделие, процес; според съдържанието на обекта – сглобена единица, детайл, комплекс, комплект; според необходимостта от проектиране – оригинално изделие, покупно изделие; според предназначението – изделие-елементна база, комбинаторно изделие [5, с. 7, с. 8 (Табл. 1.1)].

Явен е стремежът на съвкупността от хора, които са обединени от производствени отношения, да удовлетворява личните си потребности, трансформиращи се от въздействието на значителен брой причини. При все това е факт потребността от производство, което непременно съдържа технология и технически средства. В посока на казаното, човекът който купува е заинтересован от цената на изделието и качеството му. Тук търсенето е на допустимата минимална цена за допустимото максимално качество. От друга страна капиталовложителят проявява интерес към разноските, качеството, времето за излизане на изделието на пазара и печалбата. Тук ракурсът е най-малко разходи, най-високо качество, най-малко време, най-голяма печалба. Независимо от всичко, проектантът следва да обмисли различните претенции, като има предвид, че стремежът му е да проектира изделие с такова качество, което да бъде най-високо за посочената цена. В направление на

казаното отделен способ за надмогване на конкуренцията е откриването и осъществяването на нови тенденции в разработвания технически обект. Поради това съществено в проектния процес е дирене на вариации по време на стадиите му. Именно в допира със съществуващите разновидности на решение следва на основание на уточнени критерии да се извърши избор на най-добрата такава, т.е. на рационално решение [5, с. 14; 6, с. 10].

През периода на началния растеж на хората индивидът сам е изработвал и технологията, и техническите средства за производство. Следва да се отбележи, че това в някои моменти е характерно и за нашето съвремие. Споменатото е осъществимо изключително при условие, че намерението е да се произведе определен предмет, резултат от човешката дейност, в единствена бройка, а по извънредност – в неголямо количество. При сегашната конюнктура се устройва производство на значителни количества, а това предполага събирането в едно цяло на активността на пространен набор от личности. Така се поставя в действие разделението на труда и специализацията както на инженера, така и на работника. Освен това различните дейности са с възможност за осъществяване на разни местонахождения. Именно с появата на разделението на труда се поражда и необходимостта от пътища за съобщения сред вземащите участие в процеса. На елементарно ниво информацията е образна, като недостигът на време и отсъствието на хартия предполагат нейното редуциране и рационалност до краен предел. Поражда се мисълта за представяне с линии и щрихи на конкретността на съобщителните средства, а тя плавно добива устойчива форма в автономна част от проектантската работа – инженерната графика. Това е съвкупност от методи за графично изобразяване на обектите на проектирането, т.е. изделията и процесите, а в тази връзка и документирането на техническите решения. Именно отличителните особености за създаване на изображения, начините за показване на претенциите към представените технически обекти, разчитането на техническа документация и др. доказват, че инженерната графика е език за комуникиране. В същността си е съдържателен в необходимата степен и прецизен в потребното количество, което му позволява да подаде на поредната съставна част от последователността *проектиране – производство – потребление* нужната съвкупност от данни, съставляващи съобщение. Тук информацията се пренася посредством техническата документация. Тя с оглед на това, че споменатите вече проектиране, производство и потребление неведнъж са разпръснати във времеви и пространствен аспект, следва в своята съдържимост да е коректна, т.е. съобразена с правилата, както ефективна и рационална. Посочените характеристики утвърждават техническото документиране като присъща инженерна дейност, която е неразделна част и от съвременното производство. Следва да се отбележи, че именно документирането на техническите решения ангажира значителен времеви компонент на инженерния състав, а отдаването на съществено грижливо отношение на тази работа несъмнено е резултат от първостепенността на техническата документация по отношение на жизнения цикъл на изделията. Предпоставка за нейната значимост е това, че включва в себе си пространна съвкупност от данни. Тази информация предоставя възможност за понятност както на определени технически решения, така и за организацията на производството, за устройствените отношения в техносферата, за това през какъв времеви интервал се извършва подобряване на резултата от производството и др. Значението на техническата документация се потвърждава в няколко аспекта, т.е. тя е свързващото звено сред стадиите на жизнения цикъл на изделията; точно определена е по съдържание и не допуска тълкувания; съхранява съвкупността от практически усвоени знания и умения; посредством нея се осъществява споделяне на комплекси от данни с хора,

които са се усъвършенствали в определена област; техническият прогрес е подбуждан и подтикван от нея [6, с. 10, с. 11; 8, с. 3].

С поглед в миналото от просперитета на съвкупността от хора, обединени от производствени отношения е видна необходимостта от разнообразни механични средства за задоволяване на съответните потребности. В практиката е възприето словосъчетанието *технически обекти*, а те първоначално следва да се планират и да са способни да изпълняват дадена дейност с определен резултат. Заедно с проектирането се поражда неизвестността за направата на техническите обекти. Това е знак, че на инженера му предстои да извърши и дейностите по съставяне на технологичния процес. В посока на казаното, а и вследствие от ръста на целесъобразната и съзнателна инженерна практическа работа, налице е категоричност, че осигуряването на ефективно производство предполага и проектиране на неговата организираност. Има се предвид, че освен изделията, процесите също са обекти на проектиране [6, с. 12 (Табл. 2.1) – 13].

От дълги години инженерният опит е установил от практиката необходимостта да се има предвид правата и обратната взаимозависимост сред отделните периоди от време в процеса по създаване, производство и експлоатация на технически обект. Именно в жизнения цикъл на изделията е възможно изследването на различната взаимообусловеност. В посока на казаното първостепенно съдържание за дейността на конструктора е съобразяването, в самото начало на творческия процес по разработваното изделие, с условията и различните ограничителни обстоятелства, пораждащи се от въздействието на различните етапи на жизнения цикъл над етапа *проектиране*:

- обществена потребност – посредством образуваното публично задание конструкторът бива натоварен с диренето на ясно определен набор от технически решения по начин, позволяващ реализиране на първоначалните условия;

- научни изследвания – продуктите от научните търсения намаляват сферата от възможни технически решения, с които конструкторът да разполага;

- производство – решенията по заданието установяват определен порядък от условия към производството – необходимо е да бъдат произведени съответните изделия и съставките им, съобразно предвидената технология и организация на производство;

- потребление – този етап от жизнения цикъл следва да приеме или да опровергае инженерните концепции и решения, посредством равнището на пазарно търсене на изделието [5, с. 9, с. 10 (Фиг. 1.1)].

Следва да се отбележи, че в масов план решенията в етапа *проектиране* поставят в зависимост експлоатационните разноски и тези по възстановяването на работата на изделието, т.е. има се предвид възстановяването му в изправност [5, с. 10].

Предложеното изложение допуска извода, че задоволяването на определена обществена потребност с нов технически обект предполага рационални технически решения, както необходимост от проектиране и на взаимовръзките между участниците в създаването и произвеждането на изделията.

**ЛИТЕРАТУРА:**

[1] Ангелов, Д., Желязкова, Д. Стопанска логистика. Учебно помагало. Варна, 2007, Издателство „Наука и икономика”, Икономически университет – Варна, Печатна база на ИУ – Варна.

[2] Ботев, Б., Генов, Г., Ботев, Св. Техническа логистика. Шумен, 2015, Университетско издателство „Епископ Константин Преславски”.

[3] Вучков, И., Стоянов, С. Математическо моделиране и оптимизация на технологични обекти. Първо издание. София, 1980, Държавно издателство „Техника", Държавна печатница „Тодор Димитров" – клон 1, София.

[4] Давидов, К. Управлението като теория породена от практиката. Шумен, 2020, Университетско издателство „Епископ Константин Преславски".

[5] Лепаров, М., Вичева, М., Георгиев, М. Основи на инженерното проектиране. Второ преработено издание. София, 2011, Издателство „Софттрейд".

[6] Лепаров, М., Оракалиев, Д. Техническо документиране (инженерна гледна точка). Пето преработено издание. София, 2002, Издателство „Софттрейд".

[7] Миротин, Л., Багинова, В., Федоров, Л. Эволюционные закономерности логистики. – Журнал „Мир транспорта", Том 15, №3, 2017, Москва, РУТ (МИИТ), 56 – 62.

[8] Михайлов, Х., Станева, Н., Белберов, М. Инженерна графика. София, 2005, Издателска къща при ЛТУ, СД „Лотус" ИС.

[9] Младенов, Ю., Терзиев, В. Основи на управлението. Първо издание. Русе, 2011, Издателство „Силоам прес".

[10] Раковска, М., Драгомиров, Н., Луканов, К. Бизнес логистика. София, 2018, Издателски комплекс – УНСС.

[11] Стоянов, С. Методи и алгоритми за оптимизация. Първо издание. София, 1990, Държавно издателство „Техника", Държавна печатница „В. Александров" – Враца.

[12] Стоянов, С. Оптимизация на технологични процеси. Първо издание. София, 1993, Издателство „Техника", Държавна печатница „Полиграфюг" – Хасково.

[13] Nedyalkov, A. Process effectiveness or process efficiency: which indicator is more important for organizations? – Proceedings of University of Ruse – 2020, volume 59, book 5.1, Economics and management, Ruse (Bulgaria, BG), 2020, Publishing house University of Ruse „Angel Kanchev", 32 – 39.

[14] „Welcome to SOLE". – Sole.org, Laurel (Maryland, USA), SOLE – The International Society of Logistics, <http://www.sole.org/>, 09.06.2021.

# APPLICATION OF MODERN TEHNOLOGIES IN AGRICULTURAL PRODUCTION SYSTEMS*

**PETYA K. VELCHEVA-TODOROVA**

***ABSTRACT:*** *Precision agriculture plays a key role in the development of any farming production systems. It is an opportunity to realize good economic results and a prerequisite for achieving ecological regional development. It is of great importance to know the possibilities of new technologies for application in the cultivation of agricultural crops and their protection.*

***KEYWORDS:*** *precision agriculture, farming system, optical sensors, software systems for monitoring, economy*

***DOI: https://doi.org/10.46687/FITL3623***

# ПРИЛОЖЕНИЕ НА СЪВРЕМЕННИТЕ ТЕХНОЛОГИИ В ЗЕМЕДЕЛСКИ ПРОИЗВОДСТВЕНИ СИСТЕМИ

**ПЕТЯ К. ВЕЛЧЕВА-ТОДОРОВА**

***АБСТРАКТ:*** *Прецизното земеделие играе ключова роля в развитието на всяка земеделска производствена система. Това е възможност за реализиране на добри икономически резултати и предпоставка за постигане на екологично регионално развитие. От голямо значение е познаването на възможностите на новите технологии за приложение при отглеждането на земеделски култури и тяхната защита.*

В основата на прецизното земеделие е спестяването на горива за машините, сеитбен материал, вода и препарати, въобще спестяването на всички разходвани ресурси и материали, което се получава, ако не се допуска припокриване на обработваните площи. Поливането, прилагането на торове и препарати за растителна защита, сеитбата, обработката на почвата, прибирането на продукцията и въобще всички необходими за отглеждането на реколтата дейности в прецизното земеделие, можем да проследим и контролираме чрез системи за управление на оборудването и машините. [4]

За да извършим качествено скрининговане на площите не трябва да допускаме и другата крайност – изпускане на части от терена, които да не бъдат обработени с някоя от нужните процедури. Това можем да постигнем със системи за управление и на използвания инвентар /хардуеър/. Те съдържат лесни за инсталиране върху машините контролери, съвместими с работата на GPS-приемниците и дисплей, на който се показва картографирана информация от извършваната операция, позволявайки ни автоматичен контрол на няколко секции, като избегнем пропуски или застъпвания.

GPS-приемниците дават информация за навигацията на машината и за нейната скорост. Така знаем кои са обработените площи, а според скоростта автоматично регулираме налягането на разпръскване на препарата. По този начин постигаме максимална прецизност и улесняване работата на оператора, като едновременно се отчитат икономически и екологични ползи.

* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии“

Има много видове инвентар, който е конструиран така, че да е в удобство и услуга на земеделските производители. Под каквато и форма да бъдат решени – приемниците и контролерите не могат да бъдат ефективни и не биха могли да извършат необходимите изчисления без наличието на сензори от различен тип и вид.

Най – често използваните сензори са ***бордовите сензори***, които се прикачат към земеделската техника и образуват мрежа, която събира данни в реално време и обработват информацоията за бъдещо използване. Чрез тях отчитаме евентуална нужда от конкретни операции или обработки на полетата.

Най-новите варианти на ***ултразвукови и оптични сензори***, поставени върху подходяща част от трактора, комбайна, сеялката или пръскащата машина, проследяват движението и засичат разстояние до редовете, до растенията, наклон, количество реколта, проследяване на плевели и т.н. Прилагането им ни позволява свързване с GPS и управление чрез автопилот, при което операциите се извършват с точност до 2см.[1] Чрез дисплея в кабината операторът избира схемата на навигация и наблюдава движението на екрана. Информацията от сензорите, гарантира работа без допускане на грешки, като така спестяваме труд и време, а също така е възможен непрекъснат 24-часов цикъл на работа, при необходимост от спазване на кратки срокове.

Следващата необходимост, за да пресметнем коректната информация от сензорите и извършим всички изчисления на получените данни от полето, е наличието на софтуерни системи. С тях се оперираме при планиране на сезонни и извънредни дейности, необходими за обработването на терените. В зависимост от естеството на земеделските дейности, които трябва да направим, имаме нужда от софтуерни системи както стационарни, така и бордови, използвани директно на полето.

Разнообразните софтуерни системи за прецизно земеделие включват варианти за офиса, за мобилни устройства и за безжични комуникации. Стационарните софтуерни системи поддържат системата за управление на събраните данни от обработваемите площи и дават възможност различните атрибутни данни с пространствена определеност (т.е. геокодирани) да се съхраняват в отделни слоеве, които могат да се възпроизведат в карта един върху друг.[1,2] Отделните слоеве могат да представляват информация за използваните сортове семена в различни парцели, която се свързва с данните от добива; да показват почвеното съдържание, въз основа на което се изготвят карти за торене и поливане; да показват количествата добиви или друга важна информация, която се използва за анализ от системата за управление на решенията. [3] Специализираните в сферата софтуерни системи автоматично могат да калкулират даже и стойността на продукцията, както и да правят отчети за доходите, баланс и други финансови отчети.

Софтуерът за преносими устройства и безжични комуникации се отличава с лесен за разбиране и боравене интерфейс. С програмите се борави чрез смартфон, таблет, преносим компютър или модем, дисплей и бордови компютър в кабината на трактора, комбайна или друг вид селскостопанска техника. Тези устройства имат вградени GPS-приемници и позволяват позициониране, картиране и получаване на данни чрез безжична връзка, която ни предлага събиране на данни в реално време от смартфон или от машините, които се движат в полето. Тази информация може лесно да се прегледа, редактира и анализира, така че да ни помогне във вземането на решения, независимо къде се намираме. Освен това програмите позволяват бързо синхронизиране на информацията събрана от полето с тази в стационарните компютри.[5]

Освен чисто механичното обработване на полетата, като оран, сеитба и събиране напродукцията, се явява и нуждата от следене на колиеството влага необходима за

здравословното отглежане на културите. Нито една съвременна ферма не може да пренебрегне модерните технологии за управление на пръскачките.

Използвайки безжични технологии, извършваме превключване на секциите и дюзите, с цел да се пръска само там където е необходимо и в нужните количества, като избягваме припокриването и излизането извън границите на насажденията. Това естествено води до пестене на ресурси, по-качествена реколта и щадене на природата. Пример за иновативна концепция за GPS управление на секциите на пръскачките е софтуерния продукт SECTION-Control TOP. Чрез него става възможно превключването не само на секциите като цяло, но и на всяка една дюза на пръскачките поотделно. Управляващите контролери могат да бъдат електрически или пневматични. Едни контролер може да управлява до четири единични дюзи. Включени към универсалните ISO Bus терминали на Mueller-Elektronik например, те могат да управляват до 210 модула. Това отговаря на работна дължина от 52.2m, при разстояние между пръскащите дюзи от 25cm.

Системата ***Connected Farm*** предлага множество възможности за управление на информацията за полето и автопарка, работейки с различни марки машини позволява да се конфигурира според конкретните нужди и осигурява постоянен on-line достъп до информацията. Функциите, свързани с работата на полето, обхващат очертаване и картиране, обмен на данни между машините, между машините и офиса, а най-новите възможности включват NDVI (*normalized difference vegetation index)* записи. Практически ***Connected Farm*** ни позволява управление на стопанството от всеки интернет браузър, като данни могат да се събират, както чрез смартфона на земеделеца чрез мобилно приложение, така и от навигацията в земеделската техника. Модемът DCM-300 например, е необходим, за да може информацията в реално време да се синхронизира с акаунта и да бъде видима от всяка една точка на света през онлайн портала. [7,8,9]

В системата се влиза с акаунт, даващ достъп за преглед, редактиране и принтиране на цялата информация, необходима за взимането на правилните решения. Налична е например информация за движението на машините в реално време, информация за състоянието на двигателите, за границите на полето и данните за парцела. За да заработи безжичната система е необходимо в офиса си земеделеца да има инсталиран Farm Works софтуер на компютъра, който се използва за събиране на информация и акаунт за Connected Farm. На самите машини е необходимо да е монтиран дисплей за навигация Trimble от моделите CFX-750 или FmX, придружен от модем DCM-300, както и включени функции Vehicle Sync и Office Sync, за различните опции за работа. За работа на полето могат да се използват полеви компютри Trimble Juno и Nomad, таблет Trimble Yuma и смартфон с инсталирано приложение Connected Farm.

Connected Farm може да следи местоположението на машините в реално време, като така ни позволява оптимизиране на разходите за гориво, намаляване на грешките при обработката, както и предотвратяването на кражби. По отношение на автомобилния парк, Connected Farm следи положението и води записи за движението на машините, извежда съобщения на таблото за управление, а най-новите функции позволяват дистанционен контрол и генериране на отчети за извършената от машините работа. Допълнително системата запазва историята на позициите на всяка една машина и може бързо може да се определи, къде се е намирала тя в даден времеви период. Системата може да регистрира и записва продуктивността на машините, като включва времето на движение и покой. В комбинация с дисплей ни позволява да отбелязваме и да следим причините за отклонения при предварително зададен период на движение или покой, като така не е необходимо

операторът да напуска кабината, което води и до пестене на време и по-висока ефективност.[7]

Освен всичко друг, Connected Farm повишава и сигурността, чрез създаване на виртуални гео-зони и зони за алармиране. При излизане на машина извън предварително дефинираните часове или зони, системата изпраща SMS до мениджъра, като по този начин предотвратява неоторизирано използване или кражби.

При работа на полето **Connected Farm** използва безжична връзка за трансфер на данни и елиминира нуждата от USB устройства. Операторите в едно и също поле могат да обменят информация помежду си, да минимизират презастъпването и прекомерният разход на материали. Всяка една от машините има възможност за бърз обмен на информация с офиса на линии за навигация, дренажен дизайн, карти с предписание, карти с добива, и други, което води до по-добро управление на стопанството. Използвайки виртуално табло с показателите от кабината, за наблюдение разхода на гориво, заряда на акумулатора, наляганeто на маслото, температурата и други параметри, можем да направим анализ на производителността, който да служи да повишаване на продуктивността, ефективността и вземане на решения. Това е възможно благодарение на една от най-новите функционалности на приложението за таблети и смартфони на Connected Farm – въвеждане на NDVI (Normalized Difference Vegetation Index) записи, направени с ръчния сензор GreenSeeker. По този начин калкулираме количество азот например, необходимо за растенията, като тези данни също могат да бъдат запазвани и преглеждани онлайн след време при необходимост.

Възможностите за работа с приложението Connected Farm App са много. Безплатното мобилното приложение ни дава възможност да събираме и прехвърляме данни към офиса, чрез използване само на един мобилен телефон. Бидейки съвместим с всички модели iPhone и смартфони с Android, софтуерът използва вградения в телефона GPS за събиране данни от терена, които в последствие се синхронизират с наличният ConnectedFarm. По този начин е възможно да се очертават граници на имоти, да се добавя информация или снимки към различни точки от полето или да се опишат евентуални проблеми, които се наблюдават, например плевели, инсекти или други. Примери за патентовани комбинации от хардуерни и софтуерни решения за дистанционен мониторинг на различни насекоми-вредители по растителните култури са Trapview и iTRAP на SCIENTACT, представляващ лек интегриран електронен уред с лепкава плоча, който може да бъде закачен навсякъде. На полето, уреда е напълно автономен, захранван от соларен панел и батерия. Множество камери правят снимки с висока резолюция на лепкавата плоча в капана, след това снимките се изпращат през GPRS до Trapview интернет платформата, където биват анализирани автоматично за идентифициране на вредителите, а резултатите са достъпни през интернет или мобилно устройство. Контролът е в реално време и събраните данни могат да бъдат използвани за по-нататъшно разработване. [10]

Следенето на полевите данни и управлението на много капани за мониторинг може да бъде доста голямо предизвикателство. При използването на класически средства, то може да доведе до значителен процент на грешки и лошо прецизиране на решенията. Затова е нужно да използваме специализиран софтуер и хардуер като може да събираме и отчитаме събраната информация за различни периоди, но практиката доказва, че е най-оптимално ежедневното наблюдение на полетата. Използването на „умни" датчици и системи за управление на процесите на полето ни намалява и необходимостта от физическите посещенията на полетата. За да преброим уловените вредители, обикновените капани трябва да бъдат посетени на място, което означава загуба на доста време и гориво само за

събиране на информацията от овощната градина или полето. Много пъти посещенията на място са напразни (вредителите още не са се появили, или има празнина между поколенията им).

Разпознаването и отчитането на вредители на място отнема време и е изморително. С iTRAP, снимките се съхраняват на сървъра, изображенията се обработват автоматично и винаги могат да бъдат проверени от съответните експерти. Обработвайки изображенията, системата генерира автоматично известия. Аларми възникват когато се появят вредители и системата е намерила решение за тяхното премахване или е налице значително увеличение на уловените индивиди и лепкавата плоча е пълна и трябва да се подмени. В много страни има строги правила по отношение на записите, доказващи отсъствието на вредни насекоми, пътуващи с плодовете или зеленчуците. Използването iTrap може да помогне на износителите да предоставят тези доказателства и документи по автоматичен начин и в обективен вид, без допълнителни разходи.

Комбинацията с на съвременните технологии с местни метеорологични данни позволява по-прецизно вземане на решения за конкретните случаи. Използването на метеорологични станции пасва идеално за автоматично определяне на дневната и часовата степен на риск от полети на насекоми или тяхното размножаване.

Друг пример за използването на съвременните възможности на технологиите е CropSpec – интегриран сензор на Topcon Precision Agriculture, отчитащ азотното съдържание на растенията по време на движение. Работейки с ядрото от експерти на Topcon в областта на оптиката и в сътрудничество с Yara International (световен лидер в производството на азотни торове), Topcon инженерите създават CropSpec (Фиг.1) като мощен всеобхватен сензор. Topcon системата използва комбинация от два сензора (в лявата и дясната страна на кабината), които позволяват на фермера да наблюдава параметрите на растенията и да тори само при нужда.




**Фиг. 1.** Topcon CropSpec

Информацията може да се анализира за да се определят частите от полето, които имат нужда от третиране. Възможно е начертаването на прецизни карти за по-късна обработка или на момента да се предостави приложение, което позволява в реално време да се изпълняват променливи норми.[9]

CropSpec позволява на фермерите да анализират в реално време нуждите на посева и да обработят полето на момента. С други думи, приложения с променлива норма на торене се изпълняват по същото време, в което се вземат и показанията за азотно съдържание и тези апликации са базирани на нуждата на полето.

Наблюдателният метод е безконтактен, безвреден и предоставя последователни повторяеми отчитания, позволявайки сравнение на данни както от седмица на седмица, така и от година на година.

CropSpec се характеризира с два основни режима на работа: режим за четене/запис и напълно автоматичен режим, даващ на оператора голям избор относно как приложението за променлива норма да реагира на данните от сензора. Други преимущества на системата CropSpec са сензор работещ на по-голяма дистанция (2-4 метра) и по-голям обзор, който покрива повече площ на едно минаване.

Вместо да разглеждаме растенията вертикално отгоре, наклонения изглед от CropSpec сензора, в комбинация с големия обзор позволява по-точни измервания в редовите култури на по-ранни етапи на растеж. CropSpec позволява на фермерите да работят през деня и нощта с лекота и гъвкавост ненадминатата от всяка друга технология. Компактната система се монтира на покрива на трактора, далеч от работната зона, като се предотвратява възможността от повреждане на сензора докато машината работи в полето.

Възвръщаемостта на инвестициите за CropSpec е изключителна. Възможно е инвестицията за техниката да се изплати за един работен сезон от икономии в разходите за торове, и това съчетано с ползите от осигуреното точно количество торове, в нужните области на обработваните полета.

**ЛИТЕРАТУРА:**

[1] Minchev, M., "Fundamentals of GPS application in geodesy", Sofia, 2013;

[2] Mihailov, R., "Precision Agriculture", Lecture Notes, ed. TU – Varna, ISBN 978-954-20-0792-0, 2019;

[3] Mihailov, R., Researching problems in agriculture with the means of technology and digital technologies: monograph, TU - Varna, 2021, ISBN - 978-954-20-0827-9

[4] Nikolov D., Iv. Boevski, P. Borisov, M. Atanasova-Chopeva, Kr. Kostenarov, Ev. Petkov, B. Fidanska, "DIGITALIZATION IN AGRICULTURE - COMPETITIVENESS AND BUSINESS MODELS", 2022 Institute of Agrarian Economics, publisher ISBN 978-954-8612-40-1

[5] Tsvetkov, V., "Drone sprayer", Student Scientific Session '17, Ruse, pp. 113-116, 2017

[6] Tsvetkov, Il., "Investigation of the applicability of a telemetric system for testing agricultural machinery", Author's abstract of a dissertation for the acquisition of the ONS "doctor" in the specialty "Mechanization and electrification of crop production", 2010;

[7] https://cap.europe.bg, "Techniques and Practices in Precision Agriculture: From Considerations to Applications" series, accessed 03/01/2024.

[8] https://agri.bg/novini/nik-predstavya-inovativnata-tehnologiya-connected-farm-na-agra-2012-2

[9] https://www.topconpositioning.com/solutions/technology/agriculture-products/implement-controllers-and-sensors

[10] https://agrobio.elmedia.net/bg/2013-1/editorials/%D0%BF%D1%80%D0%B5%D1%86%D0%B8%D0%B7%D0%BD%D0%BE-%D0%B7%D0%B5%D0%BC%D0%B5%D0%B4%D0%B5%D0%BB%D0%B8%D0%B5_00029.html

# THE ROLE OF WIRELESS COMMUNICATIONS IN THE MANAGEMENT OF ACTIVITIES IN AGRICULTURAL PRODUCTION SYSTEMS*

**PETYA K. VELCHEVA-TODOROVA**

***ABSTRACT:*** *The rapid growth of the global population increases the need for food for the survival of mankind. Meeting this need with the planet's limited resources is a major challenge. To deal with it by increasing productivity, farmers are implementing many modern technologies, mostly based on wireless communications.*

***KEYWORDS:*** *wireless communications, monitoring platforms, precision agriculture, farming system, software systems, optical sensors*

***DOI: https://doi.org/10.46687/WYSR7895***

# РОЛЯТА НА БЕЗЖИЧНИТЕ КОМУНИКАЦИИ В УПРАВЛЕНИЕТО НА ДЕЙНОСТИТЕ В ЗЕМЕДЕЛСКИТЕ ПРОИЗВОДСТВЕНИ СИСТЕМИ

**ПЕТЯ К. ВЕЛЧЕВА-ТОДОРОВА**

***АБСТРАКТ:*** *Бързият растеж на глобалното население увеличава нуждите от храна за оцеляването на човечеството. Задоволяването на тази потребност с ограничените ресурси на планетата е голямо предизвикателство. За да се справят с него като повишават производителността, земеделските производители внедряват много съвременни технологии, базирани най-често на безжичните комуникации.*

Прецизното земеделие се състои от техники за близко и дистанционно наблюдение, използващи сензори от типа IoT - „Интернет на нещата", които помагат да се следи състоянието и различните нива на растежа на културите събирайки и обработвайки голямо количество данни, свързани със състоянието на културите. Множество параметри, като ниво на водата, температура и т.н., определят здравето на растенията. Следенето им ни дава възможност да изберем точно кои параметри да наблюдаваме и какви стойности да поддържаме, за отглеждането на здрави култури в даден момент, къде има нужда от корекции и в какви количества. За тази цел е нужна много информация от различни източници и от различни части на полето, като например за хранителните вещества в почвата, наличието на вредители и плевели, съдържанието на хлорофил в растенията, метеорологичните условия и др.

Цялата събрана информация се анализира, за да приложим правилните агрономически действия при отчитането на проблеми с отглеждането на посевите или поддържането на полето. Например, като вземем предвид етапа на развитие на растенията и съдържанието на хлорофил в тях, определяме хранителните вещества, необходими за отглеждането им. Тази информация се комбинира с характеристиките на почвата и с прогнозата за времето. По този начин тя се използва, за определим какво количество от определена тор трябва да приложим на следващия ден.

* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии"

Подходящата и навременна агрономическа информация за земеделския стопанин и прилагането на препоръките са ключови за повишаването на добивите. Основен двигател на прецизното земеделие са безжичните сензорни мрежи. Те представляват мрежа от множество безжични възли, свързани помежду си, за наблюдение на физическите параметри на околната среда. [1,2]

Всеки безжичен възел се състои от радиоприемник, микроконтролер, сензор/и, антена и други схеми, които му позволяват да осъществява комуникация с портала, предаващ данните от сензорите. Сензорите измерват физическите параметри и изпращат информацията на контролера, който я предава към облака или преносимото устройство. Селскостопанският сектор се нуждае от множество данни за почвата, естеството на културите, метеорологичните условия, видовете торове и нивата на вода. Те ще се различават за различните култури, отглеждани на една и съща почва и на едни и същи растения в различни почви и при различни метеорологични условия. Сензорите наблюдават поведението на тези параметри на културите. Благодарение на бързия напредък в технологиите на безжичните сензорни мрежи размерът и цените на сензорите намаляват, което направи възможно и прилагането им в много области на живота, включително в селското стопанство. Като цяло безжичните сензорни мрежи се състоят от един или повече безжични възела, свързани допълнително със сензори. Тези възли са малки устройства, които отговарят за събирането на данни. Възлите се разделят на два вида - възел източник, който събира данните и приемащ (или портален възел), който получава данни от възлите източници. Приемащият възел има по-голяма изчислителна мощност в сравнение с възела източник. При избора на безжични възли обаче има ограничения по отношение на енергията, паметта, мощността, размера и скоростта на предаване на данни, а също и на цената. Сред всички безжични възли MICA2 е смятан за по-подходящ в сравнение с останалите поради големия брой разширителни конектори, които го правят подходящ за свързването с няколко сензора.

През последното десетилетие са предложени много приложения за дистанционно наблюдение на здравето на културите, използващи безжични сензорни мрежи. Кибер-физичните системи могат да се опишат като интелигентни системи, състоящи се от софтуерни, хардуерни и физически компоненти, интегрирани с цел да улавят променящите се състояния на реалния свят. Трислойната система се състои от физически слой, в който се събират всички сензорни данни; мрежови слой, от който данните се предават към облака; третият е слоят за вземане на решения, в който данните се анализират и обработват. Основният принос е генерираната технологична таксономия за управление на земеделските дейности, която се ръководи от архитектура, основана на Интернет на нещата за наблюдение на здравето на културите. [4]

Системата работи двумодулно – първият модул е за мониторинг на здравето на културите, основан на безжична сензорна мрежа, който използва множество сензори за получаване на информация за състоянието на културите в реално време, а другият модул се използва за данни за нормализиран разликов вегетационен индекс (NDVI), които се получават благодарение на спектрални изображения, заснети от дрон. Тези данни са необходими за оценка на съдържанието на хлорофил, който се използва за мониторинг на здравето на културите. С бързото нарастване на броя на устройствата за IoT (Интернет на вещите) и безжичните сензорни системи, през последните няколко десетилетия се въвеждат редица комуникационни протоколи. Всеки протокол има собствени спецификации в зависимост от широчината на честотната лента, броя на свободните канали, скоростта на предаване на данни, издръжливостта на батерията, цената и други фактори.

Клетъчната технология е най-подходяща за приложения, които изискват изключително висока скорост на предаване на данни. Тя използва възможностите на GSM, 3G- и 4G-клетъчната комуникация, като осигурява надеждна високоскоростна интернет връзка, изискваща по-висока консумация на електроенергия. Клетъчната технология изисква използването на инфраструктура, разходи за експлоатация и пространство за съхраняване на резервни данни с централизирано управление. 4G-клетъчната технология се нуждае от повече енергия от батерията, но е добър вариант при подземни безжични сензорни мрежи от рода на системи за сигурност в интелигентните домове и за приложения в селското стопанство. В интелигентните напоителни системи няколко сензора за влажност на почвата са разположени на полето в т.нар. ZigBee мрежа. Показанията се предават през облак като се използва клетъчна мрежа 4G LTE. [3]

**6LoWPAN** (IPv6 over Low-Power Wireless Personal Area Networks) е IP-базиран комуникационен протокол – първият, използван за комуникация в Интернет на нещата. Той е евтин поради малката широчина на честотната лента и ниската консумация на енергия. Поддържа множество топологии тип „звезда“ и мрежово управление. Примери за приложения на 6LoWPAN са мониторингът на оборудването в здравни заведения, наблюденията на околната среда, системите за сигурност в автоматизираните жилищни сгради. Безжичната 6LoWPAN сензорна мрежа може да бъде използвана за следене свойствата на почвата на земеделските култури.

ZigBee е протокол за безжична комуникация, който се използва широко в прецизното земеделие за наблюдение на условията на околната среда, свързани със здравето на културите. Той се основава на безжичния стандарт 802.15.4. По принцип е разработен за персонални. Той има гъвкава структура, дълъг живот на батерията и поддържа мрежова, звездна и дървовидна топология с пренос на данни, които преминават през няколко вътрешни маршрутизатора на мрежата. Лесно се инсталира и поддържа големи възли. Протоколът има малък обхват с ограничена скорост на предаване на данни и не е толкова сигурен, колкото системите, основани на Wi-Fi. ZigBee е широко разпространен в приложенията за интелигентно растениевъдство от рода на интелигентни оранжерии и напоителни системи. Тази система се състои от два възела - сензорен и изпълнителен възел. Сензорният възел се състои от сензори за влажност на почвата, които следят нивото на водата. Задвижващият възел е предназначен за предприемане на действия в зависимост от нивото на водата в почвата. Цялата комуникация се осъществява чрез протокола ZigBee.

BLE е познатата интелигентна технология Bluetooth, подходящ протокол за IoT приложения, включително и в селското стопанство, разработен специално за приложения с ниска честотна лента, ниска латентност и малък обхват. Сред основните предимства на BLE спрямо типичния Bluetooth са по-краткото време за настройка, по-ниската консумация на енергия и неограничената поддръжка на възли в топология тип „звезда“. Недостатъците му са, че може да осигури комуникация само между две устройства с ниска степен на сигурност и може да изгуби връзка по време на комуникация. Инфраструктурата, основана на BLE, събира данните от сензорите. Може да се използва със смартфон за събиране на данни от сензори за влажност и за температура на почвата, разположени сред растенията.

Системите за радиочестотна идентификация **(RFID)** се състоят от четец и транспондер, които имат много малка радиочестота, наречена радиочестотен етикет, програмиран електронно с отличителна информация, която може да се прочете. Радиочестотната идентификация разполага с две технологии за системата на етикетите – първата е системата с таг за четец, а другата е с таг за пасивен идентификатор.

Четците са по-скъпи, тъй като използват повече енергия от батериите и работят на високи честоти, а идентификаторът от своя страна е с ниска консумация на енергия. Приложения, използващи радиочестотната идентификация могат да бъдат открити в „умното“ пазаруване, в здравеопазването, в системите на националната сигурност и в интелигентно селско стопанство. Интелигентната система за напояване, основана на радиочестотна идентификация, се състои от сензори за влажност и температура на почвата заедно със система за контрол на водата, така че да събира показанията на сензорите и да ги изпраща към облака. С помощта на комуникационни протоколи потребителят контролира водната помпа въз основа на данните за нивото на водата в почвата.

Wi-Fi (Wireless Local Area Network – WLAN) е най-разпространеният комуникационен протокол, който позволява на устройствата да комуникират чрез безжичен сигнал. Wi-Fi осигурява безжична локална мрежа за свързване с висока скорост на милиони локации. Wi-Fi се използва широко в приложения, основани на Интернет на нещата, включително в селскостопански системи за интелигентно напояване, наблюдение на здравето на културите и в оранжерии. Инфраструктурата следи параметрите на околната среда в оранжерията – например температура, интензивност на светлината и ниво на влажност на почвата. Тази платформа се състои от сензори, които събират данни за изменението на околната среда и ги изпращат към облак. По подобен начин друга интелигентна селскостопанска система, основана на Wi-Fi комуникационни протоколи, се състои от Raspberry Pi (серия от едноплаткови компютри с малки размери), свързани с множество сензори за събиране на данни.

През последните две десетилетия дистанционното наблюдение на състоянието на културите навлезе широко в прецизното земеделие – явление, при което физическите условия на Земята се наблюдават от разстояние чрез изчисляване на излъчената и отразената радиация, специални камери заснемат изображения за по-нататъшен анализ, за да се установят характеристиките на определена област. Тези камери се монтират на множество платформи, които биват въздушни, сателитни и чрез безпилотни летателни апарати. Всяка платформа има собствено покритие, като обхвата се определя от три фактора – разстоянието за вземане на проби, което се изчислява въз основа на пространствената разделителна способност; скоростта или честотата на събиране на данни; средното разстояние между обекта и сензора.[3]

Сателитните платформи за дистанционно наблюдение се смятат за най-стабилните сред всички платформи. Състоящи се от спътници, ракети и космически совалки, те се разделят на категории въз основа на орбитите и синхронизацията на времето. Едно от предимствата на спътниковите дистанционни изследвания е високата пространствена разделителна способност, която ги прави перспективни за извличане на обширни данни за времеви редове, а изображенията, получени от спътникови платформи, обхващат голяма площ, стабилни са и са без шум, който обикновено се предизвиква от смущения при заснемането на изображенията.

Основни проблеми при сателитните платформи са високата цена за изображения с висока пространствена разделителна способност; строго фиксираният график, поради който не могат да се събират данни в критични моменти; силно чувствителни са към метеорологичните условия. Комерсиалните платформи от рода на Pleiades-1 предоставят изображения с висока разделителна способност и време за преразглеждане от един ден. QuickBird, Landsat-8 и Sentinel са често използвани сателитни платформи за получаване на хиперспектрални изображения.

В QuickBird се използват панхроматичен (PAN) и четири мултиспектрални (MS) сензора за изображения с разстояние за вземане на проби от земята от 0.7 × 0.7–2.6 × 2.6 m и с време за преразглеждане от 1 до 3 и половина дни.

Въпреки че времето за преразглеждане на Landsat-8 е много по-голямо в сравнение с QuickBird, той предоставя изображения с 11 различни многоспектрални ленти.

Sentinel е друг широко използван сателит, част от програмата „Коперник“ на ЕС. Той има три мисии Sentinel-1, Sentinel-2 и Sentinel-3, които предоставят мултиспектрални спътникови изображения в 21 спектрални канала, с време на наблюдение от 5 до 10 дни в зависимост от това коя мисия Sentinel се използва. Sentinel-2 е често използвана платформа в прецизното земеделие, тъй като предоставя свободен достъп до данни с пространствена разделителна способност 10 м и покрива ширина на лентата 290 км. Чрез комбинирането на Sentinel-2A и Sentinel-2B времето за повторно посещение се намалява допълнително до пет дни, което помага за откриването на промени. Могат да бъдат използвани и други платформи като SAT, MODIS и WordView.

Въздушните платформи са по – приспособими в сравнение със сателитните, но все още са значително по-скъпи. Времето за повторно посещение се контролира от човек и може да бъде променено във всеки един момент. Зоната на покритие на въздушните платформи е по-голяма от тази на платформите, основани на безпилотни летателни апарати, но значително по-малка в сравнение със сателитните платформи.[6]

Платформите, основани на безпилотни летателни апарати, са доста по-приспособими и икономически ефективни в сравнение със сателитните и въздушните платформи. Те се състоят от комуникационна и навигационна система с набор от сензори. Срещат се два основни вида системи – основани на безпилотни летателни апарати тип фиксирано крило (по-често използвани) и многороторни дронове.[5] Времето за полет се определя от теглото на полезния товар. Летателните апарати тип фиксирано крило постигат по-дълго време за полет при по-лек полезен товар. Камери с висока разделителна способност с тегло под 300 грама полезен товар на безпилотен летателен апарат с фиксирано крило осигуряват полет с продължителност от около два часа. Многороторните безпилотни летателни апарати с по-голям полезен товар имат по-кратко време за полет от около 15-25 мин., през които се постига висока прецизност на резултатите без усилие.



**Фиг. 1.** Земеделски дрон DJI Agras T20

Безпилотния летателен апарат DJI Agras T20 (Фиг.1) със своите мощни характеристики и изключителни възможности за пръскане, може да извършва автономни операции на различни терени, като земеделски земи с широколистни масиви, тераси и овощни градини. Новите функции, като всепосочен цифров радар, помогат на T20 да достигне стабилността и безопасността на полета в следващото ниво, предоставяйки на потребителите високоефективни резултати.[7]

Друг такъв апарат е и EASYFLY A2500_WH с камера Tetra cam ADC Micro, която може да се използва за заснемане на хиперспектрални изображения на два различни вида култури – например лозя и домати, като изображенията, които заснема, са с много висока разделителна способност и позволяват извличане на повече информация в сравнение със сателитните изображения. [5]

Ускоряване въвеждането на цифровизацията на селскостопанските практики особено сред средните и малки земеделски стопанства ще позволи производството на растителни, както и животински продукти с все по-висока ефективност и все по-малко въздействие върху околната среда. Изследванията показват, че въвеждането на нови технологии ще бъде затруднено сред малките и средни земеделски стопанства.

Скъпите машини, липсата на инфраструктура и липсата на знания са само малка част от предизвикателствата, които земеделието трябва да преодолее.

Прецизното земеделие се основава на събирането на информация за редица показатели характеризиращи микроклиматични условия, климатични условия на терена, като същевременно могат да натрупват тази информация под формата на архив в дигитална форма, давайки възможност за хронологично проследяване на промените във всяка от използваните групи показатели.

Цифровата трансформация е необходим процес на технологично развитие на България за създаване на условия за иновации и растеж на бизнеса, повишаване ефективността на работната сила, конкурентоспособна цифрова икономика и висок стандарт на гражданите.

**ЛИТЕРАТУРА:**

[1] Minchev, M., "Fundamentals of GPS application in geodesy", Sofia, 2013;

[2] Mihailov, R., "Precision Agriculture", Lecture Notes, ed. TU – Varna, ISBN 978-954-20-0792-0, 2019;

[3] Mihailov, R., Researching problems in agriculture with the means of technology and digital technologies: monograph, TU - Varna, 2021, ISBN - 978-954-20-0827-9

[4] Nikolov D., Iv. Boevski, P. Borisov, M. Atanasova-Chopeva, Kr. Kostenarov, Ev. Petkov, B. Fidanska, "DIGITALIZATION IN AGRICULTURE - COMPETITIVENESS AND BUSINESS MODELS", 2022 Institute of Agrarian Economics, publisher ISBN 978-954-8612-40-1

[5] Tsvetkov, V., "Drone sprayer", Student Scientific Session '17, Ruse, pp. 113-116, 2017

[6] Tsvetkov, Il., "Investigation of the applicability of a telemetric system for testing agricultural machinery", Author's abstract of a dissertation for the acquisition of the ONS "doctor" in the specialty "Mechanization and electrification of crop production", 2010;

[7] https://nik.bg/preczizno-zemedelie/oborudvane-za-preczizno-zemedelie/zemedelski-dronove/

# TECHNICAL PROVISION OF THE TRAINING FOR ACQUIRING THE DRIVING LICENSE IN HIGH SCHOOLS*

**TSVETOSLAV S. TSANKOV, STANIMIRA TS. STANISLAVOVA**

***ABSTRACT:*** *This report explores the evolution of driver training methods in Bulgaria, combining traditional approaches with modern technologies. The report proposes a new mechanical simulator that provides realistic driving conditions, addressing the main shortcomings of virtual simulators and training vehicles. The simulator allows trainees to refine their skills and build muscle memory without being exposed to risks. Introducing dual education and restoring professional driver training aims to enhance student preparation and meet the needs of the transport sector. The report highlights the importance of quality training to improve road safety and reduce unemployment, particularly in high-unemployment regions.*

***KEYWORDS:*** *driver training, exercise equipment, high schools*

***DOI: https://doi.org/10.46687/DRFL3040***

# ТЕХНИЧЕСКО ОБЕЗПЕЧАВАНЕ НА ОБУЧЕНИЕТО ЗА ПРИДОБИВАНЕ НА ПРАВОСПОСОБНОСТ ЗА УПРАВЛЕНИЕ НА МПС В ГИМНАЗИИТЕ

**ЦВЕТОСЛАВ С. ЦАНКОВ, СТАНИМИРА Ц. СТАНИСЛАВОВА**

***АБСТРАКТ:*** *Настоящият доклад разглежда развитието на методите за обучение на водачи на моторни превозни средства в България, съчетавайки традиционни подходи с модерни технологии. Предлага се нов механичен тренажор, който осигурява реалистични условия на управление, като преодолява основните недостатъци на виртуалните симулатори и учебните автомобили. Тренажорът позволява на обучаемите да усъвършенстват своите умения и да изградят мускулна памет, без да бъдат изложени на рискове. Въвеждането на дуално обучение и възстановяването на професионалното обучение за водачи ще подобри подготовката и ще отговори на нуждите на транспортния сектор. Докладът подчертава значението на качественото обучение за подобряване на безопасността и намаляване на безработицата, особено в региони с висока безработица.*

## 1 Въведение

От зората на масовото използване на автомобилите по пътищата се работи по две основни взаимосвързани задачи – осигуряване на правила за пътна безопасност и предоставяне на обучение за водачите на моторни превозни средства. Разбира се сложността при изпълнението на тези задачи многократно се е увеличила до наши дни, което налага безопасността на движението по пътищата (БДП) да се изучава още от най-ранна детска възраст, през начален, прогимназиален и гимназиален етап на обучение, до придобиване на свидетелство за управление на моторни превозни средства (МПС). Една от най-големите загуби за професионалното образование в България е допълнителната безплатна възможност за придобиване от учениците на професионална категория за автомобилен водач. Стремежът към придобиване на втора професия за водач бе много добър стимул за усърдното представяне на учениците и по другите учебни предмети.

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

Отпадането на курсовете за професионални водачи започва още в началото на прехода в държавата ни, през 90-те години на миналия век, главно поради липсата на финансиране на такава част от образованието. Създаваните и използвани технически средства за обучение, като автоматизирани табла, схеми, тренажори и т.н. останаха в миналото, както и учебните автомобили, площадки и гаражите за техническо обслужване и ремонт. Много добра възможност за обучение на професионални водачи със сериозна техническа база имаше в учебните школи, които бяха на Българската народна армия (Българската армия) и провеждаха обучението по време на задължителната тогава за младите мъже наборна военна служба. [13, 14, 15, 16, 17, 18, 19]

Днес се предлага разширяване на обучението за безопасност на пътищата в училищна среда и разглеждане на възможностите за обучението в системата на средното образование по транспортни специалности. Това включва увеличаване на приема в паралелки както в професионалните гимназии по транспорт, така и в други средни училища, особено в райони с по-висока безработица. Предложението се основава на факта, че транспортният сектор генерира 17% от БВП на България, но изпитва недостиг на водачи. Това би могло да помогне за снабдяването на сектора с необходимия човешки ресурс и ще подобри обучението с професионални преподаватели. В районите с по-висока безработица това ще има положителен ефект, като учениците ще завършат с професионална подготовка. Предлага се увеличаване на възможностите за професионално образование чрез дуално обучение в професионалните гимназии за придобиване на правоспособност за управление на категория „С“. Това ще позволи управление на МПС с наставник като условие за придобиване на категорията и ще направи младежите конкурентоспособни на пазара на труда. За постигане на тези цели е необходимо обезпечаване на образованието с подготвени инструктори и бази за обучение.

Настоящата публикация се отнася до съвременното състояние на дидактическите материали, които се използват за обучението на водачи на моторни превозни средства в българските училища. Авторът е придобил опит като преподавател-инструктор на водачи на МПС, не се противопоставя на съвременните технически средства, използвани при обучението на водачите и предлага способ за предотвратяване на рязката промяна от теоретична подготовка и виртуална обучаваща среда към реалната пътна обстановка.

## 2 Традиционни методи за обучение на водачи на МПС

Обучението за управление на автомобил на учебна площадка в миналото се е провеждало в строго контролирана среда, осигуряваща безопасно пространство за упражняване на основните умения на бъдещите шофьори. В съответствие с приетите тогава стандарти, учебните площадки обикновено са били разположени в покрайнините на градовете и са били оборудвани с основни пътни знаци, светлинни сигнали и маркировки, за да имитират възможно най-близо реалната пътна обстановка.

Обучителният процес е започвал със задълбочено теоретично обучение, което е обхващало правилата за движение по пътищата, включително изучаването на различни пътни знаци, светлинни сигнали и приоритетите между различните участници в движението. Теорията е включвала и основи на пътната безопасност, както и базови механични познания за структурата и управлението на автомобила. Тази теоретична подготовка е играела съществена роля за разбиране на отговорностите и рисковете, свързани с шофирането.

След завършване на теорията, курсистите са били въвеждани в практическата част на обучението, започвайки с ориентиране в самото превозно средство. Инструкторът е

обяснявал функциите на арматурното табло, позицията на педалите и скоростния лост и е давал насоки за правилната стойка и разположение на ръцете на волана и краката върху педалите. Първоначалната ориентация е била важен етап от обучението, целящ да подготви кандидатите за основни действия и реакции при управлението на автомобила.

Практическата част на учебната площадка е позволявала на курсистите да изпълняват основни маневри, като тръгване и спиране, движение в права линия, завой наляво и надясно. Постепенно са били включвани и по-сложни маневри като паркиране на заден ход, успоредно паркиране и завиване в тесни пространства (фиг. 1). Инструкторите са наблюдавали всяка стъпка, като са насочвали курсистите към постепенна работа върху сложността на задачите и изграждане на увереност в тяхното управление.




**Фиг. 1.** Учебна площадка за обучение на водачи от категории А, В и СЕ

Финалната фаза на обучението е завършвала с практически изпит, в който курсистите е трябвало да демонстрират овладените умения. Изпитващите са оценявали тяхната прецизност при изпълнение на различни маневри, спазване на правилата за движение и реакция в различни ситуации, които могат да възникнат по време на реално шофиране. Чрез този метод на обучение, кандидат-водачите са изграждали необходимите рефлекси и устойчиви навици за безопасно поведение на пътя, преди да преминат към практиката в реална среда на пътя. [1, 2, 3, 4, 5]

## 3 Поглед към съвременните методи за симулиране на обучение за водачи на автомобили

Съвременните методи за симулиране на обучение за водачи на автомобили са изключително ефективен и безопасен начин за развитие на умения и повишаване на увереността на шофьорите. Технологиите в областта на автомобилните симулатори включват комбинация от виртуална реалност, усъвършенствани графични системи и тактилна обратна връзка, които позволяват реалистично възпроизвеждане на различни ситуации на пътя (фиг. 2).

Симулациите обхващат широк диапазон от сценарии, като градско движение, магистрали, неочаквани инциденти, опасни метеорологични условия и реакции на различни видове пътни опасности. Това помага на обучаващите се да придобият реален опит в

контролирана среда без риск за тях или околните участници в движението. Освен това симулаторите позволяват повторно проиграване на критични ситуации, което спомага на шофьорите да анализират своите грешки и да подобряват реакциите си. Също така те могат да практикуват в условия, които не са лесни за възпроизвеждане в реалния свят, като екстремни атмосферни условия или необичайни пътни ситуации.








**Фиг. 2.** Компютърни системи за симулация на управление и използване на виртуална реалност

Технологиите за тактилна обратна връзка позволяват на обучаемите да почувстват вибрации, съпротивление и други физически усещания, които симулират реалното поведение на автомобила. Например, вибрации на волана при преминаване през неравности на пътя или усещане за загуба на сцепление в хлъзгави условия. Тези тактилни стимули допълнително усилват реалистичността на симулацията и позволяват на водачите да развиват интуитивно разбиране за поведението на превозното средство.

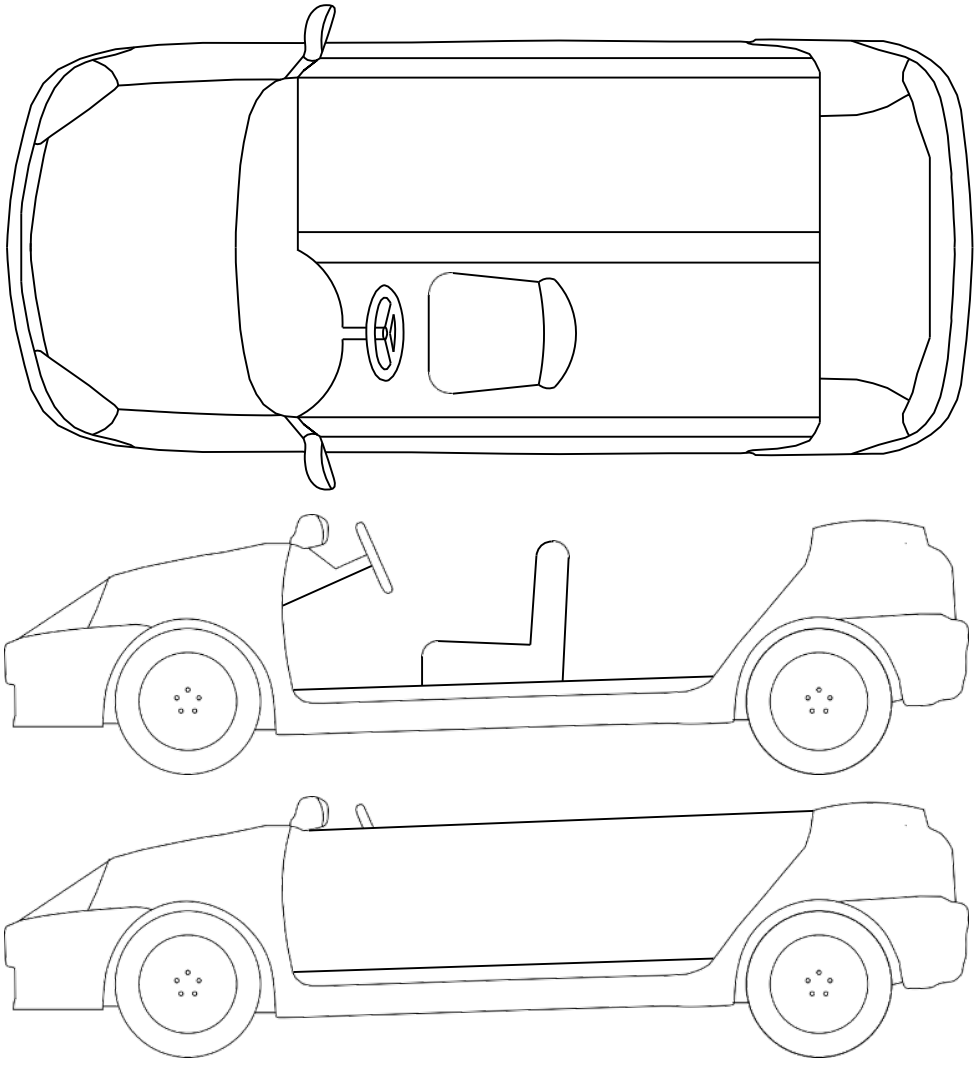
Съвременните симулатори включват и възможности за събиране на данни за поведението на водача – като скорост на реакция, спазване на правила и управление в стресови ситуации. Тези данни се използват за персонализирана обратна връзка и разработване на индивидуални обучителни програми, които помагат на всеки водач да се фокусира върху слабите си страни и да ги подобри. Това прави процеса на обучение много по-ефективен и целенасочен, като се отчита специфичното поведение и умения на всеки обучаем. Симулаторите често се използват и за обучение на професионални шофьори – като водачи на автобуси, камиони и специализирани превозни средства, където подготовката и безопасността са от особена важност. Чрез използването на симулатори, професионалните

шофьори могат да бъдат обучавани в специфични условия, като управление на тежък товар, маневриране в ограничени пространства и реагиране на извънредни ситуации на пътя.

С напредъка в технологиите, симулаторите стават все по-достъпни и по-реалистични. Въвеждането на изкуствен интелект и усъвършенствана реалност в обучението обещава още по-високо ниво на персонализация и автентичност на симулацията. Изкуственият интелект може да анализира и адаптира симулацията според поведението на обучаемия, като създава динамични и адаптивни сценарии, които отразяват реални ситуации на пътя. В бъдеще може да се очаква, че тези технологии ще доведат до още по-безопасно и ефективно обучение, което ще помогне за намаляване на пътните инциденти и ще подобри цялостната култура на шофиране. [6, 7, 9, 10, 12]

## 4 Тренажор за водачи на автомобили в реални размери

Предложено е изобретение, представляващо механичен тренажор за обучение на водачи на автомобили, който е проектиран да бъде максимално близък до реалния автомобил, за да предостави почти реална симулация на шофиране, без да поставя водачите в реална опасност (фиг. 3).



**Фиг. 3.** Чертеж на механичния тренажор за водачи на автомобили в реални размери

Механичните тренажори имат множество предимства в сравнение с виртуалните симулатори, най-вече поради факта, че те предлагат по-реалистично физическо усещане, което помага на обучаемите да развият мускулна памет и да придобият навици, които са пряко приложими в истински автомобил. В същото време те премахват риска от инциденти, който съществува при обучението в реална среда, особено при начинаещи водачи.

Един от основните недостатъци на виртуалните симулатори е липсата на реалистичен контакт с физическия автомобил и усещането за движение. Механичните тренажори преодоляват този недостатък, като предлагат истински компоненти, които обучаващите се могат да контролират и манипулират, подобно на реална ситуация. Те позволяват също така проиграване на различни сценарии, като аварийно спиране, паркиране и маневриране в ограничени пространства, без риск за обучаващите се и другите участници в движението. [6, 8, 9, 11]

Предложеният механичен тренажор трябва да бъде максимално близък до реалния автомобил, като ще включва всички основни компоненти и ще предлага реалистични условия на управление. По този начин ще се избегнат множество недостатъци на виртуалното обучение, като същевременно ще се обезопаси процесът на обучение.

Основната цел е да се съчетае безопасността на симулатора с реалистичността на управлението на истински автомобил, така че обучаемите да придобият максимално реалистичен опит и увереност.

# 5 Заключение

Развитието на методите за обучение на водачи на МПС изисква баланс между традиционните и съвременните подходи, за да се осигури цялостна и ефективна подготовка на бъдещите шофьори. Механичните тренажори и виртуалните симулатори предоставят безопасни и контролирани условия, в които курсантите могат да развиват своите умения и да натрупат увереност преди да излязат на реалния път. Осигуряването на качествено образование в системата на средното професионално образование и възстановяването на обучението за професионални водачи ще допринесе за повишаване на безопасността на пътищата, подобряване на професионалната подготовка и намаляване на безработицата в страната. Технологиите продължават да играят важна роля, като създават нови възможности за по-персонализирано и автентично обучение, което в крайна сметка ще доведе до по-високо ниво на пътна безопасност и компетентност на водачите.

**ЛИТЕРАТУРА:**

[1] Георгиев, Г. Методика за обучение на водачи на МПС. София, Държавно издателство, 1988.

[2] Иванов, П., Стоянов, Н. и др. Практическо обучение за управление на МПС. Бургас, 1991.

[3] Николов, И. Основи на пътната безопасност. София, 1994.

[4] Петров, Д. Теория и практика на шофирането. Пловдив, 1992.

[5] Стоянов, Н. и др. Пътна безопасност за бъдещите шофьори. Велико Търново, 1993.

[6] Allen, R. W., Park, G., Cook, M. L., & Fiorentino, D. The Effect of Driving Simulator Fidelity on Training Effectiveness. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 51(22), 2007, 1751-1755.

[7] Blana, E. Driving Simulator Validation Studies: A Literature Review. Institute of Transport Studies, University of Leeds, 1996.

[8] Jamson, S. L., & Merat, N. Surrogate In-Vehicle Information Systems and Driver Behaviour: Effects on Vehicle Control and Task Sharing. Transportation Research Part F: Traffic Psychology and Behaviour, 8(2), 2005, 79-96.

[9] Kemeny, A., & Panerai, F. Evaluating Perception in Driving Simulation: Comparison of Simulator and Real-World Behaviors. Transportation Research Part F: Traffic Psychology and Behaviour, 6(3), 2003, 217-232.

[10] Regan, M. A., Lee, J. D., & Young, K. L. Driver Distraction: Theory, Effects, and Mitigation. CRC Press, 2008.

[11] Salas, E., & Cannon-Bowers, J. A. The Science of Training: A Decade of Progress. Annual Review of Psychology, 52, 2001, 471-499.

[12] Stanton, N. Advances in Human Aspects of Transportation. AHFE Conference, 2017.

[13] https://www.mon.bg/nfs/2021/03/np3_savrobr_sreda_100321.pdf

[14] https://bdp-bg.net/%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%B0-%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F/

[15] https://www.mon.bg/profesionalno-obrazovanie/pravosposobnost-za-upravlenie-na-mps/uchebna-dokumentatsiya-za-obuchenie-na-kandidatite-za-pridobivane-na-pravosposobnost-za-upravlenie-na-motorni-prevozni-sredstva/

[16] https://rta.government.bg/upload/642/n37.pdf

[17] https://lex.bg/laws/ldoc/2135457094

[18] https://rta.government.bg/upload/9175/n38.pdf

[19] https://journals.uni-vt.bg/almanac/bul/vol19/iss2/art13

# THE ROLE OF ROAD TRAINS IN OPTIMIZING FREIGHT TRANSPORT IN EUROPE*

**VALENTIN K. SEMOV, ANGELINKA TS. STANISLAVOVA**

***ABSTRACT:*** *This paper examines the role of truck trains in enhancing freight transport efficiency across busy pan-European corridors, particularly in Eastern European countries like Bulgaria and Romania. It highlights the challenges posed by overloaded roads and inadequate infrastructure, suggesting that truck trains can optimize road usage and reduce harmful emissions while lowering logistics costs by allowing larger loads with fewer vehicles. The discussion also emphasizes the need for improved transportation infrastructure, supported by investments in smart technologies and longer freight vehicles, such as the innovative 18-meter solo truck design proposed, which aims to increase cargo capacity while maintaining safety and compliance with road conditions. Ultimately, the adoption of truck trains presents significant economic and environmental benefits, promoting a more sustainable transport network for Europe.*

***KEYWORDS:*** *road trains, freight transport, infrastructure, harmful emissions, logistics, transport corridors*

***DOI: https://doi.org/10.46687/LMSG8539***

# РОЛЯТА НА АВТОВЛАКОВЕТЕ В ОПТИМИЗАЦИЯТА НА ТОВАРНИЯ ТРАНСПОРТ В ЕВРОПА

**ВАЛЕНТИН К. СЕМОВ, АНГЕЛИНКА Ц. СТАНИСЛАВОВА**

***АБСТРАКТ:*** *В този доклад се разглежда ролята на автовлаковете в подобряването на ефективността на товарния транспорт в натоварените паневропейски коридори, особено в източноевропейски страни като България и Румъния. Подчертават се предизвикателствата, свързани с претоварените пътища и недостатъчната инфраструктура, като се предлага, че автовлаковете могат да оптимизират натоварването на пътищата и да намалят вредните емисии, като същевременно намалят разходите за логистика чрез транспортиране на по-големи товари с по-малко превозни средства. Обсъжда се и необходимостта от подобряване на транспортната инфраструктура, подкрепена от инвестиции в интелигентни технологии и дълги товарни автомобили, като предложената иновативна конструкция на соло камион с дължина 18 метра, която цели увеличаване на товароподемността при запазване на безопасността и съответствието с условията на пътищата. В крайна сметка, внедряването на автовлакове предлага значителни икономически и екологични ползи, насърчавайки устойчивата транспортна мрежа в Европа.*

## 1 Въведение

Автовлаковете са ключов елемент за увеличаване на ефективността в тежкотоварния транспорт, особено на дълги разстояния в натоварените паневропейски коридори. Паневропейските коридори обхващат множество държави и играят важна роля за международната търговия и икономическото развитие на Европа. Държавите в Източна Европа, като България и Румъния, често срещат проблеми поради претоварени пътища и липсата на инфраструктурни възможности за поддръжка на тежък трафик. В този контекст автовлаковете могат да предложат решение, което ще оптимизира натовареността на

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

пътищата и ще допринесе за намаляване на вредните емисии. Те също така предлагат по-добра ефективност на логистиката и по-ниски разходи, като позволяват транспортиране на по-големи товари с по-малко превозни средства, което намалява въздействието върху околната среда. Това разбира се трябва да става с развитие на транспортните средства, които да се движат по асфалтовите пътища. [5, 6, 11]

## 2 Усъвършенстването на пътищата в Европа и света

Европа е изправена пред предизвикателството да поддържа своята транспортна инфраструктура адекватна за нарастващите нужди от транзитен товарен транспорт. В много части на Източна Европа, където инфраструктурата е ограничена от тесни пътни платна, остри завои и стръмни наклони, тежкотоварните камиони срещат големи трудности, а това води до значителни икономически и социални загуби. Според доклад на Европейската комисия лошото състояние на транспортната инфраструктура в региона причинява ежегодни загуби от над 100 милиарда евро, свързани със задръствания, закъснения на товари и аварии по пътищата.

Инвестициите в транспортната инфраструктура са критични за подобряване на логистичната ефективност и икономическия растеж в Източна Европа. Пътните коридори като TEN-T (Trans-European Transport Network) представляват гръбнака на транспортната мрежа в региона и са приоритет за финансиране от страна на ЕС. TEN-T включва основни магистрални връзки, железопътни линии и терминали, които подпомагат междурегионалната свързаност и насърчават интеграцията на тежкотоварните транспортни средства.

Пример за успешна оптимизация чрез автовлакове е Швеция, която разработва мрежа от маршрути за товарни композиции с дължина до 25 метра. Проектът показва, че чрез удължаване на транспортните средства, разходите за логистика могат да бъдат намалени с до 20%. Освен това, Финландия също работи върху разширяване на инфраструктурата, за да позволи автовлакове с дължина над 30 метра, което значително подобрява ефективността на транспортния сектор в страната. Според финландското министерство на транспорта и съобщенията тези инициативи водят до подобрение на логистичните вериги и намаляват зависимостта от няколко по-малки камиона, което намалява и вредните емисии с над 15%.

В допълнение към инфраструктурните проекти, Европейският съюз инвестира в нови технологии за пътна инфраструктура, които да осигурят по-безопасно движение на товарните автомобили. Такива технологии включват интелигентни пътни знаци, системи за наблюдение на трафика и „умни“ пътни настилки, които могат да предупреждават за лед и опасни условия. Проучване на Европейската инвестиционна банка подчертава, че модернизацията на пътната инфраструктура, включваща такива технологии, може да намали аварийните случаи с до 30% и да подобри цялостната сигурност на транспортната мрежа. [12, 13, 15, 16]

## 3 Стремеж към намаляване на замърсяванията от тежкотоварните автомобили

Преминаването към автовлакове в транспортните коридори на Европа има потенциал да допринесе за значително намаляване на въглеродните емисии. Според доклад на Международната агенция по енергетика, тежкотоварният транспорт е отговорен за приблизително 25% от всички въглеродни емисии от транспортния сектор в Европа. Използването на автовлакове и нови технологии като електрически и хибридни товарни автомобили може да намали този процент с до 30% в дългосрочен план.

Електрическите автовлакове и хибридните технологии вече се прилагат в някои страни и показват, че са икономически ефективни в дългосрочен план. Например Норвегия и Холандия са водещи в създаването на зелени коридори, където електрическите и хибридни товарни автомобили могат да се зареждат по трасето. Тези зелени коридори позволяват намаляване на въглеродния отпечатък с до 30%, което съществено допринася за постигане на целите на ЕС за намаляване на емисиите.

Франция стартира програма за развитие на електрически пътища, които позволяват товарните автомобили да зареждат своите батерии по време на движение чрез електрифицирани линии, вградени в пътното платно. Според проучване на Френската национална агенция за енергийна ефективност (ADEME), това иновативно решение може да намали разхода на гориво с до 20% и да допринесе за значително по-ниски нива на вредни емисии, което го прави обещаваща технология за бъдещето.

С цел намаляване на неблагоприятните последствия за околната среда, от десетилетия се предприемат мерки по конструкцията на автомобилите, които се използват предимно за градско движение. Европейските стандарти за изгорели газове, като Euro 4, Euro 5 и Euro 6, се въвеждат поетапно с цел да намалят нивото на вредните емисии. Най-актуалният стандарт е Euro 6d, който въвежда по-строги ограничения за отделяните отработени газове, с цел подобряване на качеството на въздуха в градовете.

От много години насам, изследователите подчертават необходимостта от преход към алтернативни енергийни източници. Природният газ и пропан-бутан са доказани като ефективни алтернативи на бензина и дизела, които значително намаляват въглеродните емисии. Според проучване на International Council on Clean Transportation (ICCT), използването на природен газ в тежкотоварния транспорт може да намали емисиите на CO2 с до 20%, а на метанол и пропан-бутан – с около 15%. [13, 14, 16, 17]

# 4 Конструкция на соло товарен автомобил с голяма дължина

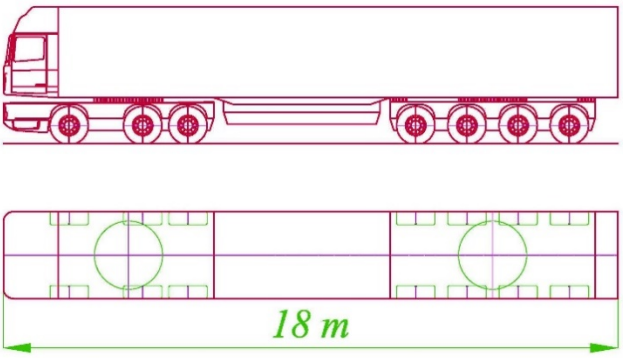
Конструкторите на товарни автомобили винаги са имали за цел да повишат товароподемността и ефективността на транспортните средства. Стремежът към разработването на много дълги соло камиони е част от по-широката тенденция в автомобилостроенето, която е насочена към увеличаване на капацитета на превозните средства. С помощта на иновации в дизайна и технологиите производителите се опитват да създадат модели, способни да отговорят на растящото търсене на транспортни услуги, особено в контекста на глобализацията и увеличената икономическа активност.

Историята показва как усилията за изграждане на дълги соло камиони са били фокусирани върху подобряване на маневреността и функционалността. Конструкцията на тези превозни средства трябва да отговаря на специфичните условия на пътищата, особено в планински райони, където завоите и наклоните създават предизвикателства.

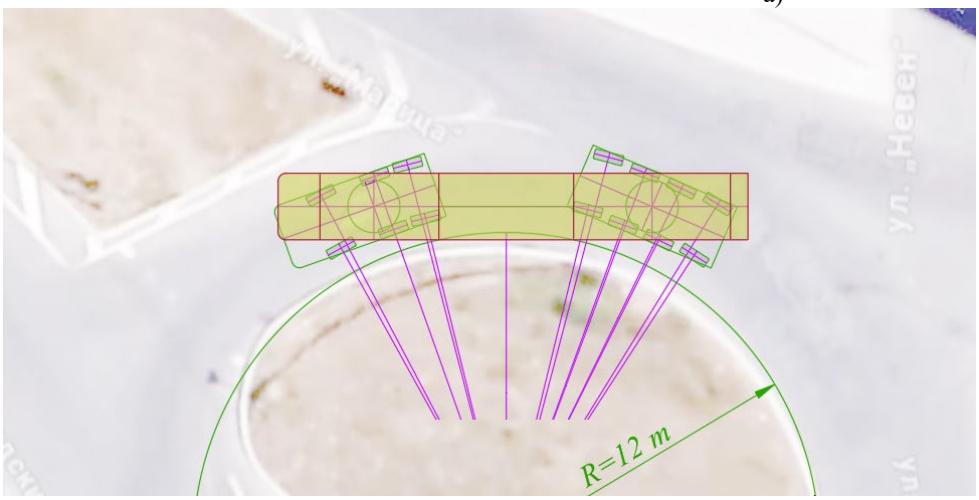
На фиг. 1 е представен иновативен модел на товарен автомобил с дължина 18 метра и максимална маса от 40 тона, включващ концепцията за автовлак, която може да се адаптира към нуждите на транспортната индустрия. Проектът е предложен с оглед на геометричните ограничения, изискващи спазване на завоите по пътищата в България, Румъния и други европейски страни, което е от съществено значение за безопасността и ефективността при движение. [1, 2, 3, 4, 7, 8, 9, 10]

Конструкцията позволява отпадане на един от предните и един от задните мостове, без да се променя дължината, а само полезният товарен обем. Тази характеристика може да оптимизира теглото и да намали производствените разходи. Прилагането на хидропневматично окачване е важно, за да се осигури плавно и стабилно движение, особено

при дълги превозни средства. Накрая дизайнът наподобява железопътен вагон с управляеми талиги или шасита, което осигурява необходимата маневреност и контрол при управление.




а)




б)

**Фиг. 1.** Модел на единичен товарен автомобил (а) и преодоляван от него завой в обратна посока (б)

## 5 Заключение

Внедряването на автовлакове по паневропейските коридори предлага значителни ползи както от икономическа, така и от екологична гледна точка. Макар че съществуват редица инфраструктурни и технологични предизвикателства, съвременните интелигентни системи за управление и инициативи за зелени коридори предоставят реални решения за тяхното преодоляване. В бъдеще автовлаковете могат да станат неразделна част от транспортната мрежа на Европа, като осигурят по-устойчив и икономически обоснован метод за превоз на товари.

**ЛИТЕРАТУРА:**

[1] Кочнев, Е.Д. Энциклопедия военных автомобилей 1769–2006 гг. Книжное издательство „За рулем“, Москва, 2006, 640 с.

[2] Лавров, О.М., Зайцев И.В., Голодовский Я.Е. Грузовые автомобили высокой проходимости. Воениздат, 1968.

[3] Тодорова, М. А., Цанков, Ц. С. Автомобил с подобрена високопроходимост за евакуация на хора от опасни райони. Сборник доклади от Международна научна конференция „Радиационната безопасност в съвременния свят“, т. 2, НВУ „Васил Левски“, Велико Търново, 2023, ISSN 2738-7607, с. 65-72.

[4] Цанков, Ц. Улучшение проходимости по бездорожью с помощью дополнительного колеса. Сборник статии от VIII международна научно-практическа интернет конференция „Рекултивация выработанного пространства: проблемы и перспективы“, Кузбасский государственный технический университет имени Т. Ф. Горбачева, 2023, ISBN 978-5-00137-296-7, с. 114-117.

[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] 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.

[7] Denton, T. & Pells, H. Automotive Technician Training: Theory 2nd Edition, Routledge, 2022, ISBN: 978-1-032-00233-0, https://doi.org/10.1201/9781003173236.

[8] Harwood, D. W. et al. Review of Truck Characteristics as Factors in Roadway Design. National Academy of Sciences, Washington, D.C., 2003, ISBN 978-0-309-08779-7.

[9] Popular Mechanics, Vol. June 1986, magazine of popular science and technology. ISSN 0032-4558.

[10] Trailer Consultation. Softwares for Commercial Vehicle Technical Calculations. https://trailerwin.com/

[11] Tsankov, Ts. Possibilities for the use of road trains on pan-European transport corridors. KNOWLEDGE – International Journal Scientific Papers, Vol. 63.3, Institute of Knowledge Management, Skopje, 2024, ISSN 2545-4439, pp. 303-309.

[12] https://julkaisut.valtioneuvosto.fi/handle/10024/80230

[13] https://transport.ec.europa.eu/transport-themes/mobility-strategy_en

[14] https://www.worldbank.org/en/topic/transport

[15] https://www.eib.org/en/projects/topics/sustainable-cities-regions/transport/index

[16] https://www.irena.org/Energy-Transition/Technology/Transport

[17] https://www.ademe-investissement.fr/en/press-releases/ademe-investissement-hisse-les-voiles-avec-neoline-pour-un-transport-maritime-decarbone/

# REVERSE LOGISTICS AND INNOVATIONS FOR MANAGING NON-REUSABLE TIRE WASTE*

**YORDANKA I. YANKOVA-YORDANOVA, TSVETOSLAV S. TSANKOV**

***ABSTRACT:*** *Non-reusable tire waste poses a significant environmental challenge due to its volume and resistance to degradation. This study explores sustainable approaches to its management, including recycling, reuse, and thermal methods such as pyrolysis. The environmental and economic benefits of these technologies are analyzed, alongside the design of efficient reverse logistics networks. By integrating innovations and optimized processes, waste reduction is achieved, and resources are repurposed for various industrial applications.*

***KEYWORDS:*** *logistics, management, pyrolysis, recycling, sustainable, tire waste*

***DOI: https://doi.org/10.46687/AEVR6118***

# ОБРАТНА ЛОГИСТИКА И ИНОВАЦИИ ЗА УПРАВЛЕНИЕ НА НЕИЗПОЛЗВАЕМИ ГУМЕНИ ОТПАДЪЦИ

**ЙОРДАНКА И. ЯНКОВА-ЙОРДАНОВА, ЦВЕТОСЛАВ С. ЦАНКОВ**

***АБСТРАКТ:*** *Неизползваемите гумени отпадъци представляват значителен екологичен проблем поради своя обем и трудната си разградимост. Настоящото изследване разглежда устойчиви подходи за тяхното управление, като включва рециклиране, повторна употреба и термични методи като пиролиза. Анализирани са екологичните и икономически ползи от тези технологии, както и проектирането на ефективни мрежи за обратна логистика. Чрез интеграция на иновации и оптимизирани процеси се постига не само намаляване на отпадъците, но и оползотворяване на ресурсите за различни индустриални приложения.*

## 1 Въведение

През последните години необходимостта от опазване на околната среда придобива все по-голяма значимост. Индустриалното производство и нарастващото потребление генерират огромни количества отпадъци, които оказват сериозно отрицателно въздействие върху природните ресурси и екологичния баланс. В този контекст обратната логистика заема ключова роля, като предлага устойчиви решения за намаляване на замърсяването чрез оптимизирано управление на отпадъците, включително рециклиране, повторна употреба и интегрирани системи за тяхното ефективно обработване.

Обратната логистика се дефинира като цялостен процес, който обхваща планирането, изпълнението и контрола на обратния поток на суровини, материали и готови продукти. При управлението на гумените отпадъци този процес включва редица специфични дейности. Сред тях са събирането на гуми, излезли от употреба, което изисква създаване на специализирани пунктове и внедряване на системи за връщане, които улесняват потребителите. В някои държави, като Германия, сервизите за подмяна на гуми директно ги предават на рециклиращи центрове, докато в Япония автоматизирани технологии позволяват сортиране на гумите според формата и размера. [1, 3, 6]

* Докладът е финансиран по проект № РД-08-124/01.02.2024г. – „Иновации и интерактивни технологии в обучението по Производствени технологии“

Рециклирането и повторната употреба на гумите също заемат важна част от управлението на отпадъците. Съвременните технологии позволяват тяхното раздробяване за производство на гумена гранула, използвана в спортни настилки и шумоизолационни панели. Освен това, гумите с минимални повреди често се възстановяват чрез ремонт, което ги прави годни за повторно използване в транспортния сектор. Възстановяването на каучуковия слой чрез „регенериране“ също е утвърдена практика, която намалява нуждата от нови ресурси.

Настоящият доклад изследва възможностите за оползотворяване на гумените отпадъци, разглеждайки съвременните подходи за тяхното управление. Особен акцент се поставя върху рециклирането, термичната обработка и иновационните технологии като пиролиза. Внимание се обръща и на проектирането на ефективни мрежи за обратна логистика, които да осигурят устойчиво управление на тези ресурси. Чрез интегрирането на такива подходи се търси не само намаляване на екологичния отпечатък, но и създаване на икономически ефективни решения за повторно използване на отпадъчните продукти.

## 2 Основни концепции на обратната логистика

Обратната логистика при гумите включва дейности като:

- *Събиране на излезли от употреба гуми:* Например, създаване на специализирани пунктове за събиране на стари гуми в градски и селски райони. В Германия, например, потребителите могат да върнат старите си гуми директно в сервизите за подмяна, които след това ги изпращат към рециклиращи центрове.
- *Сортиране според състоянието и типа:* Разделяне на гумите според тяхното състояние (износени, повредени, неотговарящи на стандартите за безопасност) и типа (автомобилни, индустриални, селскостопански). Например, в Япония гумите се сортират автоматизирано чрез технологии за разпознаване на формата и размера.
- *Рециклиране и повторна употреба:* Рециклирането включва различни технологии, като механично раздробяване на гумите за производство на гумена гранула, която се използва в настилки за спортни площадки. В Нидерландия, голяма част от рециклираните гуми се използват за шумоизолационни панели.

Повторната употреба, от друга страна, включва ремонт и повторно пускане в експлоатация на гуми, които могат да бъдат възстановени. Например, „регенериране“ на нов слой каучук върху използвани гуми е популярна практика в транспортния сектор (фиг. 1).



**Фиг. 1.** Регенериране на гума за товарен автомобил

## 3 Начини за оползотворяване на стари гуми

*ПОВТОРНА УПОТРЕБА*

Гуми с минимални повреди могат да бъдат ремонтирани и използвани повторно – използване на гуми за вторични приложения, като бариери на писти или други технически цели.

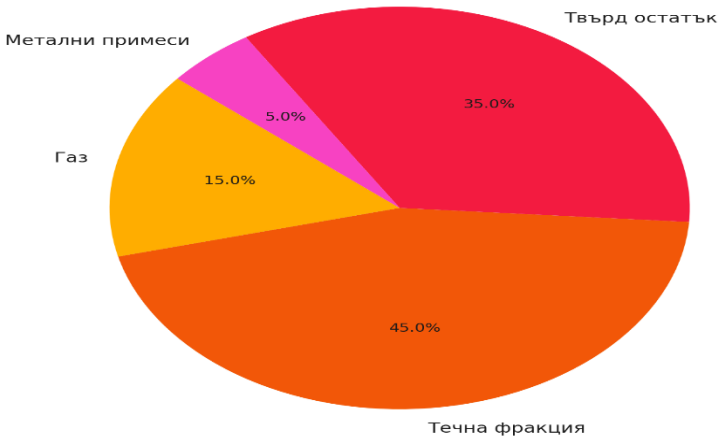
*РЕЦИКЛИРАНЕ*

- *Механично рециклиране:* Гумите се раздробяват и се използват като суровина за нови продукти като настилки за спортни площадки или шумоизолационни материали.
- *Термално рециклиране:* Извличане на енергия чрез изгаряне в специализирани инсталации, при спазване на екологичните норми.
- *Химическо рециклиране:* Разлагане на гумения материал до основни компоненти за използване в нови производствени процеси.

*ПИРОЛИЗИРАНЕ*

Гумените отпадъци, включително автомобилни гуми и конвейерни ленти, представляват значителен екологичен проблем поради обема си и затрудненото им разграждане. Пиролизата е метод за термично разграждане на тези материали в отсъствие на кислород, което води до получаване на газове, течни фракции, твърд въглероден остатък и метални примеси. Процесът протича при температура около 450°C и генерира три основни продукта: газ, течни горива и твърд въглероден остатък. [4, 5, 7]

Разпределението на продуктите, получени при пиролиза на гумени отпадъци е представена на фиг. 2. Основните фракции включват течна част (45%), твърд въглероден остатък (35%), газове (15%) и метални примеси (5%). Тези данни демонстрират потенциала за повторно използване на продуктите в различни индустриални приложения.




**Фиг. 2.** Разпределение на продуктите от пиролиза на гумени отпадъци

Пиролизата е екологично безопасен процес, при който не се отделят токсични съединения като диоксид на сярата или азотни оксиди. Получените течни продукти могат да се използват за отопление или като компоненти в производството на различни горива, докато твърдият въглероден остатък намира приложение като адсорбент, суровина за бездимно гориво или възстановител в металургията.

В твърдия въглероден остатък се съдържат значителни количества пепел и летливи вещества, които ограничават директното му приложение. За подобряване на качествата му се прилагат различни методи на облагородяване. Магнитната и вибрационната сепарация

позволяват ефективно отделяне на метални примеси, като масовият дял на отделените компоненти достига до 5%. Немагнитните метални остатъци също могат да бъдат отделени чрез вибрационна техника, което подобрява чистотата на крайния продукт. Допълнителното тежкосредно обогатяване, основано на разлики в плътността, намалява пепелното съдържание до стойности между 5% и 9,3%.

Термичната обработка на въглеродния остатък при температури около 800°C допринася за намаляване на летливите вещества под 0,4% и увеличава порьозността на материала. В резултат се елиминират токсични миризми и се отварят нови възможности за приложение.

Старите гуми също така намират приложение като алтернативен източник на енергия, особено в циментови заводи и други индустрии. Тяхната употреба в строителството и земеделието включва укрепване на почви, изграждане на подпорни стени и изолационни материали. В земеделието се използват като тежести за покриване на силажи или за създаване на временни конструкции. Освен това, старите гуми могат да се преработват в креативни и нестандартни приложения, като мебели, детски площадки и дизайнерски елементи.

Пиролизата на гумени отпадъци предоставя устойчива алтернатива за управление на отпадъците и намаляване на замърсяването. Получените продукти след подходящо облагородяване могат да намерят широко приложение в индустрията, строителството, земеделието и дори в дизайнерски решения, което доказва икономическата и екологичната целесъобразност на процеса.

# 4 Проектиране на мрежа за обратна логистика със стари гуми

Проектирането на мрежа за обратна логистика за управление на стари гуми включва няколко основни етапа:

- определяне на ключови участници, включително центрове за събиране на гуми (пунктове за рециклиране и ремонт), заводи за преработка (пиролиза, механично и термално рециклиране) и логистични оператори за транспортиране на отпадъците;
- оптимизация на транспортната мрежа чрез разработване на маршрути за ефективно събиране и доставка на гумите до преработвателните съоръжения, както и използване на софтуер за планиране на транспорт, който минимизира разходите и въглеродните емисии;
- интеграция на технологиите чрез инсталиране на съоръжения за пиролиза за обработка на големи количества гуми и въвеждане на системи за автоматизирано сортиране и обработка;
- проследимост и контрол чрез създаване на база данни за проследяване на движенията на гумите по цялата мрежа и въвеждане на метрики за измерване на ефективността (например количество обработени гуми, генерирани ресурси, намалени емисии);
- разширяване на мрежата чрез установяване на партньорства с производители, които да използват рециклирани материали в своите продукти, както и развитие на потребителска осведоменост чрез програми за връщане на стари гуми.

Оптимизацията на транспортната мрежа за управление на стари гуми е от съществено значение за ефективността на обратната логистика. Основната цел е да се намалят разходите, изминатите разстояния и въглеродните емисии, като същевременно се подобри капацитетът на транспортиране. Основен етап в оптимизацията е събирането на подробна

информация за местоположението на центровете за събиране, заводите за преработка и логистичните хъбове. Географски информационни системи се използват за картографиране на транспортната мрежа, като това позволява да се анализират маршрути и логистични възможности. Освен това данните за обемите на гумите и тяхната честота на транспортиране се използват за създаване на прогнозни модели.




**Фиг. 3.** Схема на мрежа за обратна логистика със стари гуми

Съвременните алгоритми за маршрутизиране, като алгоритъма на Дейкстра или модели за разпределение на товари (Vehicle Routing Problem, VRP), се използват за изчисляване на най-ефективните маршрути. Софтуери за транспортно управление, като Route4Me или SAP Transportation Management, предлагат възможности за автоматизирано планиране на маршрути, което минимизира транспортните разходи и времето за доставка. Включването на междинни пунктове за консолидиране на товари може значително да намали броя на курсовете и да оптимизира натоварването на транспортните средства. Групирането на товари от различни източници осигурява по-голяма ефективност на превоза. За оптимизацията е от съществено значение да се изберат подходящи транспортни средства. Превозните средства с висок капацитет или електрически камиони могат да намалят въглеродните емисии и оперативните разходи. Ефективността се повишава чрез анализ на съответствието между капацитета на камиона и обема на транспортираните гуми. [2, 8, 9]

Внедряването на автоматизирани системи за управление на транспорта и IoT устройства за проследяване в реално време позволяват адаптивно планиране на маршрути въз основа на данни за трафик или метеорологични условия. Тези технологии не само подобряват ефективността, но също така улесняват управлението на ресурсите. Оптимизацията на маршрутите и използването на превозни средства с ниски емисии спомагат за намаляване на въглеродния отпечатък на транспортната мрежа. Допълнително предимство е увеличаването на използването на алтернативни горива и възобновяеми енергийни източници. Симулационни инструменти се използват за прогнозиране на възможни сценарии и тестване на различни стратегии за транспортиране. Анализът на

„какво ако“ сценарии позволява да се идентифицират потенциални предизвикателства и да се разработят решения, преди да бъдат приложени в реални условия. Тези подходи представляват основата за изграждане на ефективна транспортна мрежа, която допринася за устойчивото управление на стари гуми.

# 5 Заключение

Обратната логистика за управление на стари гуми предлага възможности за устойчиво използване на ресурсите, намаляване на отпадъците и подобряване на екологичните показатели. Използването на иновативни технологии като пиролиза, механично и термално рециклиране, в съчетание с оптимизирани логистични мрежи, осигурява ефективно оползотворяване на гумите чрез повторна употреба, рециклиране и алтернативни приложения. Тези процеси не само намаляват натоварването върху природните ресурси, но и предоставят значителни икономически и социални ползи. Чрез интеграция, сътрудничество и иновации в управлението на тези потоци, компаниите могат да допринесат за глобалните усилия за устойчиво развитие. Внедряването на автоматизирани системи за управление, IoT устройства и софтуери за планиране на транспорт подобряват ефективността и проследимостта на логистичните процеси. Успешното управление на отпадъците от стари гуми доказва, че съвременните технологии и практики могат да трансформират екологичните предизвикателства в устойчиви решения, които допринасят за икономическо развитие и намаляване на екологичния отпечатък. [1, 2, 5, 7]

**ЛИТЕРАТУРА:**


[1] Макаревич, Е.А., Папин, А.В., Неведров, А.В., Игнатова, А.Ю. Переработка отработанных автомобильных шин и транспортерных лент. II Всероссийская молодежная научно-практическая конференция «Экологические проблемы промышленно развитых и ресурсодобывающих регионов: пути решения», 2017.

[2] Bazan, E., Jaber, M. Y., & Zanoni, S. (2016). A Review of Mathematical Inventory Models for Reverse Logistics and the Future of its Modeling: An Environmental Perspective. Applied Mathematical Modelling, 40(5-6), 4151–4178.

[3] Bernon, M., Cullen, J., 2007. An integrated approach to managing reverse logistics, International Journal of Logistics: Research and Applications, Vol. 10, pp. 41-56.

[4] Carter, C.R., Ellram, L.M., 1998. Reverse logistics: A review of the literature and framework for future investigation, Journal of Business Logistics, Vol. 19, pp. 85-102.

[5] Crainic, T. G., & Laporte, G. (1997). Planning Models for Freight Transportation. European Journal of Operational Research, 97(3), 409–438.

[6] Daaboul, J., Duigou, J., Penciuc, D., Eynard, B., 2013. Reverse Logistics: Network Design Based on Life Cycle Assessment. 20th Advances in Production Management Systems, United States, pp.450-460.

[7] Ramezani, R., Bashiri, M., Tavakkoli-Moghaddam, R., 2013. A new multi-objective stochastic model for a forward/reverse logistic network design with responsiveness and quality level. Applied Mathematical Modelling 37, pp. 328–344.

[8] SuPLight, 2012. Document Deliverable 1.5: SuPLight application scenarios. SuPLight, EU FP7 Project, N°263302.

[9] Thienen, S., Delesalle, P. et al., 2014. The hidden value in Reverse Logistics. Deloitte Consulting. Vlachos, D., & Dekker, R. (2003). Return Logistics in Closed-Loop Supply Chains. International Journal of Production Research, 41(5), 1021–1040.

# UNIVERSAL METALWORKING MACHINES FOR AUTO AND TRACTOR REPAIR WORKSHOPS*

**DIDIYA-KLARA A. GENCHEVA, ATANAS A. GENCHEV**

***ABSTRACT:*** *With the development of the automotive industry and the increasing need for efficient maintenance, auto and tractor repair workshops face growing challenges regarding speed and quality of repair activities. Universal metalworking machines that integrate functions such as grinding, milling, turning, and reaming are crucial for these workshops. These machines optimize workflow, save time and space, and enhance repair quality, making them ideal for environments where space and resources are limited. Specialized equipment, such as crankshaft grinding machines, cylinder boring and honing machines, surface grinders, and universal lathes, plays an essential role in ensuring the precision and durability of critical vehicle components. The patented universal metalworking machine, specifically designed for flat grinding and milling, offers a versatile solution tailored for auto and tractor workshops. Combining stability with precision, this machine provides an innovative approach to complex repair tasks. It also features safety mechanisms and user-friendly adjustments. Built with engineering solutions that minimize vibrations and enhance reliability, this universal machine represents a valuable investment in quality and long-term efficiency for modern auto repair workshops.*

***KEYWORDS:*** *universal metalworking machine, automotive repair, surface grinder, auto repair workshop, tractor repair*

***DOI: https://doi.org/10.46687/TTNR4598***

# УНИВЕРСАЛНИ МЕТАЛООБРАБОТВАЩИ МАШИНИ ЗА АВТОТРАКТОРНИ РАБОТИЛНИЦИ

**ДИДИЯ-КЛАРА А. ГЕНЧЕВА, АТАНАС А. ГЕНЧЕВ**

***АБСТРАКТ:*** *С развитието на автомобилната индустрия и нарастващата нужда от ефективна поддръжка, автотракторните работилници се изправят пред нови предизвикателства, свързани със скоростта и качеството на ремонтните дейности. Универсалните металообработващи машини, които комбинират функции като шлайфане, фрезоване, струговане и разстъргване, са от съществено значение за тези работилници. Те оптимизират работния процес, спестяват време и пространство и повишават качеството на ремонтите, което ги прави идеални за среди с ограничени ресурси. Специализираното оборудване, като машини за шлайфане на колянови валове, разстъргване и хонинговане на цилиндри, плоскошлифовъчни машини и универсални стругове, играе важна роля за осигуряване на прецизност и дълготрайност на критични компоненти на превозните средства. Патентованата универсална металорежеща машина, проектирана специално за плоско шлайфане и фрезоване, предлага гъвкаво решение, адаптирано за автотракторни работилници. Комбинирайки стабилност и прецизност, тази машина предоставя иновативен подход за сложни ремонтни задачи. Тя е снабдена с механизми за безопасност и удобни настройки. С инженерни решения, които намаляват вибрациите и гарантират надеждност, тази универсална машина представлява ценна инвестиция за качеството и дългосрочната ефективност на съвременните автосервизи.*

## 1 Въведение

С развитието на автомобилната индустрия и растящите нужди от ефективна поддръжка на автопарка, автотракторните работилници се изправят пред нови

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие МАТТЕХ 2024 – ФТН“

предизвикателства, свързани с бързината и качеството на ремонтните дейности. В тези работилници, където често се обслужват тежкотоварни превозни средства и земеделска техника, е от съществено значение да се разполага с оборудване, което да позволява изпълнението на широк спектър от задачи с висока прецизност и минимално време за настройка.

Металообработващите машини са сред основното оборудване в такива работилници. Те позволяват обработка на детайли от метал – от прецизни части на двигателя до различни компоненти на шасито и трансмисията. Въпреки разнообразието от операции, които трябва да се извършват, автотракторните работилници често имат ограничено пространство и ресурси. Поради тази причина съществува силна нужда от машини с универсални възможности – машини, които могат да комбинират функции за шлифоване, фрезоване, струговане и разстъргване в един корпус.

Универсалните металообработващи машини предоставят не само икономически, но и практични предимства. Те спестяват време и пространство, като позволяват на операторите бързо да превключват между различни операции, което увеличава производителността и гъвкавостта в работилницата. Тези машини са проектирани с акцент върху устойчивостта и лесната пренастройка, което ги прави идеални за средно и дребно серийно производство в автотракторните работилници. Именно универсалността на металообработващите машини дава възможност на работилниците да затворят цикъла на ремонтните дейности и да гарантират, че превозните средства са готови за експлоатация в най-кратък срок, без компромис с качеството на извършваните операции.

## 2 Металообработващи машини за автотракторни работилници

Машините за шлайфане на колянови валове са от основно значение при ремонта на автомобилните двигатели, тъй като коляновите валове са едни от най-сложните и скъпи компоненти. Тези валове поемат голямо натоварване и са подложени на износване, особено в зоните на основните и мотовилковите шийки. Затова възстановяването на първоначалните им геометрични параметри е от ключово значение за ефективността и надеждността на двигателя. Машините за шлайфане на колянови валове осигуряват прецизна обработка на износените лагери, като връщат валовете до стандартните размери. Те работят с висока точност, което позволява да се постигне идеално гладка повърхност, необходима за намаляване на триенето и осигуряване на дълготрайност на компонентите. В процеса на шлайфане детайлите се закрепват внимателно и се използват специални технологии за контрол на формата и диаметъра на обработваните повърхности. Машините осигуряват висока степен на автоматизация, което позволява по-лесно калибриране и минимизира човешките грешки. [2, 3, 4, 6]

При износването на цилиндрите в двигателите, причинено от постоянното триене с буталата и буталните пръстени, се налага прецизна работа с машини за разстъргване и хонинговане. Процесът започва с разстъргването, което подготвя цилиндрите до определен ремонтен размер. Това е ключово за постигането на правилен контакт между буталото и цилиндъра, а така също осигурява гладка база за следващата обработка. След разстъргването, хонинговащата глава оформя специфична винтова мрежа върху вътрешните стени на цилиндрите, която задържа слой масло, предпазвайки повърхностите от прекомерно износване. Този фино структуриран слой масло помага за поддържане на оптималната температура и смазочен слой между буталото и цилиндъра, като същевременно предотвратява нагряването. Тази комбинация от разстъргване и хонинговане

е особено важна за поддържане на цилиндровите стени в идеално състояние, удължавайки живота на двигателите и повишавайки тяхната ефективност.

Плоскошлифовъчните машини играят важна роля в поддръжката на цилиндровите глави и блокове, където е необходимо постигането на идеално равни уплътнителни повърхности (фиг. 1). При тези машини обработката се извършва върху големи плоски повърхности, което изисква стабилна настройка и прецизно водене на инструмента. Шлайфаните цилиндрови глави и блокове са от съществено значение, тъй като трябва да гарантират плътно уплътняване при съединенията, предотвратявайки течове на гориво, масло или охлаждаща течност. Плоскошлифовъчните машини осигуряват тази гладка и прецизна повърхност, която е ключова за правилната работа на двигателя. Те са оборудвани с различни типове шлифовъчни дискове, които могат да се настройват спрямо конкретните изисквания на детайлите, което прави тези машини идеални за автосервизи, които обслужват различни типове двигатели и компоненти.



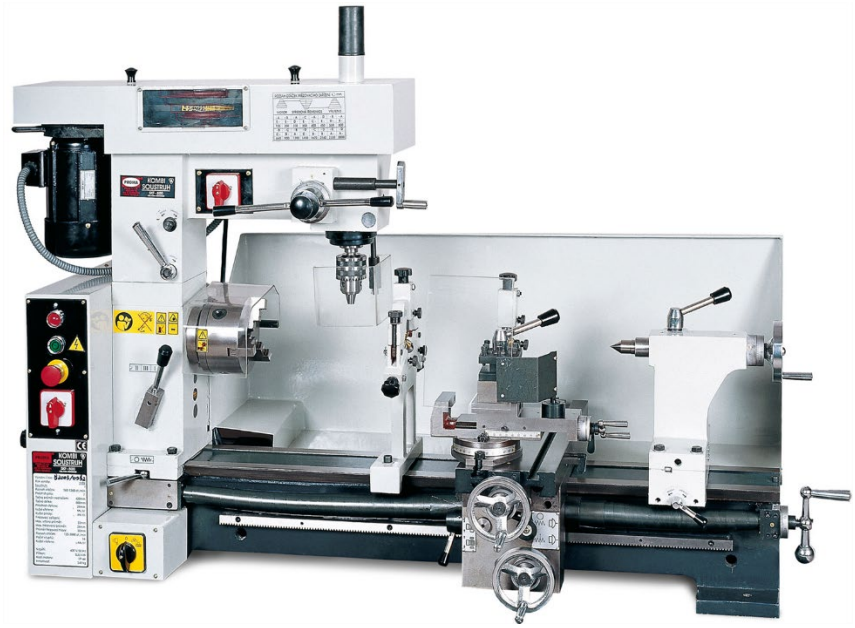

**Фиг. 1.** Плоскошлифовъчна машина MG1400

Универсалните стругове заемат особено място в арсенала на автотракторните работилници, тъй като са способни да обработват множество детайли с разнообразна форма и размери. Чрез тях се извършват важни операции като престъргване на спирачни дискове, барабани, както и обработка на други цилиндрични елементи в автомобила. Големите и стабилни стругове позволяват работа върху тежки детайли, като осигуряват точност и надеждност, докато по-малките настолни стругове са удобни за бързи и по-малки задачи. Универсалните стругове са изключително ценни за автосервизите, защото позволяват обработката на голям брой детайли на място, без необходимостта от външни услуги. Тази гъвкавост значително намалява времето за обслужване и разходите, като същевременно подобрява качеството на ремонтите.

## 3 Комбинирани металообработващи машини

В съвременните автотракторни работилници нараства необходимостта от универсални металообработващи машини, които съчетават множество функции в един уред. Тези комбинирани машини оптимизират пространството, намаляват разходите и повишават ефективността на работния процес. Такива могат да са например:

- **Комбинирани стругове с фрезова глава.** Пример за такава машина е комбинираният струг SKF-800 kombi, който съчетава струговане и фрезоване (фиг. 2). Той е оборудван със 7-степенна скоростна кутия, осигуряваща прецизност при работа;
- **Мултифункционални кръглошлифовъчни машини.** Машината CTG-500 комбинира кръглошлифовъчен шлайф и заточна функция. Тя е подходяща за вътрешно, външно и конусно шлайфане на детайли, както и за шлайфане на плоски, вертикални и наклонени повърхности и канали;
- **Универсални шмиргели с лентов шлайф.** Шмиргелът BERNARDO KSA 200 комбинира шлайфане и шлифоване, разполагащ с абразивен диск и безконечна шкурка под формата на лента. Тази комбинация позволява обработка на изделия от метал, дърво и полимери, идеална за повърхностно и контурно шлайфане.

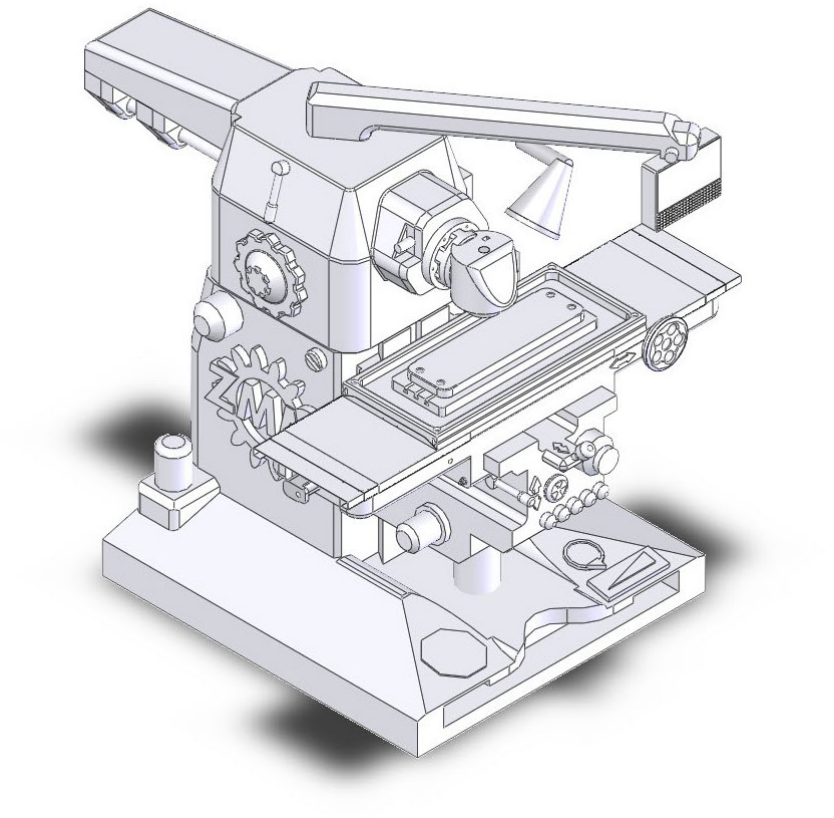


**Фиг. 2.** Комбиниран струг SKF-800

Използването на такива комбинирани машини в автотракторните работилници предоставя значителни предимства, като намаляване на времето за настройка, оптимизация на работното пространство и повишаване на производителността. Тези уреди позволяват на техниците да извършват разнообразни операции без необходимост от смяна на оборудването, което води до по-ефективен и икономичен работен процес.

## 4 Машината за извършване на плосък шлайф и фрезоване

Патентованата универсална металорежеща машина е иновация, която съчетава функционалностите на шлайфане и фрезоване на метални повърхнини, предназначена за автотракторни и други ремонтни работилници. Тя е защитена с патент за изобретение № 67648 B1 по заявка № 113403, публикуван в бюлетин № 202408.2 на 30.08.2024 от Патентно ведомство на Република България. Освен това, машината има и европейско свидетелство за промишлен дизайн от Службата за интелектуална собственост на Европейския съюз (EUIPO) с номер 008574826-0001, издадено на 13.06.2021 г., както и регистрация на полезен модел от Патентното ведомство на България, с рег. № 4174 U1, публикувана на 17.01.2022 г. Общ вид на машината е даден на фиг. 3. [1, 2]



**Фиг. 3.** Универсална металорежеща машина

Основната цел на изобретението е да осигури металорежеща машина, която извършва плоско шлайфане и фрезоване на метални повърхности, като същевременно притежава функции за прецизна обработка на метални детайли, предназначени за ремонтни дейности в автотракторни и други работилници, обслужващи транспортни средства. Машината разполага с конзола, седло, хоризонтален и вертикален шпиндел, както и работна маса с направляващи паралели по осите Z, Y и X. Тя е допълнително подсилена с чугунен фундамент и цифрово-програмно управление, което осигурява стабилност и прецизност. На чугунения фундамент е монтиран корпус, към който е закрепено завъртащо се тяло с шпинделен хобот и сменяема шпинделна глава, позволяваща закрепване на различни фрезери и шлифовъчни дискове. Работната маса е оборудвана със защитни щитове и може да бъде снабдена с електромагнитен държател за допълнителна стабилност на детайлите.

Машината е снабдена със стоп педал за аварийни ситуации и с педал с избираеми функции в зависимост от текущите операции. Завъртащото се тяло, изработено заедно с шпинделния хобот, осигурява максимална стабилност и прецизност, като в него е интегрирана степенна предавателна кутия. Преминаването между различните степени и избора на шпиндел се осъществява чрез завъртане на концентрични колела, монтирани върху тялото. Освен това, машината разполага с резервоар за охлаждаща течност, който е свързан с помпа, монтирана върху фундамента, за поддържане на подходяща температура при работа.

Всички ключови детайли на машината са изработени от чугун, за да се намалят вибрациите при работа и да се осигури стабилност. За безопасност фундаментът е закрепен към земята и заземен за защита от токов удар. Неподвижният корпус и фундаментът са

конструктивно интегрирани, но могат да се съединяват с винтове и фиксиращи щифтове, като между тях задължително има уплътняваща паста, предотвратяваща изтичането на охлаждаща течност. Вертикалните направляващи позволяват ръчно или електромеханично преместване на конзолата, на която са разположени повечето управляващи лостове и бутони. Седлото се движи по хоризонталните направляващи, а работната маса изпълнява движения по оста X. В режим на плосък шлайф с хоризонтален шпиндел масата може да извършва и бързи възвратно-постъпателни движения.

# 5 Заключение

Автотракторните работилници се нуждаят от ефективни и многофункционални металообработващи машини, за да отговорят на съвременните изисквания за бързина и качество на ремонтите. Универсалните машини, съчетаващи функции като шлайфане, фрезоване, струговане и разстъргване, осигуряват значителни предимства за тези работилници, където пространството и ресурсите често са ограничени. Внедряването на универсални машини оптимизира работния процес, намалява времето за обслужване и разходите, като същевременно подобрява качеството и дълготрайността на извършваните ремонти.

Специализираните машини, като тези за шлайфане на колянови валове, разстъргване и хонинговане на цилиндри, плоскошлифовъчни машини и универсални стругове, са съществена част от арсенала на всяка модерна автотракторна работилница. Те позволяват прецизно обработване на компонентите, което удължава експлоатационния живот на двигателите и гарантира безпроблемната им работа. Комбинираните металообработващи машини също играят ключова роля, като обединяват различни операции в един уред, което допълнително улеснява работата на операторите и оптимизира пространството в работилницата. [2, 3, 5, 8]

Патентованата универсална металорежеща машина предоставя иновативно решение за нуждите на автотракторните работилници, като обединява функциите на шлайфане и фрезоване, съчетавайки стабилност и прецизност. Тази машина не само предоставя възможност за прецизна обработка на детайли, но и осигурява безопасност и лесна настройка. Чрез конструктивни и инженерни решения, които намаляват вибрациите и гарантират надеждност, тя осигурява дългосрочна инвестиция в ефективността и качеството на ремонтните дейности в автотракторните работилници.

**ЛИТЕРАТУРА:**

[1] Патент за изобретение с рег. № 67648 B1, по заявка № 113403, публикуван в бюлетин № 202408.2 на 30.08.2024 от Патентно ведомство на Република България, наименование: Металорежеща машина

[2] Tsankov Ts., Konstantinova E. Equipment of autotractor workshops with machine tools. Scientific Conference with international participation MATTEH 2020, Conference proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 369-374.

[3] https://www.polymeta.bg/?v=982494d74c59

[4] https://www.koledzhikov.bg/

[5] https://intralink.bg/index.php/

[6] https://www.polymeta.bg/

[7] https://www.metalpack-bg.com/

[8] https://ks-metal.bg/

# MOST APPLICABLE HARDWARE TECHNOLOGIES AND MATERIALS FOR PHYSICAL PROTOTYPING*

**MARIELA L. ANTONOVA, STAMEN I. ANTONOV**

***ABSTRACT:*** *This paper reviewed the different types of 3D printer technology available in the consumer market, with a particular focus on printers that use plastic filament. It is gaven a brief introduction to other technologies, particularly printers that use liquid resin.*

***KEYWORDS:*** *3D print, design*

***DOI: https://doi.org/10.46687/FBUI9449***

The commonest type of 3D printer works with spools of plastic (called filament), which it melts and lays down to create objects. Others use lasers or projectors to harden light-sensitive resin. Still others either sinter powder or lay down binders to form objects from powder. The sheer number of technologies can be overwhelming. There is a lot of experimentation going on in the field at the moment, and hundreds of companies are developing new printers on what seems like a daily basis. The materials available have proliferated too.

## 1 Filament Printers

By far the commonest consumer-level 3D printing technology is fused filament deposition manufacturing, sometimes called FDM (which technically applies to just one manufacturer) or more generically FFF for fused filament fabrication. In general it is possible to named to these printers as filament 3D printers. These printers pull plastic filament off a spool, melt it, and lay down the melted plastic in a fine line, typically around 0.2 mm high and a few times as wide.

Figure 1 shows a typical filament printer, which would have a spool of filament next to it if it were running. It is labeled the common convention for naming the axes of a printer. The x axis here is left to right, the y axis is away, and the z axis is vertical. There are several different architectures of filament printers. [1, 3, 7, 8]

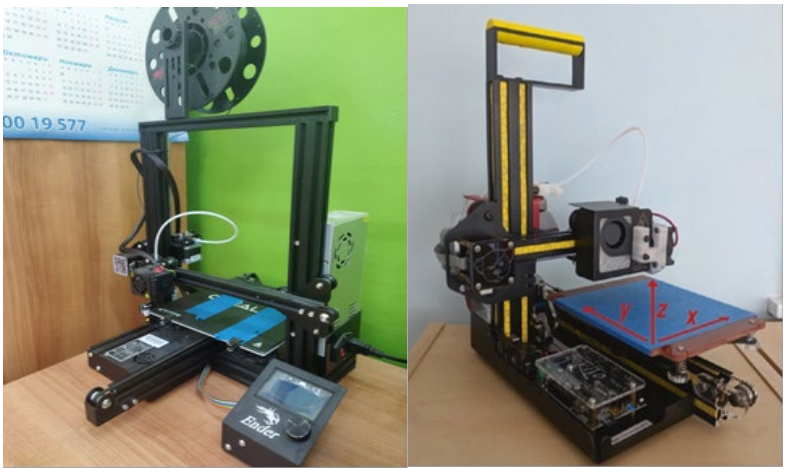



**Figure 1.** A typical consumer 3D printers

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие MATTEX 2024 – ФТН“

## 2 Parts of a Filament Printer

A filament printer is pretty simple - a common analogy is to be called a computerized hot glue gun. However, there are several critical parts that affect reliability, print quality, and what kinds of materials, can be used.

***1. Stepper Motors***

Consumer 3D printers usually have four or more stepper motors (Figure 2.), commonly called steppers. As the name implies, these are precise motors that move their shafts in predefined angular steps.

Typically, one motor drives each axis (sometimes two, on the vertical, or z, axis) by being coupled through pulleys to a belt or cable, or to a drive screw for an axis (often used for the z axis). Another motor drives the extruder gear. The steps per millimeter of the gears (how much an axis, or the filament, moves as the motor turns) is one of the things limiting how accurate a 3D printer can be, although it is not usually the principal limitation. Motors for 3D printers typically have 200 steps per revolution.

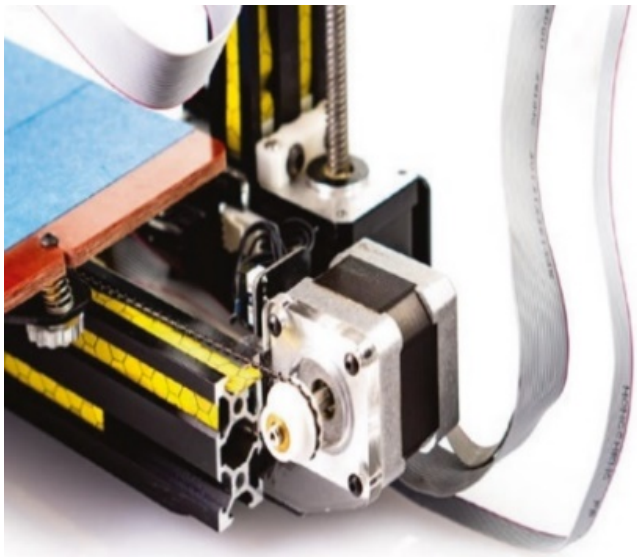


**Figure 2.** Stepper motor

***2. Control***

3D printers are controlled by microcontrollers. Many of these use a processor that is an adaptation or descendant of the Arduino open source microcontroller standard. Nowdays, many consumer printers still use open-loop control, meaning that they do not have sensors checking that the printer is running as planned, except for sensors monitoring temperatures of the print bed and extruder.

Most printers do not need to be tethered to a computer. If they are, it is to feed the commands to create a model, not to directly control the motors and temperatures. A printer runs some sort of firmware on its controller to do that lowlevel control. Firmware is just software that is used to control a machine.

***3. Build Platform***

Prints are created on a flat platform, interchangeably referred to as the print bed or print platform. Most are equipped with a heater, which allows to be used more materials. Depending on the printer design, the print bed may move in one or two directions, or not at all.

***4. Extruder***

The extruder is the part of the printer that melts and moves the filament. It is made up of several parts. We have already mentioned the extruder drive gear and its motor, which push the filament into the hot end. The hot end in turn is comprised of a heater, a nozzle, and a sensor (called a thermistor) to sense how hot the nozzle is. The nozzles are very precise. They typically measure 0.35–0.50 mm in diameter and can be made entirely of metal, or they may be lined with a material called polytetrafluoroethylene (PTFE) to minimize jamming. Allmetal hot ends are required for printing many materials. The hot end includes a heating element and a sensor to regulate temperature, a thermal transition zone (often with a heatsink and fan on the cold end), and a nozzle that is usually made of brass. Recently, hardened-steel and ruby-tipped nozzles have appeared - some filaments are very abrasive, and these are more resistant to abrasion. Figure 3. is a close-up of a nozzle.

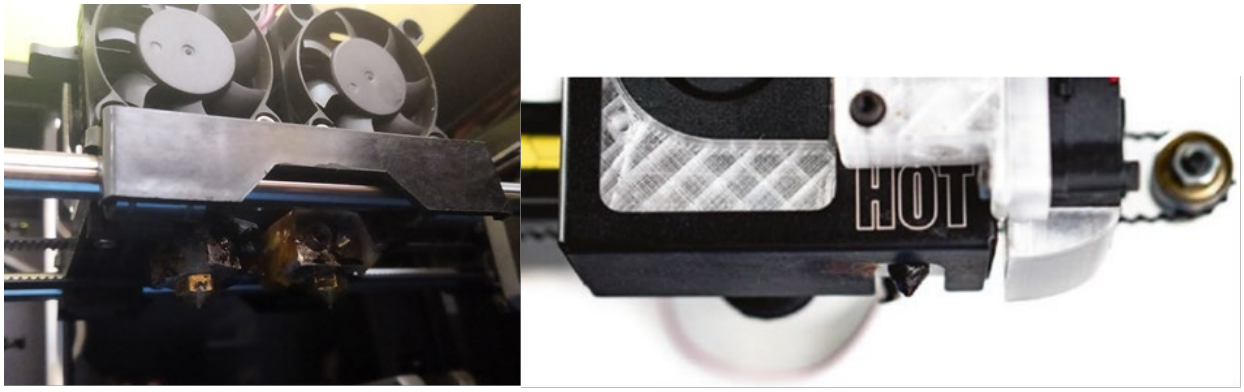



**Figure 3.** Extruders (Nozzle)

***5. How Printing Works***

First, filament has to be pulled from the spool into the printer, usually with a gear driven by a stepper motor. There are a variety of geometries for this. Sometimes a gear is right next to where the plastic will be melted (the hot end), and sometimes it is separated by a flexible tube, called a Bowden tube. Extruders with a gear pulling in filament without an intermediary tube are called direct-drive extruders. Figure 4 shows the drive gear on a Bowden-style printer.

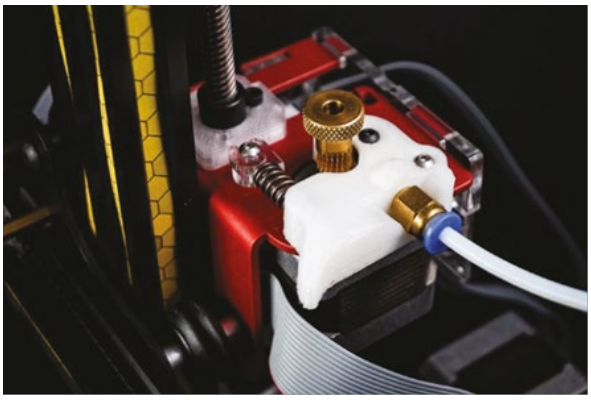


**Figure 4.** Extruder gear on a printer with a Bowden tube

Some manufacturers works with direct-drive extruders; many have moved now to some form of Bowden extruder. The main advantage of having the gear right at the extruder is simplicity,

though it also means that the motor is being carried around with the hot end. This can in turn mean slower printing and other issues. A print starts with a 3D CAD virtual model, which is turned into a series of commands for the stepper motor and the temperature controls. Once those commands are loaded onto the printer, via cable, SD card, or wireless connection, the printer will first heat up the nozzle and the platform (if it has a heater). Once everything is up to temperature and the printer performs whatever self-checks it is capable of, printing begins. [4, 5, 9]

The first layer of the print has to stick well to the platform. There are various techniques for ensuring this. Some involve software settings, and others are related to using the correct platform surface for the material which are printing. Assuming that the print sticks, as a layer builds up, there are areas that do and do not have plastic within one layer. This means that the nozzle will be extruding during some parts of the layer, and not during others.

Suppose that it have to printing something that had a part sticking out, like cantilever with tilt angle. As it builts up the print layer by layer, it would eventually reach the first layer of the fundament of the cantilever. But as it is laided out plastic to form the first layer, it would just fall down since there was nothing to support it. To address problems like that, it is used support material. Support is extra material that is added to the model to allow it to print a layer at a time. Figure 5 shows a print with support. Printers can handle overhangs of about 45 degrees - the subsequent layers overlap a bit and allow to print these moderate slopes. Printers can also bridge over open areas. If has to be printing a hollow cube, for instance, the top will be over open space, but supported on all four sides.



**Figure 5.** Print with support

***6. Filament Choices***

There are many choices for 3D printer filament. The quality of the 3D printing filament will make the difference between failed print and a well-printed product model.

By far the commonest filament material is PLA, polylactic acid. It is a biodegradable, corn-based (sometimes sugarcane-based) plastic. It melts at a relatively low temperature and will stick to a variety of platform surfaces. PLA usually requires an extruder temperature of around 210 degrees. One of the reasons it is so popular is that PLA does not require a heated platform. Low-cost printers usually suggest that to put blue painter'stape (pad). The downside of PLA is that, well, it melts at a low temperature. PLA is a very good material for quick prototypes, student projects, and the like. There are specialty filled PLA mixes that contain stone, wood, metal, or glow-in-the-dark fine particles. Objects made with this can look surprisingly like they are made of the respective substance, with a bit of polishing. However, these mixes are hard on nozzles and tend to abrade them; hardened or ruby nozzles can get around this problem.

PET (polyethylene terephthalate) is a very common plastic in the non-3D printing world, used for water bottles and many other things. PETG is a type of PET that is often used in 3D

printing; some varieties aretranslucent. It needs an extruder temperature higher than PLA—around 230–260 C.

Acrylonitrile butadiene styrene (ABS) is the plastic used for LEGO bricks, among many other things. It is durable and far less vulnerable to warping in warm temperatures. The flip side of that is that it requires a high nozzle temperature—from about 220–260 C. A heated bed is also an absolute requirement for ABS, at 90–110 C.

Nylon is a strong printing material, which also requires a high temperature of around 240–270 C. The biggest challenge with nylon, other than the high extruder temperature, is that it does not want to stick to anything.

Dissolvable Support. Some printers have more than one extruder. One reason for buying such a machine is to allow the use of support material that can be dissolved away, either with water or other chemicals.

Resin Printers: SLA, DLP, and LCD.

The consumer resin printer market has been coming into its own recently with a great deal of experimentation. There are three types of resin printer on the market right now: stereolithography (SLA), Digital Light Processing (DLP), and a variation of DLP that uses a liquid-crystal mask (LCD) with an LED illumination source. Laser SLA printers use optics to move around an ultraviolet laser spot to cure UV-curable resin within one layer at a time. This layer is peeled off the bottom of a tank (or dropped down into the tank, and then the next layer is cured, and so on. DLP, on the other hand, uses a projector to cure a whole layer at a time; LCD printers are similar but use an LCD mask illuminated by LEDs to illuminate a layer at a time. Some low-cost resin printers use a modified cell phone screen in place of the projector.

Resin 3D printers have an ability to create far finer detail than filament-based printers. A resin printer is limited by its laser spot size (SLA) or the pixel size (DLP and LCD). This means that resin prints can have very smooth surfaces relative to those created by a printer using filament. Resin printers still need to create support, but the nature of the support is a little different. Typical printers are “bottom-up” and build a layer at a time, which is peeled off the bottom of a tray.

Printers that use a laser to cure resin use a series of coordinates that the laser spot moves through, philosophically similar to the commands thatcontrol a filament-based printer (fig. 6). They can generally move the laser spot much faster than a printer can move a heated nozzle, though. Although most have proprietary software, some of them have adapted software developed for filament printing. Printers that use a projector need a series of 2D images, one for each layer. Some of these printers have an HDMI port as an input, and their software treats the printer as a second monitor on hich it displays those images.

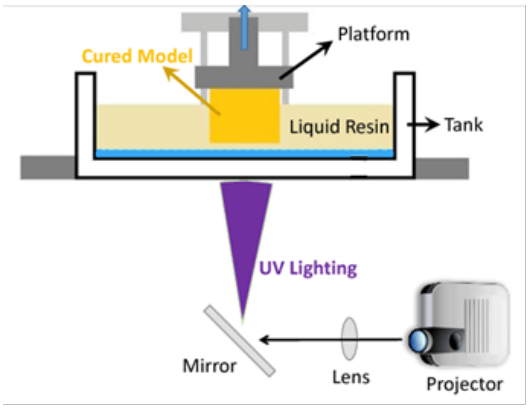



**Figure 6.** Resin print in progress

Post-processing is required on SLA prints, and typically involves washing off the print with isopropyl alcohol to remove uncured resin and exposing the print to UV light to ensure that the resin is fully cured.

Other Technologies. The overall field of 3D printing has been expanding in many different directions.

One of the oldest technologies in this space is selective laser sintering (SLS). Typically, a very fine powder is spread on a build platform, and a laser is used to sinter the powder together. More and more powder is added as the print grows. SLS can be used to make very fine, detailed prints. SLS prints do not need support, because the unfused powder acts as a support. However, the powder is very fine and SLS is an expensive technology.

Many machines that print metal use a process called direct metal laser sintering (DMLS), which is the SLS process used for metals. Metal powder has to be worked in an inert atmosphere to prevent fires, so DMLS machines are very expensive since they need to be completely enclosed and filled with an inert gas. Other processes like selective laser melting (SLM) and electron beam melting (EBM) use even higher power to more fully fuse metal powder. [2, 6]

# 3 Conclusion.

In the last ten years or so, 3D printers have gone from being large pieces of industrial equipment to hobbyist novelties, to classroom staples. There are many different 3D printers, but fundamentally they all create an object by building up one layer at a time on some sort of platform. The basic idea of 3D printing (or additive manufacturing) is that it is create objects by building them up one layer at a time. The components, a product of 3D print technologies, can be used for research purposes, for tests or for direct working use in machines and mechanisms.

**REFERENCES:**

[1] Благовест Банков, Изследване на възможностите за използване на технологии за 3D печат в логистичното осигуряване, Научна конференция „Логистиката и обществените системи” - 2023 г. Велико Търново, с. 215 - 224, ISSN 2367-7902.

[2] Благовест Банков, Ванко Ганев, Изследване на движението на проектил на боеприпас 7.62х54 във водна среда, Научна конференция „Актуални проблеми на сигурността”, Велико Търново 2023 г, с.1511 - 1516, ISSN 2367-7473.

[3] Благовест Банков, Росен Лазаров, 3D технологии и проектиране на сложни елементи от въоръжението, Научна конференция „Актуални проблеми на сигурността“, Велико Търново 2019, с.112-116, ISSN 2367-7475.

[4] Лалев Х. Л., Цанков Ц. С., Георгиева Ц. Л. 3D сканиране с Kinect for Windows. Международна научна конференция УНИТЕХ’16, Габрово, 2016, ISSN 1313-230X.

[5] Лалев Х. Л., Цанков Ц. С., Георгиева Ц. Л. Приложение на компютърното зрение в системите за ревърс инженеринг. Научна конференция MATTEX 2016, Шумен, 2016, ISSN 1314-3921.

[6] Antonov S.I., Izsledvane na prilozhenieto na CAD/CAM/CAE sistemite i tehnologiite za barzo prototipirane pri proektiraneto na komponenti na tehnicheskite sistemi, Shumen, 2021g., ISBN 978-619-7531-31-2.

[7] Brunet P, Hoffmann C, Roller D, CAD Tools and Algorithms for Product Design, Springer-Verlag Berlin Heidelberg, 2000, ISBN 978-3-642-08548-2.

[8] Horvath J, Cameron R, Mastering 3D Printing, Pasadena, ISBN: 978-1-4842-5841-5.

[9] Grzegorzewski P, Soft Modeling in Industrial Manufacturing, ISBN 978-3-030-03200-5.

# CALCULATION AND SELECTION OF SOME BASIC MACHINE ELEMENTS*

**MARIELA L. ANTONOVA, STAMEN I. ANTONOV**

***ABSTRACT:*** *Machines and mechanisms are made up of machine elements, united in nodes and groups. Most of them are found in all machines and mechanisms and have the same functions. The subject of consideration in the article will be fixed axes and straight shafts.*

***KEYWORDS:*** *machine elements, mechanisms, construction*

***DOI: https://doi.org/10.46687/LVMB8001***

Axles and shafts are generally cylindrical bodies of constant or variable cross-section and serve most often to secure the associated rotating machine elements.

The following distinction is made between axles and shafts in mechanical engineering. The axles merely support the machine elements attached to them, whereby they themselves may or may not participate in the rotary motion. The shafts, in addition to supporting the elements attached to them, also transmit torque. According to these definitions, axes will be calculated mainly in bending and very short axes in shear, while shafts will be calculated mainly in torsion and bending (for long shafts) or in torsion and shear (for short shafts). [1, 2, 4, 6, 9, 10]

Those parts of the axles and shafts with which they touch their supports are called necks or heels. The supports themselves are called bearings.

The structural form of the axles and shafts is determined both by the loading of the transmitted forces and moments, and also by the manufacturing and assembly technologies of the related details.

Shafts are divided into the following types:

- Straight shafts;
- Crankshafts;
- Torsion shafts;
- Articulated-telescopic shafts;
- Flexible shafts.

Axes are divided into:

- Immobile;
- Rotating.

Only fixed axes and straight shafts will be considered in the article. Their relationship with the elements attached to them largely dictates their structural form. The connection point in the axle or shaft must be shaped to allow the transmission of forces and moments while minimizing stress concentrations. For this purpose, sharp transitions from one diameter to another, cutting threads, making channels, grooves, etc., should be avoided in busy areas. similar. Fixing of machine elements connected to the axle or shaft is not done with locking screws.

When two or more elements with a press assembly are mounted on one side on the axis or shaft, steps of different diameters must be made on the shaft or axis, with the innermost step being made with the largest diameter, so that the holes of the parts can to pass freely to the place of their connection.

* Докладът е частично финансиран по проект № РД-08-110/31.01.2024 „Научна конференция с международно участие MATTEX 2024 – ФТН“

The diameters of all places on the shaft or axle where parts are assembled and which must be made with some accuracy are selected from the standard series of diameters so that gauges may be used in making them for convenience and ease measurement.

Axles and shafts are made of steel, and more recently of high-strength nodular cast iron. The choice of the material is made in view of the strength and deformation requirements, as well as the possibility of hardening. In general mechanical engineering, when heat treatment is not required, ordinary carbon steels C4, C5, C6 are most often used, and when greater strength is required, alloy steels such as 40X, 40XH, 40XHMA, 30XГT, etc. are used.

# 1 Calculating axles

## 1.1. Strength calculation

The axles serve to support the elements connected to them, and according to whether or not they participate in the rotary movement, they are fixed or rotating. For example, the axles of crane wheels and bicycles are stationary. The axles of railway wagons are movable and rotate together with the fixed wheels connected to them. Fixed axes are acted upon by forces transverse to their geometric axis, which may be constant or variable in magnitude, but almost always with a constant direction. Rotating axes are loaded in bilateral (alternating sign) bending, because even when they are subjected to constant direction forces, with one complete rotation of the axis, the peripheral threads go from tension to compression and vice versa. As a result of the friction in the bearings, the axle will also be loaded in torsion, which can be neglected due to the small frictional forces.

The size and type of load, as well as the shape and material from which it is made, are decisive for determining the dimensions of the axle.

Starting from the condition of equal bending strength (equal maximum bending stress) in each section of the solid axis, which will ensure the least weight of the axis, we will be able to write (Fig. 1).

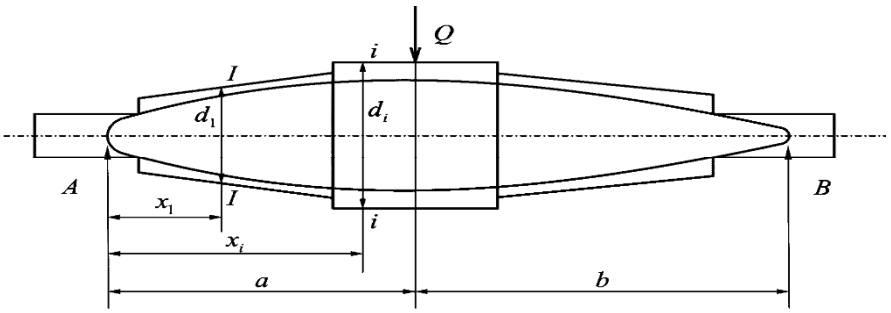



Fig. 1. Axis with equal bending strength

for section $I - I$: $M_{or1} = A \ X_1 = \frac{\pi}{32} d_1^3 \sigma_{or}$,

for section $i - i$: $M_{ori} = A \ X_i = \frac{\pi}{32} d_i^3 \sigma_{or}$,

whence by eliminating $\sigma_{oz}$, result: $d_i = d_1 \sqrt[3]{\frac{x_i}{x_1}}$.

This expression allows the diameter of any section of the axis to be determined if the diameter of at least one section is known. From the last expression it is also seen that the theoretical form of such an axis will be a rotational cubic paraboloid.

In order to simplify the construction of the axis, in practice the theoretically found shape of a body of uniform bending strength is usually ignored, and the rotating cubic paraboloid is replaced by cones or cylinders of different diameters whose contours best fit the contour of the paraboloid. At the same time, in order to reduce to a possible minimum the concentration of stresses in the places of a sudden (sudden) change in diameter imposed by design or technological considerations, the transitions from one diameter to the other are made with smooth roundings.

For the bending stress in a given section with axis diameter d, we can write:

$$\sigma_{or} = \frac{M_{or}}{W_{or}} = \frac{32M_{or}}{\pi d^3} \leq [\sigma_{or}],$$

where Mor is the maximum bending moment for a given step of constant diameter, and Wor is the resisting bending moment for the corresponding section about the axis.

When axes are stationary and loaded with dynamic (sign-changing) forces, the shape of the axis is usually determined in advance for structural or technological reasons. Bending moments are calculated from the forces applied to the axis for the individual sections and then a bending check is made for the individual sections of the axis. Allowable bending stresses are given in tables and reference books. [3, 7, 8]

For a symmetrical cycle, which is typical of rotating axes, the stresses are calculated using the formula:

$$\sigma_{max} = \frac{M_{or}}{W_{or}}.$$

If the voltage changes in a pulsating cycle:

$$\sigma_m = \sigma_a = \frac{\sigma_{max}}{2}$$

As a general rule, higher strength steels are more sensitive to stress than lower strength steels. It follows that when little safety is obtained for a given section of axle whose shape creates a concentration of stress, it can be increased usually not by using steel of greater strength, but by changing the shape of the axle. It should be borne in mind that the sharper the transition from one section to another, the greater the stress concentration will be. Therefore, the transition of the axle profile from smaller to larger diameter should be gradual, with good roundness, with an arc touching the smaller diameter (Fig. 2).

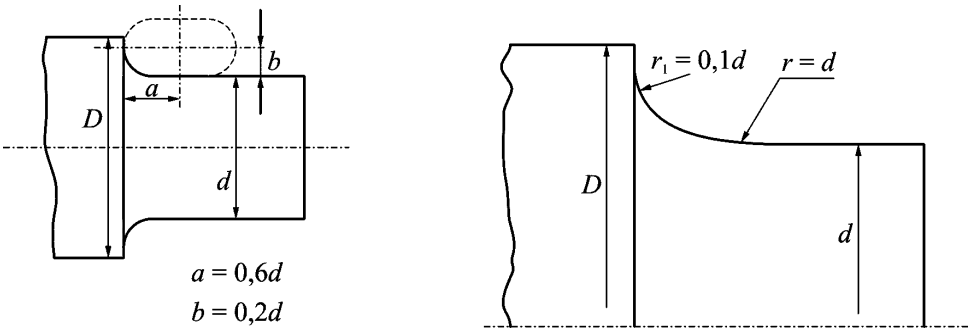



Fig. 2. Shapes of the transition curve instead of stress concentration

### 1.2. Deformation calculation

With the axis of strength calculated in this way, we are not sure whether under the action of the external forces applied to it, it will not be deformed so much that the sagging will exceed the prescribed deformations. On the other hand, the sag will cause the journal axes to tilt relative to the bearing axes, and if the tilt is greater than the clearance between the journal and the bearing shell allows, a very uneven pressure distribution will result, causing severe heating and jamming in the bearing (fig. 2).

In the technical literature, it is common to prescribe that the largest sag of the axis (shaft) should not exceed 0,0002 до 0,0003 ($f = (0{,}0002…0{,}0003)l$) from the inter-bearing distance. It is also accepted that the largest permissible tilt of the geometric axis of the axis relative to the geometric axis of the bearing does not exceed 0.001 for sliding and 0.01 for radial ball bearings. These values are considered indicative, since the permissible tilt of the axle neck in the bearing depends on both the bearing clearance and the length of the bearing shell, the stiffness of the bearing mount, etc. and should be checked on a case-by-case basis.

To determine the amount of sag, Moore's method of graphically determining the elastic line of the axis is best applied, which will be discussed further, since it is also used in calculating shafts.

## 2 Calculation of straight shafts

Shafts are usually calculated for strength according to their geometric shape. Often times, however, especially in cases where machine elements (gears, pulleys, etc.) are mounted on the fast-rotating shafts, for the correct operation of these elements, the deformations of the shaft under the action of the forces applied to it and of the transmissions are also required torque not to exceed predetermined values. Such shafts are additionally calculated based on the permissible bending and twisting deformations.

Fast rotating shafts must also be checked at the so-called critical revolutions, i.e. that the revolutions of the shaft do not coincide with or are not multiples of the revolutions corresponding to the natural oscillations of the system, in order to avoid resonance.

### 2.1. Calculation of luminance straight shafts

By definition, the shaft is a machine element that transmits torque and which, under the action of external forces transverse to its geometric axis, is almost always subjected to bending. It follows that a given section of the shaft will experience both bending and torsional stresses at the same time.

If in a given section of the shaft with a diameter "d", the bending moment "Mor", which occurred under the action of external forces transverse to its geometric axis, and the transmitted torque "Md" are known, then for the bending and twisting stresses in this section will can be recorded:

$$\sigma_{or} = \frac{M_{or}}{W_{or}} = \frac{32M_{or}}{\pi d^3}$$

$$\tau_{yc} = \frac{Md}{W_c} = \frac{16Md}{\pi d^3} = \frac{Md}{2W_{or}}.$$

For the magnitude of the equivalent (resultant, reduced) stress in the shaft section, there are so-called strength theories. For example, according to the fourth strength theory, the equivalent stress is determined by the formula:

$$\sigma_{EKB}^{IV} = \sqrt{(\sigma_{OI})^2 + 3(\tau_{CP})^2} \le [\sigma_{OI}]$$

In the last expression the values for the allowable stress depend $[\sigma_{o2}]$ both on the material of the shaft and on its loading regime and are tabulated.

When keyways or splined connections are cut on the shaft, the bearing section is reduced and also the bending and twisting moments of resistance will be smaller than those corresponding to the outer diameter "d"of the shaft.

When we do not know the forces acting transversely to the axis of the shaft, or when the bending moment caused by these forces is small compared to the torque that the shaft transmits (as is the case with shafts from gearboxes and reducers), the shaft is calculated seems to be loaded only in torsion.

In such cases, for a given section with diameter d of the shaft, we can write":

$$\tau_{yC} = \frac{M_{yC}}{W_C} = \frac{Md}{W_C} = \frac{16Md}{\pi d^3} \le [\tau_{yC}],$$

from where we determine the diameter of the section:

$$d = \sqrt[3]{\frac{16Md}{\pi[\tau_{yC}]}}.$$

If in the last expression instead of the torque "Md"we enter the power "N"transmitted by the shaft and assuming that the power is equal to the torque by the angular velocity, we can write:

$$N = Md.\omega; \quad N = Md.\frac{\pi.n}{30}.\frac{1}{1000}[kW]$$

$$Md = 9554\frac{N}{n},$$

where N is the set power in kW;
n – shaft revolutions per minute;
Md - the requested torque in N.m.

**2.2. Calculation of straight shafts of deformation**

Often, in addition to its strength, the size of the deformations to which it is subjected during operation is decisive for the sizing of a shaft. These deformations are of two types: sagging under the action of forces directed transversely to the geometric axis of the shaft, and twisting under the action of torque transmitted by the shaft. The magnitude of bending deformations - the so-called sag of the shaft is more important for the regular operation of the machine, since it can lead to incorrect operation of the elements connected to the shaft, such as bevel gears, bearings, etc. The following norms have been experimentally established for the permissible sag of the shaft: for gear wheels, the size of the sag of the shaft in the place of attachment of the wheels should not exceed 0.01 to 0.03 of the engagement module; for an induction motor to work properly, its maximum shaft sag should not exceed 0.1 of the motor's air space.

Finding the shaft sag line boils down to solving the differential equation of its elastic line:

$$W'' = \frac{M_{or}}{JE},$$

where Mor is the bending moment of the applied external forces;

J - axial moment of inertia for the corresponding section of the shaft;

E - the modulus of linear deformation of the material from which the shaft is made.

Usually Mor/J is a discontinuous function of x and plotting the shaft sag line is done graphically by Moore's method.

The elastic line of a shaft of constant cross-section loaded by external bending forces is considered as a curved line that is inscribed in the chain polygon obtained by the fictitious loading of the same shaft with a continuous load corresponding to its moment area at pole distance $H = EJ$.

To determine the amount of shaft sag, the diameter of which remains constant, proceed as shown in fig.3.

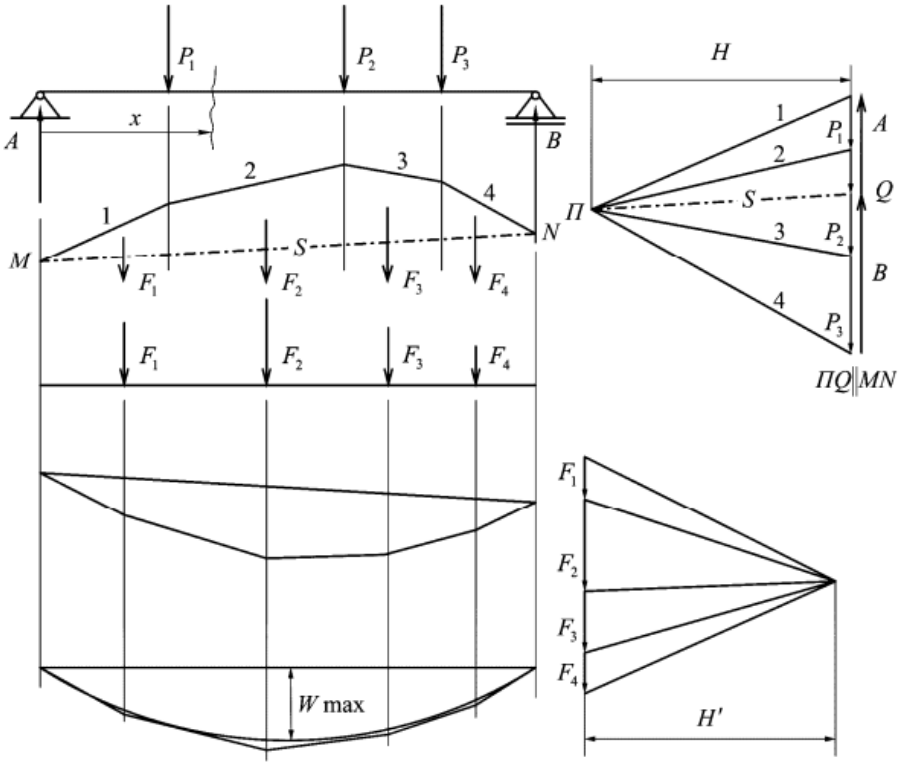



Fig. 3. Graphical determination of straight shaft sag by Moore's method

1. A length scale is selected: 1cm = *a* cm and the shaft is drawn. Force scale is selected: 1 cm = б *kN* and we draw the forces acting on it.

2. An arbitrary but convenient pole distance H is chosen and the force and chain polygons are drawn according to the forces acting on the shaft. The support reactions are determined.

3. The chain polygon defines the bending moment diagram. Thus for an arbitrary section "x"of the shaft

$$M_{or}^{x} = W^{x} a.б.H \ [Nm].$$

4. The same shaft is considered under continuous load from the moment diagram, which is decomposed into separate figures, at the center of gravity of each of which will act, the so-called area force - F.

The following scale is defined for area forces 1 cm = d N/$m^2$ with an arbitrarily chosen pole distance H` and draw the force and chain polygons for the fictitious load. The sides of the chain polygon will be tangents to the elastic line of the shaft, where the points of contact will lie on the continuation of the vertical sides of the areas with which the shaft is thought to be loaded.

From the thus obtained elastic line, the maximum deflection *Wmax* in millimeters is measured. But since the pole distance *H'* is chosen arbitrarily and not equal to *EJ,* it is *EJ/ H`d* times less, i.e. in the drawing the sag is *EJ/H`d* times greater than in reality. On the other hand, the shaft is drawn a times smaller, due to which its sag is also a times less. Considering the above, for the calculation of the sag, the expression is obtained

$$f_{\max} = W_{\max} .a \frac{H'.d}{E.J} [m]$$

Shaft sag cannot be reduced by selecting higher grade steels because the linear strain modulus *E* for plain and high grade steels is nearly the same. From this it follows directly that if the size of the deformation obtained under the action of forces transverse to its geometric axis is decisive for the dimensioning of the shaft, the shaft must be made of ordinary carbon steel, since this steel is cheaper.

Shaft sag can only be reduced by increasing its diameter, or by locating the machine parts attached to the shaft as close as possible to the bearings (gears, pulleys, clutches, etc.), or by making these parts as small as possible own weight.

Another type of deformation that the shaft will experience as a result of the transmission of torque Md is torsional deformation. It is determined by the magnitude of the twist angle

$$\max \theta = \frac{M_{yC}}{G.J_C} \le [\theta]; \quad \frac{32M_{yC}}{G\ \pi d^3} \le [\theta];$$

$$d \ge \sqrt[4]{\frac{32M_{yC}}{\pi.G\ [\theta]}}; \qquad d \ge \sqrt[4]{\frac{5760M_{yC}}{\pi^2 G\ [\theta]^\circ}}.$$

## 3 Conclusion

Machine elements is one of the fundamental engineering disciplines, where the theory, calculation and construction of machine components, elements and assemblies with general engineering purpose are studied.Mechanical engineering is the basis for the creation and multiplication of material goods and hence for raising the standard of living of people. This is because without productive machines there is no production.

The production of Bulgarian machines from the total scale of the market is about 30% and this has its logical explanation. "The mechanical engineering industry in Bulgaria, due to its historical specialization, is largely limited to the production of conventional lathes, CNC lathes, band sawing machines, drilling machines, milling machines and multi-operational woodworking machines. This is one of the structural factors determining the market share, since most of the other machines are only available from foreign manufacturers. [5, 11, 12]

**REFERENCES:**

[1] Ангелов, Г., Машинни елементи, София, Техника, 1972.

[2] Арнаудов, К. Б., И. Димитров, П. Йорданов, Л. Лефтеров. Машинни елементи. София, Техника, 1980.

[3] Балтаджиев, А., Атанасов, Цв. Машинни елементи I и II ч. (пособие за курсови проекти), Технически университет- Варна, 2009.

[4] Банков, Б. Изследване на възможностите за използване на технологии за 3D печат в логистичното осигуряване. Научна конференция „Логистиката и обществените системи" - 2023 г. Велико Търново, с. 215 - 224, ISSN 2367-7902

[5] Банков, Б., Ганев, В. Изследване на движението на проектил на боеприпас 7.62х54 във водна среда. Научна конференция „Актуални проблеми на сигурността", Велико Търново 2023 г, с.1511 - 1516, ISSN 2367-7473

[6] Банков, Б., Лазаров, Р. 3D технологии и проектиране на сложни елементи от въоръжението. Научна конференция „Актуални проблеми на сигурността", Велико Търново 2019, с.112-116, ISSN 2367-7475

[7] Димчев, Г., Панайотов, П. Машинни елементи. София, Нови знания,2008.

[8] Лефтеров, П., И. П. Димитров, П. В. Йорданов, Е. Х. Ганчев. Машинни елементи. София,Техника, 1994.

[9] Попов, М. Машинни елементи. София, Техника, 1989.

[10] Христов, Д., Г. Петков, Н. Чавушан, С. Начев, М. Проданов. Пресмятане и конструиране на машинни елементи. София, Техника, 1967.

[11] Цанков, Ц. С., Александрова, А., Спасова, М. Полезен модел на ремарке за мотоблок. Научна конференция с международно участие MATTEX 2018, Шумен, 2018, ISSN 1314-3921, с. 203-209.

[12] Цанков, Ц., Станиславова, С. Способ за подбуждане на интерес у учениците в прогимназиален етап, към знания за якостта на материалите. Сборник статии от XIII международна научно-практическа конференция „Инновации в технологиях и образовании", ч. 4, филиал на КузГТУ в г. Белово, 2020, ISBN 978-5-00137-065-9, с. 196-201.

# СЪДЪРЖАНИЕ

АРХИТЕКТУРА НА ИНТЕГРИРАНА СИСТЕМА С АСИНХРОННИ ПОТРЕБИТЕЛСКИ ВХОДОВЕ В ОПЕРАЦИОННА СРЕДА, ИЗГРАЖДАЩА МОТИВИРАЩО И НЕСТРЕСОВО ОБКРЪЖЕНИЕ, Валентин Т. Атанасов, Тихомир С. Трифонов ..... 3

ХАРДУЕРНИ ПЛАТФОРМИ, СЪВМЕСТИМИ С ЕЗИКА ЗА ПРОГРАМИРАНЕ P4, Мустафа Б. Узун, Валентин Т. Атанасов ..... 8

ИЗСЛЕДВАНЕ НА МАШИННО ОБУЧЕНИЕ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ВЪВ ВИДЕОНАБЛЮДЕНИЕТО, Силвия Х. Николова ..... 17

СОФТУЕРНА ОБРАБОТКА НА АУДИО СИГНАЛИ В ЦИФРОВА АУДИО РАБОТНА СТАНЦИЯ STUDIO ONE ЧРЕЗ ЕФЕКТ ПРИСТАВКИ, Даниел Р. Денев, Александра П. Дочева ..... 23

АРХИТЕКТУРА НА СОФТУЕРНО-ДЕФИНИРАНА МРЕЖА, БАЗИРАНА НА ПРОГРАМИРУЕМИ ПРОТОКОЛНО-НЕЗАВИСИМИ ПАКЕТНИ ПРОЦЕСОРИ P4, Мустафа Б. Узун, Валентин Т. Атанасов ..... 39

МОДЕЛ НА АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ПРОЦЕСИ В ОБРАЗОВАТЕЛНАТА СФЕРА С ПОМОЩТА НА PYTHON И DJANGO, Десислава Н. Иванова, Валентин Т. Атанасов ..... 48

НЯКОИ АСПЕКТИ НА АВТОМАТИЗИРАНИТЕ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ПРОЦЕСИ В ОБРАЗОВАТЕЛНАТА СФЕРА, Десислава Н. Иванова, Валентин Т. Атанасов ..... 57

ИЗГРАЖДАНЕ НА LAN МРЕЖА МЕЖДУ ПРОГРАМИРУЕМ ЛОГИЧЕСКИ КОНТРОЛЕР И МИКРОКОНТРОЛЕР, Даниел Р. Денев ..... 65

ТЕХНОЛОГИЯТА MIMO – ЗНАЧЕНИЕ, СЪЗДАВАНЕ И ПРИЛОЖЕНИЕ, Илкер А. Хатиб, Даниел Р. Денев ..... 71

ЕВОЛЮЦИЯ И ПРЕДИЗВИКАТЕЛСТВА В РАЗВИТИЕТО НА 5G МРЕЖИ – ТЕХНОЛОГИИ, СИГУРНОСТ И БЪДЕЩИ ПРИЛОЖЕНИЯ, Илкер А. Хатиб ..... 79

КОМПЮТЪРНО ЗРЕНИЕ – МЕТОД НА ДЕЙСТВИЕ И НЕГОВОТО ПРИЛОЖЕНИЕ В СВЕТА НА ТЕХНОЛОГИИТЕ, Красимир И. Христов, Танер Б. Язаджиев ..... 88

ИЗГРАЖДАНЕ НА ИНФОРМАЦИОННА МРЕЖА С NETWORK NOTEPAD, Стефан М. Казаков ..... 94

ТЕХНОЛОГИЯТА EDGE COMPUTING И ОПТИМИЗАЦИЯТА НА МРЕЖОВИТЕ РЕСУРСИ – УСЛОЖНЕНИЯ И ВЪЗМОЖНОСТИ, Илкер А. Хатиб, Даниел Р. Денев . 103

МЕТОД ЗА МИНИМИЗИРАНЕ И ПРЕМАХВАНЕ НА ЗВУКОВИ ИЗКРИВЯВАНИЯ ПРИ СКРИВАНЕ НА ЦИФРОВИ ДАННИ В ПРОЦЕСА НА ЦИФРОВИЗАЦИЯ, Даниел Р. Денев ..... 111

КРИПТОАНАЛИЗ – МЕТОДИ ЗА РАЗБИВАНЕ НА ШИФРИ, Алекс Я. Данев ..... 117

ИЗСЛЕДВАНЕ НА ВЛИЯНИЕТО НА КВАНТОВИТЕ КОМПЮТРИ ВЪРХУ RSA АЛГОРИТЪМА, Георги Д. Димитров ..... 125

# СЪДЪРЖАНИЕ

ИНТЕРНЕТ НА НЕЩАТА (IoT) – ПРОТОКОЛИ ЗА КОМУНИКАЦИЯ, ПРИЛОЖЕНИЯ И БЪДЕЩИ ТЕНДЕНЦИИ В ИНТЕЛИГЕНТНИ ДОМОВЕ И УСТОЙЧИВО РАЗВИТИЕ, Михаил С. Сейков, Петя К. Колева ..... 130

ПРИЛОЖЕНИЕ НА КОНВОЛЮЦИОННИ НЕВРОННИ МРЕЖИ ЗА РАЗПОЗНАВАНЕ НА ОБЕКТИ ПРИ ВИДЕОКАМЕРИ С AI, Силвия Х. Николова ..... 136

ПРЕДИМСТВА И НЕДОСТАТЪЦИ НА АЛГОРИТЪМА БЕРНУЛИЕВ НАИВЕН БЕЙСОВ КЛАСИФИКАТОР, Нели А. Арабаджиева-Калчева, Гинка К. Маринова, Мая П. Тодорова ..... 143

ПРИЛОЖЕНИЕ НА АНАЛИЗА НА ВИДОВЕТЕ ОТКАЗИ И ПОСЛЕДСТВИЯТА ОТ ТЯХ ЗА ОЦЕНКА НА НАДЕЖДНОСТТА НА ЧОВЕШКИЯ ФАКТОР, Нели А. Арабаджиева-Калчева, Цветослав С. Цанков, Мая П. Тодорова, Гинка К. Маринова ..... 147

РАЗВИТИЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ И ПРИЛОЖЕНИЯТА МУ В СЪВРЕМЕННИЯ СВЯТ, Емили К. Димитрова, Даниел Р. Денев ..... 153

КОМПЮТЪРНА СИГУРНОСТ И УПРАВЛЕНИЕ НА ТРАФИК В КОМУНИКАЦИОННИТЕ МРЕЖИ, Димитър Р. Илиев, Даниел Р. Денев ..... 161

МЕТОД „К-НАЙ-БЛИЗЪК СЪСЕД“, Мая П. Тодорова ..... 170

ИЗКУСТВЕНА НЕВРОННА МРЕЖА, Гинка К. Маринова ..... 174

ПРОТИВОДЕЙСТВИЕ И БОРБА С КОРУПЦИЯТА В ПУБЛИЧНИТЕ АДМИНИСТРАЦИИ, Илиана К. Симеонова, Елица Ю. Кузманова ..... 178

НАЙ-ДОБРИ ПРАКТИКИ ЗА СИГУРНОСТ НА КРАЙНИТЕ УСТРОЙСТВА, Денис И. Звезделинов, Димитър Н. Грешков ..... 188

ФИШИНГ АТАКИ – РАЗПОЗНАВАНЕ И ЗАЩИТА, Йовко М. Христов, Десислав М. Христов ..... 194

УПРАВЛЕНИЕ НА РИСКА В ОРГАНИЗАЦИЯТА, Десислава Д. Георгиева ..... 204

ПРИЛОЖЕНИЯ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В КИБЕРСИГУРНОСТТА, Стоян Р. Стоянов ..... 213

КИБЕРАТАКИ И НОВОВЪЗНИКВАЩИ ТЕХНОЛОГИИ – НОЖ С ДВЕ ОСТРИЕТА, Зорница Н. Младенова-Ангелова, Георги Т. Манев ..... 222

ЦИФРОВОТО ПРЕДСТАВЯНЕ НА ВИРТУАЛНИ ИЗОБРАЖЕНИЯ, Кирил Ф. Янчев . 229

ПРЕОБРАЗУВАНЕ НА ДАННИТЕ ОТ СКЕНЕРА ВЪВ ВИРТУАЛНИ ИЗОБРАЖЕНИЯ, Кирил Ф. Янчев ..... 233

АКУСТИЧНО ПОЛЕ И ФИЗИЧЕСКИ ХАРАКТЕРИСТИКИ НА МОРСКАТА ВОДА, Евгени Г. Стойков ..... 237

ПРОВЕЖДАНЕ НА СТРАТЕГИЯ ЗА ОБОСОБЯВАНЕ НА ТЕРИТОРИИ ЗА ДАЛЕКОПЕРСПЕКТИВНО РАЗВИТИЕ, Румяна К. Тодорова, Красимира К. Кирилова ..... 240

ТРИГОНОМЕТРИЧНАТА НИВЕЛАЦИЯ В ПРОЕКТИРАНЕТО И СТРОИТЕЛСТВОТО НА ЛИНЕЙНИ ОБЕКТИ, Иван Д. Иванов ..... 247

# СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ НА КАДАСТРАЛНАТА КАРТА, Мирем Е. Ниязи-Юсуф ..... 253

НОРМИ ЗА ИЗПЪЛНЕНИЕ, КОНТРОЛ И ПРИЕМАНЕ НА СТРОИТЕЛНО-МОНТАЖНИ РАБОТИ В МОСТОВОТО СТРОИТЕЛСТВО В БЪЛГАРИЯ, Ани А. Стефанова ..... 258

ИЗПОЛЗВАНЕ НА ДИСТАНЦИОННИТЕ МЕТОДИ ЗА ОЦЕНКА И ЕКОЛОГИЧЕН МОНИТОРИНГ НА АГРОЕКОСИСТЕМИТЕ В ПЛАНИНСКИТЕ РАЙОНИ, Кристина К. Янчева ..... 268

БЪДЕЩЕТО НА ГЕОДЕЗИЯТА, Ванеса Г. Георгиева, Евгени Г. Стойков ..... 273

РАДИОКОМУНИКАЦИОННИ ТЕХНОЛОГИИ В ГЕОДЕЗИЯТА, Стефан Д. Добрев .. 276

СПЕКТРАЛНИ ОТРАЖАТЕЛНИ ХАРАКТЕРИСТИКИ НА ОСНОВНИТЕ КЛАСОВЕ ПРИРОДНИ ОБЕКТИ ПРИ ДИСТАНЦИОННИ ИЗСЛЕДВАНИЯ НА ЗЕМНАТА ПОВЪРХНОСТ, Найлян М. Салиева ..... 281

LOCATION SELECTION METHOD FOR THE INITIAL POINTS OF HORIZONTAL BRIDGE GEODETIC NETWORKS, Ani A. Stefanova ..... 289

ПРОГНОЗИРАНЕ НАРАСТВАНЕТО НА СУМАРНАТА ГРЕШКА ПРИ ЖИРОСКОПИЧНИ ИЗМЕРВАТЕЛНИ СРЕДСТВА, Андрей И. Богданов, Теодора Д. Пеева ..... 298

ЗА РАЦИОНАЛНИТЕ РЕШЕНИЯ В КОНТЕКСТА НА ИНТРАЛОГИСТИКАТА, Светлозар П. Стоянов, Женя П. Георгиева, Николай Х. Йорданов ..... 302

ПРИЛОЖЕНИЕ НА СЪВРЕМЕННИТЕ ТЕХНОЛОГИИ В ЗЕМЕДЕЛСКИ ПРОИЗВОДСТВЕНИ СИСТЕМИ, Петя К. Велчева-Тодорова ..... 308

РОЛЯТА НА БЕЗЖИЧНИТЕ КОМУНИКАЦИИ В УПРАВЛЕНИЕТО НА ДЕЙНОСТИТЕ В ЗЕМЕДЕЛСКИТЕ ПРОИЗВОДСТВЕНИ СИСТЕМИ, Петя К. Велчева-Тодорова ..... 314

ТЕХНИЧЕСКО ОБЕЗПЕЧАВАНЕ НА ОБУЧЕНИЕТО ЗА ПРИДОБИВАНЕ НА ПРАВОСПОСОБНОСТ ЗА УПРАВЛЕНИЕ НА МПС В ГИМНАЗИИТЕ, Цветослав С. Цанков, Станимира Ц. Станиславова ..... 320

РОЛЯТА НА АВТОВЛАКОВЕТЕ В ОПТИМИЗАЦИЯТА НА ТОВАРНИЯ ТРАНСПОРТ В ЕВРОПА, Валентин К. Семов, Ангелинка Ц. Станиславова ..... 327

ОБРАТНА ЛОГИСТИКА И ИНОВАЦИИ ЗА УПРАВЛЕНИЕ НА НЕИЗПОЛЗВАЕМИ ГУМЕНИ ОТПАДЪЦИ, Йорданка И. Янкова-Йорданова, Цветослав С. Цанков ..... 332

УНИВЕРСАЛНИ МЕТАЛООБРАБОТВАЩИ МАШИНИ ЗА АВТОТРАКТОРНИ РАБОТИЛНИЦИ, Дидия-Клара А. Генчева, Атанас А. Генчев ..... 338

MOST APPLICABLE HARDWARE TECHNOLOGIES AND MATERIALS FOR PHYSICAL PROTOTYPING, Mariela L. Antonova, Stamen I. Antonov ..... 344

CALCULATION AND SELECTION OF SOME BASIC MACHINE ELEMENTS, Mariela L. Antonova, Stamen I. Antonov ..... 350




# ИГРОВИ КОМПЮТЪРЕН ФОРУМ

# 2024

На 25.10.2024 г. се проведе игрова сесия към „Игрови компютърен форум“, част от Научната конференция с международно участие MATTEX 2024. Събитието събра на едно място преподаватели представители на средното и висше образование, студенти, ученици и любители на видеоигрите. Основната цел беше да се покаже, че видеоигрите имат широк спектър на приложимост в образователния процес на студенти и ученици, спомагайки за развитието на техните когнитивни процеси и интелектуална дейност.

Организаторите на „Игрови компютърен форум“ изказват благодарности към Средно училище „Панайот Волов“ и Професионална гимназия по механотехника, електроника, телекомуникации и транспорт „Христо Ботев“. Благодарим на техните отбори за активното участие във форума.

Уважаеми участници в „Игрови компютърен форум“,

С дълбоко уважение и искрена благодарност се обръщаме към вас, за да изразим нашето признание за вашето участие в тазгодишното издание на „Игрови компютърен форум“. Вашата ангажираност и принос към игровите процеси допринесоха не само за успеха на събитието, но и за утвърждаването на форума като водеща платформа за обмен на знания и идеи в света на видеоигрите.

Вашата страст към игрите и готовността да споделяте опит със съученици и студенти направиха всяка игра и дискусия значими. Разговорите за гейм дизайна, игровите механики и новаторските подходи в графиката и звуковия дизайн вдъхновиха нови идеи и посоки за развитие на форума. Показахте, че индустрията на видеоигрите не е просто забавление, а сложна екосистема от иновации и творчество, която допринася за личното и образователното ви развитие. Форумът демонстрира, че видеоигрите не само забавляват, но и предлагат нови форми на комуникация, взаимодействие и културно изразяване.

Вашето участие в игрите и дискусиите бе ключово за създаването на атмосфера на сътрудничество и обмен на идеи. Без вашия ентусиазъм този форум нямаше да бъде толкова успешен и вдъхновяващ. Вие очертахте както настоящите тенденции в обучението чрез игри, така и бъдещите предизвикателства и възможности.

От името на екипа на „Игрови компютърен форум“ благодарим за смелостта ви да споделяте опит, за страстта към игрите и за ангажираността към развитието на образователния процес. Надяваме се, че дискусиите, връзките и приятелствата, създадени тук, ще доведат до дългосрочни сътрудничества и нови проекти.

С нетърпение очакваме следващото издание на форума, когато отново ще изследваме нови постижения и иновации в света на видеоигрите. Дотогава ви желаем успех във всички бъдещи начинания и творчески проекти!

С уважение и благодарност,

Екипът на „Игрови компютърен форум“


КОРПУС 3


КОРПУС 3
MANDALORIAN



*Източник на изображението: ТАСС*

## *90 години от рождението на Юрий Гагарин*

На 9 март 2024 година се отбелязват 90 години от рождението на първия космонавт в човешката история, пилотирал космически полет на 12 април 1961 година.
Това е съветският  военен пилот и космонавт полковник Юрий Алексеевич Гагарин.