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



Том 2, част 1

2026

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, Part 1

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 2026

СБОРНИК НАУЧНИ ТРУДОВЕ

МАТТЕН2026

CONFERENCE PROCEEDINGS

Том 2, част 1 **Volume 2, Part 1**

Комуникационна и компютърна техника и технологии

Информационни, технически и икономически проблеми на системите за сигурност

Communication and Computer Technologies

Information, Technical and Economic Problems of Security Systems

Университетско издателство
"Епископ Константин Преславски"

Настоящият сборник съдържа научни доклади, изнесени на проведената през месец октомври 2026 година в Шуменския университет научна конференция с международно участие MATTEX 2026 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 2026 held at Konstantin Preslavsky University of Shumen in October 2026. 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
Prof. Lazar Stosic, 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/FTN26M1

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

ARTIFICIAL INTELLIGENCE: PAST, PRESENT AND FUTURE*

PROF. IVAN TSONEV, KREMEN HRISTOV

ABSTRACT: *The paper examines the development of artificial intelligence through several related questions: which ideas have retained their scientific value through the periods of decline, how capital and computing power are changing the field, how today's capabilities are verified, and who bears responsibility when systems not only generate content but also take actions. The historical part traces the periods of declining interest and sharp cuts in public and private funding. Technical limitations, unmet expectations and the emergence of cheaper solutions caused these. Turning to the present, the paper considers investment, energy consumption, benchmark results, scientific applications and the effects on employment. The main conclusion is that the development of the largest general-purpose models has become concentrated mainly in large technology companies. Universities, however, retain an essential role in fundamental research, specialized scientific applications, independent verification, education, and the maintenance of data and tools for work in the Bulgarian language.*

KEYWORDS: *artificial intelligence, AI winters, AI agents, independent evaluation, universities, Bulgarian language*

DOI: https://doi.org/10.46687/MT26ITX

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ: МИНАЛО, НАСТОЯЩЕ И БЪДЕЩЕ

ПРОФ. ИВАН ЦОНЕВ, КРЕМЕН ХРИСТОВ

АБСТРАКТ: *Докладът разглежда развитието на изкуствения интелект през няколко свързани въпроса: кои идеи са запазили научната си стойност през периодите на спад, как капиталът и изчислителните мощности променят тази област, как се проверяват днешните възможности и кой носи отговорност, когато системите не само създават съдържание, но и извършват действия. Историческата част проследява периодите на спад в интереса и рязко свиване на публичното и частното финансиране. Причините са технически ограничения, неизпълнени очаквания и появата на по-евтини решения. За настоящето са разгледани инвестициите, потреблението на енергия, резултатите от сравнителни изпитвания, научните приложения и отражението върху заетостта. Основният извод е, че разработването на най-големите модели с общо предназначение се съсредоточи главно в големи технологични компании. Университетите обаче запазват съществена роля във фундаменталните изследвания, специализираните научни приложения, независимата проверка, образованието и поддържането на данни и средства за работа на български език.*

1 Въведение

През октомври 2024 г. две последователни Нобелови награди показаха колко дълбоко машинното обучение е навлязло в науката. Наградата по физика бе присъдена на Джон Хопфийлд и Джефри Хинтън за основополагащи открития и изобретения, направили възможно машинното обучение с изкуствени невронни мрежи. На следващия ден Дейвид Бейкър получи половината от наградата по химия за изчислително проектиране на белтъци, а Демис Хасабис и Джон Джъмпер си поделиха другата половина за предсказване на белтъчни структури [12].

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Тези отличия показват, че методите на изкуствения интелект вече са част от научната работа във физиката, химията и биологията. В същото време разработването на най-големите модели с общо предназначение изисква средства и изчислителна мощ, с които разполагат главно няколко големи компании. Оттук следва въпросът, на който е посветен този доклад: как се разпределят създаването, приложението и независимата проверка на тези системи.

Основна теза. През последното десетилетие разработването на най-големите модели с общо предназначение се съсредоточи главно в големи технологични компании. Това не намалява значението на университета, а определя по-точно неговите задачи: фундаментални изследвания, приложения в отделните науки, независима проверка на обявените резултати, подготовка на специалисти и поддържане на знания и данни с обществено значение. Независимата проверка е особено необходима, когато разработчикът сам определя начина на изпитване и достъпа до необходимата за оценяването информация, а използването на системата може да има правни, финансови, медицински или други практически последици.

2 Минало: научни ограничения, завишени очаквания и свиване на финансирането

Историята на тази област не може да се обясни нито само с научните открития, нито само с размера на финансирането. Двете са свързани. Очакванията за бърз технически напредък привличат средства. Когато резултатите не се потвърдят извън лабораторните демонстрации, доверието намалява, а финансирането от публични бюджети и частни инвестиции се свива.

През 1950 г. Алън Тюринг поставя въпроса дали машините могат да мислят, но го заменя с проверима задача: може ли в разговор поведението на машината да бъде различено от човешкото [19]. Предложението за срещата в Дартмут от 1955 г. дава име на новата научна област и поставя задачата езикът, абстракцията, решаването на задачи и самоусъвършенстването да се изследват с помощта на машини [11]. По онова време работата се извършва главно в университети, финансирането е публично, а резултатите се публикуват открито.

Първите влиятелни системи работят със символи и правила. Те се справят с ясно ограничени задачи, включително доказване на теореми и медицинска диагностика, но трудно отчитат изключенията и промените в обстоятелствата. Поддържането на ръчно описани бази от знания е скъпо, а убедителната демонстрация невинаги води до надеждна система за всекидневна работа [17].

Първият продължителен спад започва след натрупването на тези разминавания. Докладът ALPAC от 1966 г. определя машинния превод като недостатъчно качествен и икономически неоправдан. Критиките към ранните невронни мрежи и британската програма по изкуствен интелект допълнително намаляват доверието. Последват бюджетни съкращения, но те са следствие и от техническите ограничения, а не самостоятелна причина [1], [17].

През 80-те години експертните системи са полезни в тесни области, но разработването им е скъпо. Специализираните машини губят предимството си пред по-евтините работни

станции. Изследванията продължават: обратното разпространение на грешката се утвърждава през 1986 г., AlexNet показва значението на данните и графичните процесори през 2012 г., а архитектурата Transformer поставя основите на големите езикови модели през 2017 г. ChatGPT ги прави общодостъпни през 2022 г. [10], [14], [16], [21]. Основните етапи са обобщени в табл. 1.

Таблица 1. Основни етапи в развитието на изкуствения интелект

Период	Какво се променя	Защо има значение
1950–1956	Тюринг предлага поведенческа проверка; Дартмут дава име на полето	Интелигентността става предмет на експеримент и инженерна работа
1960-те – 80-те	Символни програми и експертни системи	Силен резултат в тесен обхват, но трудна и скъпа адаптация
1986–2012	Обратно разпространение на грешката, повече данни и изчислителна мощ	Моделите откриват закономерности в данните, вместо да следват само предварително зададени правила
2016–2017	AlphaGo и архитектурата Transformer, основана на механизма на вниманието	Обучението чрез многократно изиграване на партии и механизмът на вниманието разширяват кръга от задачи
2021–2022	AlphaFold2, големите езикови модели и ChatGPT	Методите навлизат пряко в научната и всекидневната работа
2025–2026	Обработка на текст, изображения, звук и видео; изпълнение на поредица от действия	Проверява се надеждността на поредицата от действия, не само точността на отделния отговор

Историческите спадове не могат да се обяснят само със свиването на финансирането. Те настъпват, когато заявената широка приложимост на даден метод се сблъска с висока цена, ненадеждност или ограничен обхват. Намаляването на средствата задълбочава отлива. При планиране на университетска програма трайният научен въпрос трябва да се разграничава от текущия инвестиционен интерес.

3 Мащабът на капитала и инфраструктурата

Вложенията днес са без исторически аналог за тази област. Докладът на Станфордския университет за 2026 г. оценява общите корпоративни инвестиции през 2025 г. на 581,69 млрд. щатски долара. В сумата влизат сливания и придобивания, миноритарни участия, частни вложения и публични предлагания, само частните инвестиции са 344,66 млрд. долара. Gartner прогнозира световни разходи от 2,59 трилиона долара през 2026 г. [5], [18]. Категориите са различни и числата не бива да се събират. И двете обаче показват необичайно висока концентрация на средства и очаквания.

Тази инфраструктура има материална цена. Международната агенция по енергетика изчислява, че центровете за данни са потребили около 415 тераватчаса електроенергия през

2024 г., приблизително 1,5% от световното потребление. В основния сценарий потреблението достига около 945 тераватчаса през 2030 г. [8]. Не цялото потребление се дължи на изкуствения интелект, но ускореното изграждане на изчислителни мощности е водеща причина за очакваното увеличение.

От размера на вложенията не следва автоматично нито че е налице спекулативен балон, нито че обществената полза е гарантирана. Разходът за инфраструктура измерва готовността да се поеме риск, а не постигнатата производителност. Пазарната оценка, подобряването на техническите показатели, приходите от услугата и практическата полза за дадена организация са различни величини. Смесването им прави анализа впечатляващ, но неточен.

За академичните институции практическото следствие е ясно. Дългосрочна програма не трябва да зависи изцяло от един доставчик, временна отстъпка за изчислителен ресурс или изпитване, чиито условия могат да бъдат променени без публично описание. Устойчивостта се търси в преносими данни, възпроизводими процедури, общи стандарти и достъп до повече от една технологична среда.

4 Неравномерни способности и преминаване към действия

Възможностите на съвременните модели се различават значително според задачата. Според доклада на Станфордския университет Gemini Deep Think достига резултат, съответстващ на златен медал от Международната олимпиада по математика през 2025 г. При разчитане на аналогови часовници обаче най-добрият резултат е 50,6%, при около 90,1% за хората. В ChemBench, изпитване с над 2700 въпроса по химия, водещите модели надминават средното представяне на химици, но грешат и при привидно прости задачи [18]. Подобен резултат описва поведението при определени условия, той не доказва обща способност.

Особено бързо се развиват системите, които следват зададена цел, използват запаметена информация и работят с други приложения. При OSWorld, изпитване за работа в компютърна среда, най-добрият резултат се повишава от приблизително 12% на 66,3% за около година и половина, при около 72% за човек. Това е съществен напредък, но системата все още не завършва успешно приблизително една от три задачи. При по-дълга последователност рискът от натрупване на грешки нараства [7], [18].

Разликата между създаването на съдържание и извършването на действие има пряко практическо значение. Неточен абзац може да бъде редактиран преди публикуването му. Погрешно наредено плащане, промяна в медицински запис или задействан лабораторен процес вече засягат реална система. Рискът зависи не само от качествата на модела, но и от предоставения достъп, продължителността на задачата, изискването за човешко потвърждение и възможността извършеното да бъде отменено.

5 Разделението на труда между индустрията и университета

През 2025 г. 91,2% от моделите, които съставителите на годишния доклад на Станфордския университет включват сред водещите разработки, са създадени от компании. Показателят не обхваща всички съществуващи модели. Същият доклад сочи, че при разработките за научни задачи водещото място все още принадлежи на университетите и

публичните научни организации [18]. Следователно към компаниите са се изместили главно разработките, които изискват най-големи изчислителни мощности и финансови средства.

Това не означава, че системите, разработени от компании, са по начало по-ненадеждни. Големите компании разполагат с инженерни екипи, данни и изчислителни мощности, които университетите рядко могат да осигурят. Проблемът е друг: разработчикът често решава какви данни да използва, как да изпита системата, кои резултати да оповести и до каква информация да предостави достъп на външни изследователи. Поради това външната оценка се извършва при непълна информация.

Тъкмо тук е необходима независима научна проверка. Причината не е недоверие към компаниите, а необходимостта заявените качества на системата да бъдат проверени от институция, която не участва в нейното разработване и предлагане. Когато системата получава достъп до информационни, финансови, медицински или производствени процеси, проверката трябва да обхваща не само точността на отговорите, но и условията, при които системата може да действа.

6 Науката: ускорение без прехвърляне на отговорността

AlphaFold е показателен пример за научна полза и опровергава простото противопоставяне между университети и компании. Системата е разработена от компания, но се опира на структурни данни, натрупвани с публично финансиране десетилетия наред. По данни на Google DeepMind системата е използвана от над три милиона изследователи в повече от 190 държави и е цитирана в над 35 000 научни публикации [6], [9]. Тези сведения са на разработчика. Те показват разпространението, но сами не доказват научния принос.

Ограниченията личат по-ясно при по-сложни научни задачи. В PaperArena, изпитване за подготовка на научен труд, най-добрата система получава 38,8 точки при 83,5 за специалисти с докторска степен. В ReplicationBench, където се проверява възпроизвеждането на резултати от публикации по изчислителна астрофизика, водещите модели остават под 20% успеваемост [18]. Тези изпитвания не обхващат цялата научна работа, но проверяват продължителната работа, избора между възможности и оценката на междинните резултати.

Науката не е само получаване на правилен отговор. Тя изисква значим въпрос, обоснован метод, проследими данни и автор, който носи отговорност за заключението. Моделът може да предложи повече хипотези, да съкрати търсенето и да ускори анализа. Преценката кое може да се приеме за доказателство остава отговорност на изследователя и научната институция.

7 Трудът, Европа и българският език

Данните за заетостта не позволяват еднозначен извод. Изследване в действителна работна среда показва, че помощник с генеративен изкуствен интелект повишава производителността при обслужването на клиенти с 14 до 15%, най-вече при служителите с по-малък опит [2]. Докладът на Станфордския университет посочва и че заетостта сред разработчиците на софтуер на възраст между 22 и 25 години е близо 20% под равнището от

2024 г. Това не доказва, че изкуственият интелект е единствената причина, но е пряко свързано с въпроса как завършващите студенти навлизат на пазара на труда [18].

За България е по-полезно да излезем от общия спор дали Европа „изостава“. По данни на Евростат през 2025 г. 20,0% от компаниите в Европейския съюз с поне десет заети използват поне една технология с изкуствен интелект. За България делът е 8,5%, сред най-ниските в Съюза [4]. Това е конкретният проблем: българските компании се нуждаят от подготвени специалисти, подходящи данни и способност да преценят дали дадено приложение действително подобрява работата им.

Работата на български език поставя отделна задача. Големите езикови модели обикновено се представят по-слабо извън английския, особено когато данните за обучение и оценяване са недостатъчни или не отразяват местния контекст [15]. Българските университети трябва да създават езикови корпуси с ясен произход и уредени права, да систематизират терминологията в отделните области и да подготвят задачи за оценяване в администрацията, науката и професионалната практика. Без такава работа качеството не може да се измерва надеждно.

8 Бъдещето: сценарии вместо дата

Публичният разговор често търси дата, на която системите ще решават широк кръг задачи на равнище, сравнимо с човешкото. За подобна способност обаче няма общоприето определение и единно изпитване. Затова Организацията за икономическо сътрудничество и развитие (ОИСР) разглежда четири възможни посоки до 2030 г., а не една прогноза. Международният доклад за безопасността на изкуствения интелект от 2026 г. също отделя наблюдаваните способности от предположенията за бъдещото им развитие [7], [13]. Тези варианти служат за сравнение на решения, не за определяне на срок.

По-надеждно е да се следят измерими признаци: задачи с каква продължителност системата изпълнява без съществена грешка, как се проверява резултатът, колко струва надеждното изпълнение и какво се променя при свързване с лабораторен уред, информационна система или робот. Подобни показатели могат да се сравняват във времето. Високият резултат при едно изпитване обаче не доказва разбиране и не позволява да се изчисли каква част от бъдещата работа ще бъде автоматизирана.

9 Задачата на университета

Съсредоточаването на финансови средства и изчислителна мощ в компаниите не превръща университетите в наблюдатели. То налага университетът да избере онези дейности, за които има собствена компетентност и може да носи отговорност. Виждам четири непосредствени задачи.

Най-напред е независимата оценка. Необходима е проверка върху задачи на български език и върху задачи от отделни научни и професионални области. Данните за обучение и изпитване трябва да бъдат ясно разграничени. Критериите трябва да бъдат описани, а отрицателните резултати също да се публикуват. Отделно направление е създаването на контролирани синтетични изображения за сравнение между човешкото и компютърното зрение [27]. При системи, които извършват действия, оценката трябва да обхваща

предоставения достъп, изискването за човешко потвърждение, регистрирането на извършените действия и начина за възстановяване след грешка.

Следва работата в собствената дисциплина. Полезният принос на университета не се изчерпва с обучаването на огромен модел с общо предназначение. Той може да бъде надежден набор от данни, малък специализиран модел, метод за сравнение, изследване за възпроизвеждане на публикувани резултати или проверено използване на готова система в лабораторната и професионалната работа. В тези случаи познаването на предмета често е по-ценно от мащаба на изчисленията. Примери за специализирани разработки са изкуствените имунни системи за синтез на сигнали с оптимални автокорелационни свойства [22, 25], личностовата персонификация на големи езикови модели [23] и прилагането на трансфер на знания при разпознаване на частично видими обекти [24].

Приложението на технологиите в обучението е предмет на съвременни педагогически изследвания [28]. Образованието поставя по-труден въпрос. Ако една задача се решава с едно запитване към модел, тя вече не измерва онова, за което е създадена. Студентът трябва да защити избора си, да покаже източниците и при нужда да възпроизведе съществената част от работата. ЮНЕСКО препоръчва човешката преценка и отговорност да останат водещи, а всяка употреба да бъде оценявана от учебното заведение според учебната цел [20]. Общата забрана се прилага трудно. Безусловното приемане обезсмисля изпитването.

Научната добросъвестност изисква проследимост. Трябва да е ясно какви данни са използвани, с коя версия на модела е работено, какво е проверено и кои решения са взети от автора. От 2 август 2026 г. Европейската комисия започна да прилага основните правила на Регламент (ЕС) 2024/1689 относно изкуствения интелект, включително задълженията за прозрачност при определени взаимодействия със системи и при синтетично съдържание [3]. Регламентът не решава въпроса за авторството в университета, но изисква по-ясно разграничаване на произхода на съдържанието и човешката намеса.

Част от тази работа изисква средства: изчислителна мощ, защитена среда, права върху данни и технически персонал. Пример за университетска изчислителна инфраструктура е клъстерната паралелна система в среда MPI, описана от Станев, Николов и Цанков [26]. Друга част може да започне без собствен суперкомпютър: правила за документиране, промяна на оценяването, общи набори от задачи и данни за оценяване и сътрудничество между катедри. Недостигът на мащаб не е оправдание за липса на метод.

10 Заключение

Седемдесетгодишната история на изкуствения интелект показва редуване на научен напредък, завишени очаквания и корекции. Спадовете не са били предизвикани само от недостиг на средства. Финансирането е намалявало, когато методите са се оказвали по-ненадеждни, по-скъпи или с по-тесен обхват от обещаното. Сегашният подем се различава по мащаба на вложенията и по това, че системите постепенно преминават от създаване на съдържание към изпълнение на поредица от действия.

Затова бих оставил настрана въпроса кога машината ще стане „като човека“. По-полезно е да обсъдим в какви случаи сме готови да се доверим на решението на една система, с какви доказателства за надеждността ѝ разполагаме и кой носи отговорност, когато въз основа на резултата се предприема действие. Университетът има място в този

разговор не по историческо право, а защото съчетава познание в отделните науки, процедури за проверка и отговорност за качеството на образованието.

Университетът не може и не е необходимо да съперничи на големите компании по изчислителна мощ. От него се очаква да проверява твърденията и да подготвя хора, които разбират границите на средствата, с които работят, и носят отговорност за решенията си.

Бележка за източниците. Историческите твърдения са сверени с първични публикации и с актуален обзор на развитието и последвалия спад на експертните системи. Данните за настоящето са към 10 септември 2026 г. Стойностите за корпоративни и частни инвестиции се отнасят до различни категории. Моделите, включени от съставителите на доклада на Станфордския университет сред водещите разработки, не представляват пълно преброяване. Данните за разпространението на AlphaFold са обявени от разработчика. Прогнозите за 2030 г. очертават възможни посоки, а не единно предвиждане.

ЛИТЕРАТУРА:

[1] ALPAC. Languages and Machines: Computers in Translation and Linguistics. National Academy of Sciences, 1966.

[2] Brynjolfsson E., Li D., Raymond L. R. Generative AI at Work. Quarterly Journal of Economics, Vol. 140, No. 2, 2025, pp. 889–942.

[3] European Commission. Commission starts enforcing AI Act rules and new transparency requirements on 2 August. 2026.

[4] Eurostat. 20% of EU enterprises use AI technologies. News article, 11 December 2025.

[5] Gartner. Gartner Forecasts Worldwide AI Spending to Grow 47% in 2026. 2026.

[6] Google DeepMind. AlphaFold: Five Years of Impact. 2025.

[7] International AI Safety Report. International AI Safety Report 2026. UK Department for Science, Innovation and Technology, 2026.

[8] International Energy Agency. Energy and AI. Paris: IEA, 2025.

[9] Jumper J. et al. Highly accurate protein structure prediction with AlphaFold. Nature, Vol. 596, 2021, pp. 583–589.

[10] Krizhevsky A., Sutskever I., Hinton G. E. ImageNet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems, Vol. 25, 2012.

[11] McCarthy J., Minsky M., Rochester N., Shannon C. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. 1955.

[12] Nobel Prize. Press releases: The Nobel Prize in Physics 2024; The Nobel Prize in Chemistry 2024. 2024.

[13] OECD. Exploring Possible AI Trajectories through 2030. OECD Artificial Intelligence Papers, No. 55, 2026.

[14] OpenAI. Introducing ChatGPT. 2022.

[15] Pava J. N. et al. Mind the (Language) Gap: Mapping the Challenges of LLM Development in Low-Resource Language Contexts. Stanford HAI and The Asia Foundation, 2025.

[16] Rumelhart D. E., Hinton G. E., Williams R. J. Learning representations by back-propagating errors. Nature, Vol. 323, 1986, pp. 533–536.

[17] Senator T. E. Applying Lessons from the Expert Systems Boom and Bust. Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 40, 2026.

[18] Stanford Institute for Human-Centered Artificial Intelligence. The 2026 AI Index Report. Stanford University, 2026.

[19] Turing A. M. Computing Machinery and Intelligence. Mind, Vol. 59, No. 236, 1950, pp. 433–460.

[20] UNESCO. Guidance for Generative AI in Education and Research. Paris: UNESCO, 2023.

[21] Vaswani A. et al. Attention Is All You Need. Advances in Neural Information Processing Systems, Vol. 30, 2017.

[22] Беджев Б. Й., Николов Н. Р., Цанков Ц. С. Обучаема изкуствена имунна система използваща „добри“ пътища за синтез на сигнали с оптимални автокорелационни свойства. MATTEX 2018, т. 2, част 2, Шумен, 2018, с. 3–11. ISSN 1314-3921.

[23] Алексиева А. Е., Кулев Н. З., Манов Л. Е. Личностова персонификация на големи езикови модели на базата на IPIP-50. Сборник доклади от научна конференция „Актуални проблеми на сигурността“, НВУ „Васил Левски“, Велико Търново, 2026, с. 807–814. ISSN 2367-7473 (PDF).

[24] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[25] Николов Н. Р., Беджев Б. Й., Цанков Ц. С. Приложение на изкуствените имунни системи при синтеза на сигнали с оптимални автокорелационни свойства. MATTEX 2016, т. 2, Шумен, 2016, с. 23–29. ISSN 1314-3921.

[26] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, сборник доклади, т. 1, Шумен, 2011, с. 229–232. ISSN 1314-3921.

[27] Manov L. E. Creation of a parametrically controlled synthetic image dataset of Ishihara-like plates for comparing human and computer vision. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2026, National Military University, 2026. ISSN 2815-4282.

[28] Бурова И. Същност на технологиите и приложението им в обучението. Е-списание „Образование и развитие“, бр. 17, 2026, с. 78–83. ISSN 2603-3577.

CLUSTERING IN AUTONOMOUS AGENTS WITH LLM ACTING UPON A SHARED PROCESS OR MARKET*

NIKOLAY R. NIKOLOV, TSVETOSLAV S. TSANKOV

ABSTRACT: *The use of autonomous agents based on large language models (LLM) is becoming a standard in modern information systems. The presence of several autonomous agents operating on a common object of control leads to the manifestation of the Kuramoto effect, with the potential to predetermine the behavior of the individual agents. One of these effects is the formation of spontaneous clustering (cartels). The aim of this paper is to present a model describing the process and to demonstrate that the formation of such synchronous decisions is determined by systemic preconditions.*

KEYWORDS: *artificial intelligence, large language models, Kuramoto model, synchronization, clustering, critical threshold, order parameter, algorithmic collusion, digital sovereignty*

DOI: https://doi.org/10.46687/MT26NRN

КЛЪСТЕРИЗАЦИЯ ПРИ АВТОНОМНИ АГЕНТИ С LLM, ВЪЗДЕЙСТВАЩИ ВЪРХУ ОБЩ ПРОЦЕС ИЛИ ПАЗАР

НИКОЛАЙ Р. НИКОЛОВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Използването на автономни агенти, базирани на големи езикови модели (LLM), става стандарт в съвременните информационни системи. Наличието на няколко автономни агента, работещи върху общ обект на управление, води до проява на ефект Курамото с потенциал да предопредели поведението на отделните агенти. Един от ефектите е формиране на спонтанна клъстеризация (картели). Целта на доклада е да се представи модел, описващ процеса, и да се посочи, че формирането на подобни синхронни решения е определено от системни предпоставки.*

1 Въведение

Настоящият доклад изследва и доказва числено един слабо разпознат системен ефект: когато множество независими големи езикови модели (Large Language Models, LLM) действат едновременно върху общ обект – един и същ пазар, информационен поток или управлявана техническа система – те спонтанно се самоорганизират и се клъстеризират, тоест изходите им се сближават и се фазово заключват в едно или няколко устойчиви струпвания. За формален апарат е използван моделът на Курамото за свързани фазови осцилатори, който е каноничен инструмент за описание на колективна синхронизация [1], [4]. Реализирани са шест числени експеримента (N до 500 агента), които потвърждават: (1) наличието на остър критичен праг на свързване Kc ≈ 1.60, над който подреденост та нараства скокообразно; (2) коалесценция на първоначално случайни фази в общ клъстер; (3) формиране на множество обособени клъстери при нехомогенна популация; и (4) – най-съществено за практиката – че синхронизация настъпва дори при липса на пряка връзка между агентите, единствено чрез споделения управляван обект. Обсъдени са

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

произтичащите рискове: спонтанни алгоритмични „картели“, манипулация на пазари и на информационната среда, ерозия на цифровия суверенитет и на когнитивния капацитет.

1.1. Постановка на проблема

При анализа на системи с изкуствен интелект (ИИ), интегрирани в критичните ведомства оценяват тяхната управляемост, устойчивост, оптималност, вътрешните колизии, наличието на целенасочени външни въздействия, предвидимостта, обхвата на засегнатите обществени отношения и очакваното развитие. Всички тези оценки мълчаливо предполагат, че отделната система може да бъде разглеждана изолирано. Настоящият доклад показва, че това допускане е несъстоятелно: когато много ИИ системи оперират върху един и същ обект, между тях възниква колективна динамика, която не се свежда до сбора на индивидуалните поведения. Програмните модели за автоматизиране на когнитивни процеси са разгледани в [7].

Съвременните пазари и информационни среди все по-често се обитават не от хора, а от автономни езикови модели, които анализират, вземат решения и генерират съдържание в реално време. Броят им расте, а взаимодействието между тях – макар често непряко и слабо – е постоянно. Именно това слабо взаимодействие, натрупано в общата среда, е достатъчно да задейства спонтанна самоорганизация.

1.2. Цел, теза и хипотеза

Целта на доклада е да докаже количествено, че използването на множество LLM върху един процес или пазар води до клъстеризация на тяхното поведение. Основната теза е формулирана като проверима хипотеза:

> *Хипотеза H.* Съществува критична стойност на свързаност K_c такава, че при интензивност на споделяните данни над K_c популацията от LLM агенти преминава фазов преход от некохерентно към частично или напълно синхронизирано състояние, при което изходите им се групират в един или няколко устойчиви клъстера – независимо дали агентите са свързани пряко или само чрез общия обект на въздействие.

1.3. Методика

Използван е моделът на Курамото - минимален апарат за колективна синхронизация. Всеки LLM се съпоставя на фазов осцилатор с естествена честота, а интензивността на споделяните данни - на силата на свързване. Проведени са шест числени експеримента с интегриране по метода на Ойлер (стъпка dt = 0.01), с популации до N = 500 агента. Като количествена мярка се използва параметърът на подреденост r, допълнен с езиково-специфични индикатори. Изводите се съпоставят с наблюдавани ефекти на пазарите и в информационната среда.

2 Математически основи на модела на Курамото

Моделът е предложен от японския физик Йошики Курамото през 1975 г. и описва как популация от независими периодични генератори спонтанно се самосинхронизират [1]. Класическата илюстрация е 100 метронома върху обща подвижна платформа: стартирали с различни фази, те постепенно обменят енергия и се синхронизират. Платформата тук играе ролята на **общия обект** – точно както пазарът или управляваната система свързват иначе независимите LLM.

2.1. Общи условия

Състоянието на i-тия осцилатор се описва с фазата му $\theta_i \in [0, 2\pi)$. Всеки има собствена (естествена) честота ω_i, изтеглена от разпределение $g(\omega)$. Динамиката на популация от N агента с еднородно (all-to-all) свързване е:

$$d\theta i / dt = \omega i + (K / N) \Sigma j \sin(\theta j - \theta i), i = 1, \ldots, N \quad (1)$$

където $K \geq 0$ е **силата на свързване**. Членът $\sin(\theta_j - \theta_i)$ привлича всеки осцилатор към фазата на останалите: когато K е малко, естествените честоти доминират и агентите се движат хаотично; когато K е голямо, привличането надделява и настъпва синхронизация [2].

2.2. Параметър на подреденост

Степента на колективна синхронизация се измерва с комплексния параметър на подреденост:

$$r\, ei\psi = (1 / N) \Sigma j\, ei\theta j \quad (2)$$

Величината $r \in [0, 1]$ е модулът на средния фазов вектор, а ψ е средната фаза. При пълна некохерентност фазите са равномерно разпръснати и $r \approx 0$; при пълна синхронизация всички фази съвпадат и $r = 1$. Именно r е нашата **количествена мярка за клъстеризация**. С нейна помощ уравнение (1) приема компактния „средно-полеви“ вид $d\theta_i/dt = \omega_i + K \cdot r \cdot \sin(\psi - \theta_i)$, който показва ясно, че силата на обратната връзка към всеки агент е пропорционална на вече постигнатата подреденост r – оттук произтича лавинообразният характер на прехода.

2.3. Критичен праг и фазов преход

Курамото показва, че за широк клас симетрични едномодални разпределения $g(\omega)$ съществува **критична стойност** на свързването:

$$Kc = 2 / (\pi \cdot g(0)) \quad (3)$$

Под K_c единственото устойчиво състояние е некохерентното ($r = 0$). Над K_c некохерентността губи устойчивост и се появява синхронизирано решение, чиято подреденост нараства като $r \propto \sqrt{(K - K_c)}$ [3]. Това е фазов преход от втори род: качествена промяна в поведението на цялата система при преминаване на един-единствен параметър през прага. За гаусово разпределение с дисперсия $\sigma^2 = 1$ имаме $g(0) = 1/\sqrt{(2\pi)}$ и оттам $K_c \approx 1.596$ – стойност, която числените ни експерименти възпроизвеждат точно (раздел 5).

2.4. Клъстерни състояния

Синхронизацията невинаги е глобална. Когато разпределението на честотите е многомодално или когато свързването е нехомогенно (силно вътре в групи и слабо между тях), системата се установява в **многоклъстерно състояние**: образуват се няколко вътрешно синхронизирани струпвания, всяко със своя обща фаза, които остават взаимно дефазирани [5]. В този режим локалната подреденост в рамките на всеки клъстер е близка до 1, докато глобалната подреденост r остава ниска. Именно този сценарий е най-релевантен за реални пазари, съставени от разнородни коалиции автоматизирани търговци.

3 LLM като фазови осцилатори: обосновка

За да е приложим апаратът на Курамото, е необходимо да обосновем защо един езиков модел може да се разглежда като осцилатор с определима „честота“ на поведението. По-долу са изложени пет независими аргумента, всеки от които посочва вграден периодичен или цикличен механизъм в съвременните ИИ системи.

Таблица 1. *Пет вградени механизма, които позволяват осцилаторното третиране на LLM*

№	Механизъм	Осцилаторна интерпретация
1	Периодичност в генеративните процеси	Генеративните архитектури проявяват ритмично редуване на фази на изследване (креативност) и на дообучаване/уточняване, което дефинира естествена честота на генериране.
2	Динамика на обучение с подкрепление (RL)	Балансът exploration–exploitation е по същество осцилаторен: агентът периодично редува изследване на нови стратегии и експлоатация на известни оптимални действия.
3	Темпорална динамика в sequence modeling	Gating механизмите в LSTM/GRU създават периодични цикли на запомняне и забравяне и функционират като адаптивни осцилатори с променлива честота.
4	Колективна динамика в мултиагентни системи	При взаимодействие на много агенти в обща среда се проявяват емергентни осцилаторни свойства дори когато отделните агенти не са проектирани като осцилатори.
5	Параметри Top-P, Top-K и температура	Тези параметри очертават ограничена област, от която се избират най-вероятните продължения; наличието на граници поражда повторяемост (цикличност) в избираните решения.

Тези аргументи показват, че „честотата“ на един LLM е измерима характеристика на неговия темп и стил на генериране. Разликите в архитектура, настройки и обучаващи корпуси задават **разпределението g(ω)** на естествените честоти в популацията – точно величината, която определя критичния праг по уравнение (3). Отделно направление при моделирането на поведението на LLM е личностовата им персонификация на базата на IPIP-50 [8].

4 Механизъм на свързване през общ процес или пазар

4.1. Пряко срещу непряко свързване

Свързването между LLM може да е **пряко** – чрез API интеграции, споделени данни и взаимно четене на изходи – или **непряко**, когато агентите изобщо не обменят “пряко” информация, а само наблюдават и въздействат върху един и същ обект. Вторият случай е практически по-важен: тук платформата на Курамото (общата подвижна основа) е самият пазар или управлявана система. Всеки агент оценява състоянието ѝ, реагира и с реакцията си я променя; следващият агент чете вече променено състояние. Така обектът действа като среда с памет, която пренася малки количества „енергия“ между иначе изолирани агенти и ги синхронизира.

4.2. Модел на непрякото свързване

Нека общият обект има състояние m(t) (например агрегиран пазарен сигнал), което релаксира към колективния изход на агентите с характерно време τ:

$$dm/dt = -(m - z)/\tau,\ z = (1/N)\,\Sigma\, e^{i\theta j} \qquad (4)$$

Всеки агент от своя страна се адаптира не към другите агенти, а към фазата на обекта:

$$d\theta i/dt = \omega i + K \cdot |m| \cdot \sin(\arg m - \theta i) \quad (5)$$

Уравнения (4)–(5) описват затворен контур на обратна връзка: агентите оформят обекта, обектът оформя агентите. Дори при нулево пряко свързване този контур поражда ефективно взаимодействие и – над съответния праг – синхронизация. Числената проверка на този сценарий (фигура 5) е ключовото практическо доказателство на доклада.

4.3. Параметърът на свързване като интензивност на данните

В реалните системи K не е абстракция, а се материализира чрез интензивността на споделяните данни: публични API, пазарни бюлетини, общи корпуси от знания и косвени взаимодействия в средата. Тъй като броят на автоматизираните участници и обемът на споделяните данни нарастват монотонно във времето, ефективното K на реалните пазари се движи в посока **нагоре** – тоест системата естествено дрейфи към и отвъд критичния праг. Това превръща клъстеризацията от възможност в очаквана тенденция. –

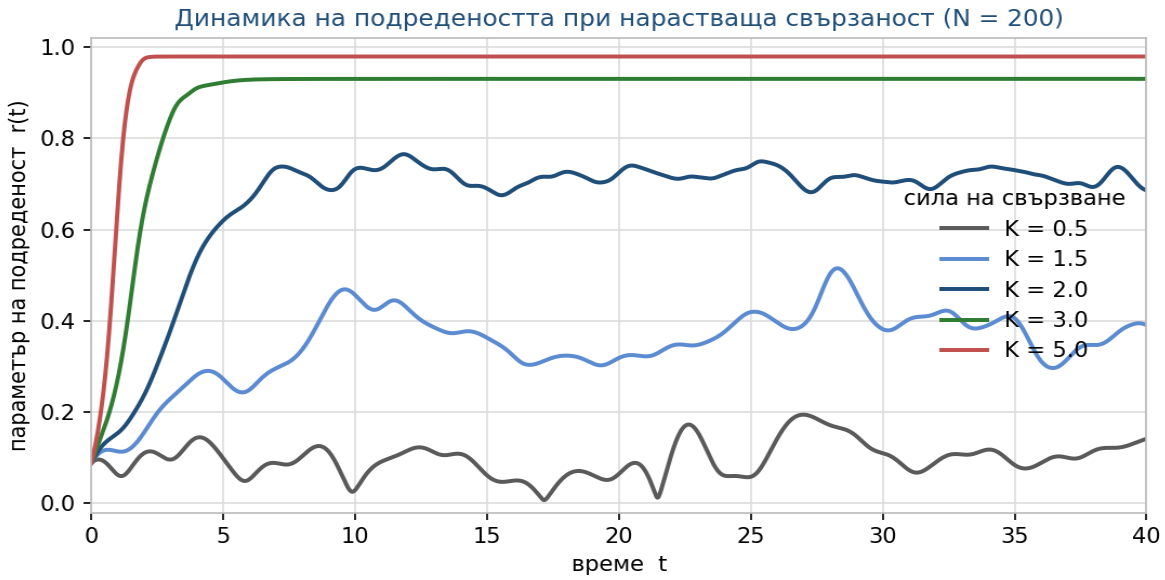
5 Числени експерименти и резултати

5.1. Постановка на експеримента

Всички симулации интегрират уравнение (1) (или (4)–(5) за непрякото свързване) по метода на Ойлер със стъпка dt = 0.01. Естествените честоти се теглят от гаусово разпределение N(0, 1), освен където изрично е указано друго. Началните фази са равномерно случайни в [0, 2π). Отчита се параметърът на подреденост r по уравнение (2).

5.2. Динамика на подредеността

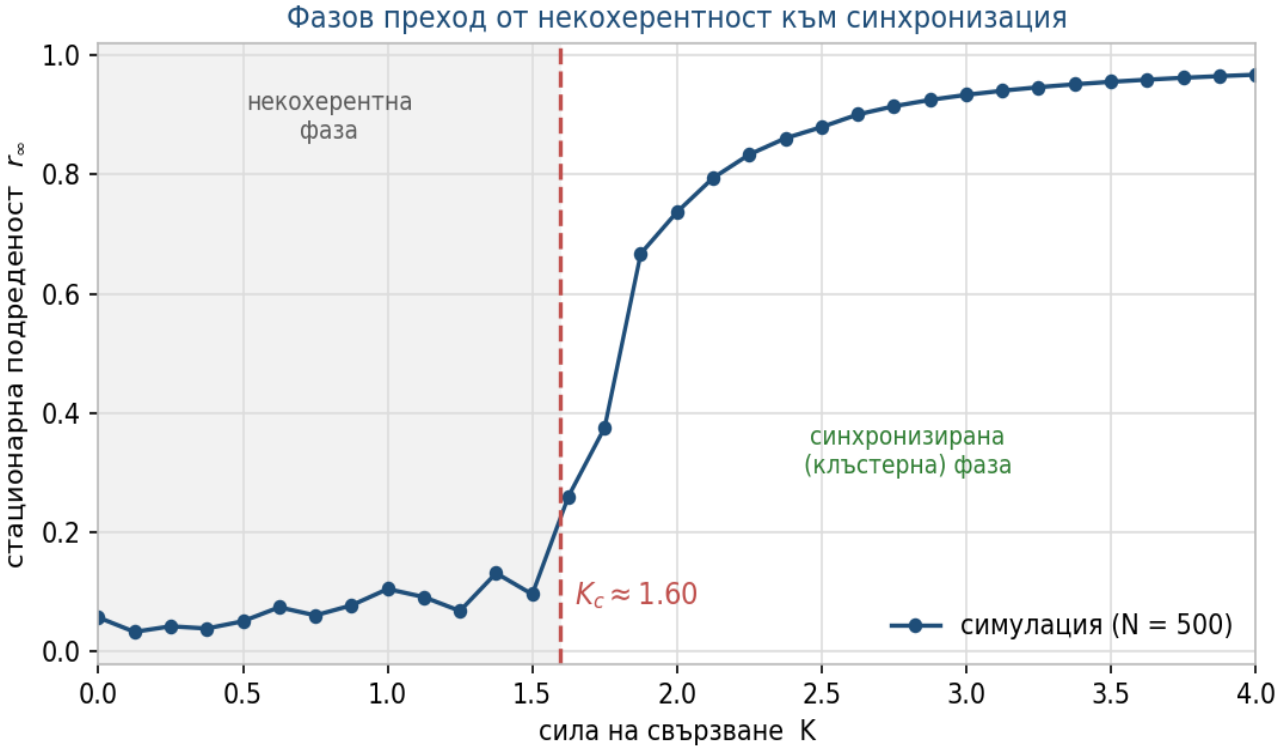
Фигура 1 проследява r(t) за нарастващи стойности на K при фиксирана популация (N = 200) и общи начални условия. При K = 0.5 подредеността флуктуира около нулата – агентите остават некохерентни. С увеличаване на K кривите се повдигат и се стабилизират на все по-високо плато, а при K = 5.0 системата достига r ≈ 0.98 практически мигновено. Наблюдава се ясна монотонна зависимост на стационарната подреденост от свързаността.



Фиг. 1. *Еволюция на параметъра на подреденост r(t) при пет стойности на K*

5.3. Фазов преход и критичен праг

Фигура 2 представя стационарната подреденост r∞ като функция на K за N = 500. Резултатът е класически фазов преход: под $K_c \approx 1.60$ подредеността е практически нулева (шум от краен размер), а над прага нараства стръмно. Вертикалната прекъсната линия отбелязва теоретичната стойност по уравнение (3); съвпадението между теория и симулация е отлично. Таблица 2 дава числените стойности.



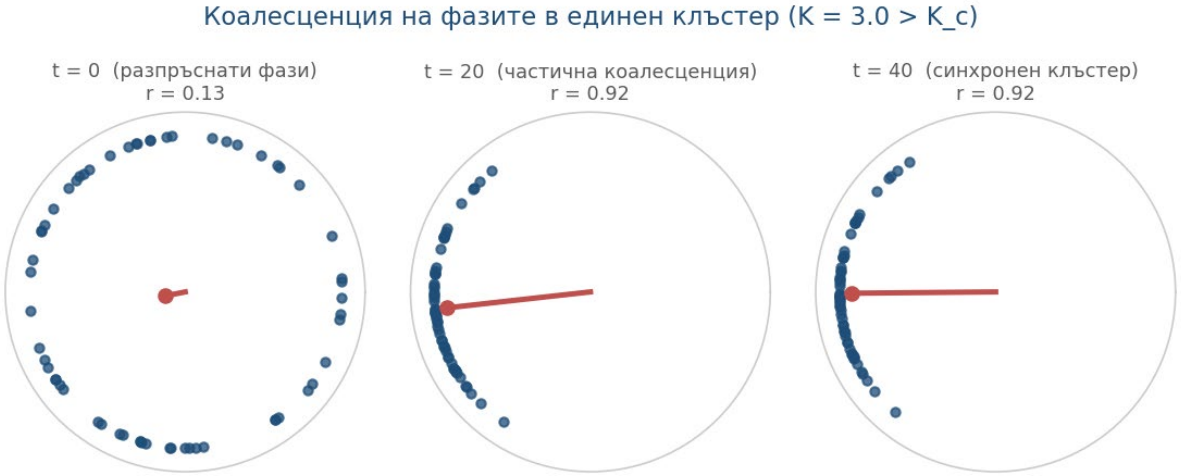
Фиг. 2. *Фазов преход r∞(K); критичен праг Kc ≈ 1.60 (прекъсната линия)*

Таблица 2. *Стационарна подреденост срещу свързаност (N = 500). Скокът настъпва точно около Kc*

K	0.5	1.0	1.5	2.0	3.0	4.0
r∞ (симулация)	0.05	0.11	0.10	0.74	0.93	0.97
Състояние	некохер.	некохер.	праг	синхрон	синхрон	синхрон

5.4. Коалесценция на фазите

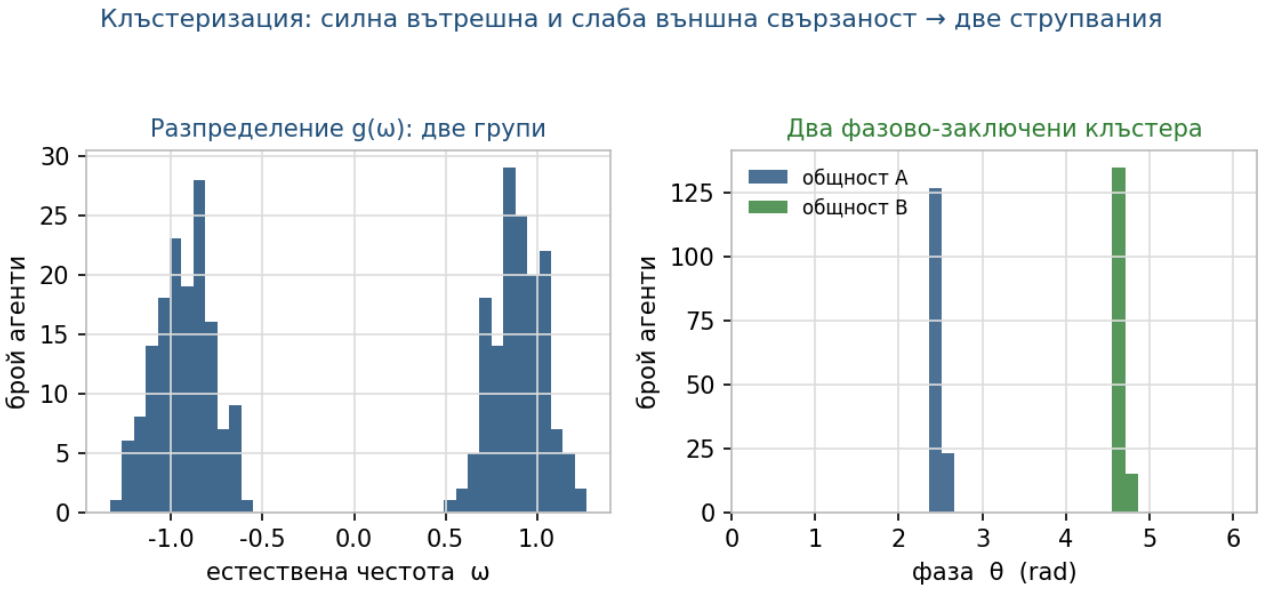
Фигура 3 показва фазовите портрети върху единичната окръжност в три момента при K = 3.0 (над прага). В началото (t = 0) точките са разпръснати и векторът на подреденост е почти нулев (r = 0.13). С времето фазите се събират в тесен сноп и до t = 40 системата достига компактен клъстер с r = 0.92. Червеният вектор – средният фазов вектор – нараства и се стабилизира, визуализирайки прехода към синхрон.



Фиг. 3. *Коалесценция на 60 фази в единен клъстер (K = 3.0). Червеният вектор е r·e^{iψ}*

5.5. Клъстеризация при нехомогенна популация

Фигура 4 демонстрира глобална клъстеризация: моделирани са две общности (напр. два сегмента на пазара) със силно свързване вътре в общността ($K_{вътр} = 4.0$) и слабо между общностите ($K_{външ} = 0.25$). Резултатът е недвусмислен – образуват се два тесни, взаимно разфазирани клъстера. Вътрешната подреденост на всяка общност е $r_A = r_B = 0.999$, докато глобалната подреденост остава едва r = 0.45. Това е количественият подпис на многоклъстерно състояние: висока локална, ниска глобална кохерентност.

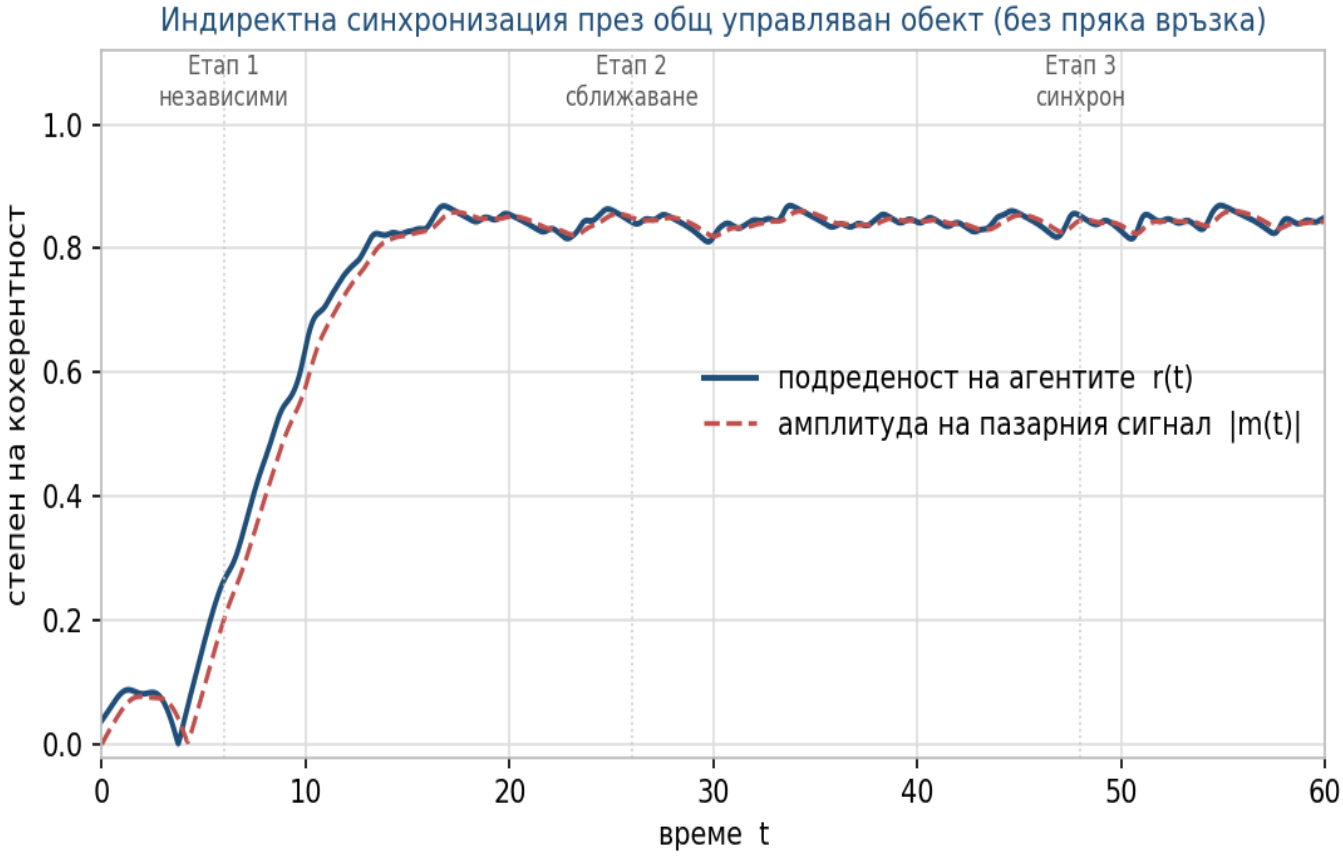


Фиг. 4. *Две честотни групи → два фазово-заключени клъстера (rA = rB = 0.999; r_глоб. = 0.45)*

5.6. Индиректна синхронизация през общ обект

Фигура 5 проверява централния практически сценарий: 120 агента без никаква пряка връзка помежду си, свързани единствено чрез общ управляван обект по уравнения (4)–(5). Виждат се три

етапа, каквито наблюдава и интерактивната симулация: (1) независими заявки и разпръснато поведение; (2) сближаване, когато пазарният сигнал |m(t)| започне да нараства; (3) синхрон, при който агентите и обектът се стабилизират. Крайната подреденост достига r ≈ 0.85 – тоест общият обект сам по себе си е достатъчен посредник за синхронизацията. Това е решаващото доказателство на хипотезата H.



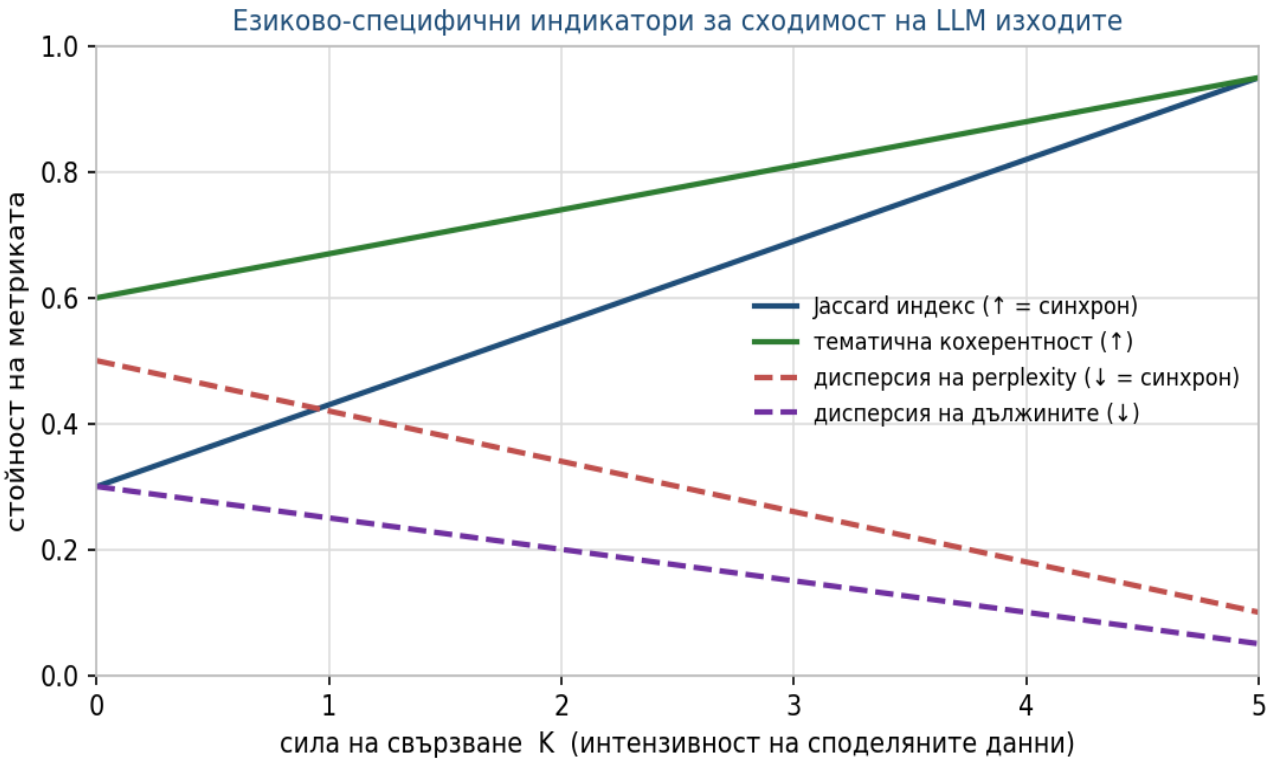
Фиг. 5. *Синхронизация само чрез споделен обект (без пряко свързване); финално r ≈ 0.85*

5.7. Езиково-специфични индикатори

Абстрактната фаза θ намира конкретен израз в наблюдаеми характеристики на текстовите изходи. Фигура 6 проследява четири такива индикатора спрямо K: индексът на Жакар за припокриване на ключови думи и тематичната кохерентност нарастват, а дисперсията на перплекията и дисперсията на дължините на отговорите спадат. И четирите се движат синхронно с параметъра на подреденост – потвърждение, че фазовата синхронизация се проявява като реална конвергенция на съдържанието, а не само като абстрактна метрика.

5.8. Обобщение на резултатите

Шестте експеримента образуват свързана верига на доказателството: съществува праг (фиг. 2), над него настъпва синхронизация във времето (фиг. 1) и в пространството на фазите (фиг. 3); при разнородна популация синхронизацията се разпада на **множество клъстери** (фиг. 4); синхронизация възниква и без пряка връзка, само през общия обект (фиг. 5); и всичко това има измеримо езиково изражение (фиг. 6). Взети заедно, резултатите потвърждават хипотезата H.



Фиг. 6. *Езикови индикатори за сходимост на изходите като функция на K*

6 От синхронизация към клъстеризация

6.1. Условия за клъстеризация

Резултатите очертават три режима според свързаността и хомогенността на популацията. При ниско K доминира некохерентност – множество разнообразни, независими изходи. При високо K и еднородна популация настъпва глобална синхронизация – един доминиращ клъстер, който е най-опасен за разнообразието на пазара. При умерено K и разнородна популация се установява многоклъстерен режим – няколко устойчиви коалиции. Реалните екосистеми от LLM почти сигурно попадат в последните два режима, защото данните се споделят интензивно, а моделите се групират около малък брой доставчици и обучаващи корпуси.

6.2. Мащабируемост с броя на агентите

Съществен е фактът, че праговото поведение не отслабва с растежа на N - напротив, при по-голяма популация преходът става по-добре дефиниран, а флуктуациите от краен размер под прага намаляват. С други думи, колкото повече автоматизирани търговци навлизат на един пазар, толкова по-надеждно и по-рязко системата се клъстеризира, щом свързаността надхвърли K_c. Тъй като и броят агенти, и интензивността на споделяните данни растат, тенденцията към клъстеризация е самозасилваща се.

6.3. Обхват на валидност и ограничения

Моделът на Курамото е съзнателно минимален и това е едновременно неговата сила и неговото ограничение. Той улавя универсалния механизъм на фазова синхронизация, но абстрахира редица особености на реалните LLM: изходите им са високоразмерни (не една фаза), взаимодействието не е строго синусоидално, а свързването може да е насочено и с времево закъснение. Тези усложнения обаче по правило понижават, а не повишават прага за синхронизация

– насочените връзки и закъсненията могат да породят допълнителни колективни режими (бягащи вълни, химери), но рядко премахват самата тенденция към клъстеризация. Затова изводите тук следва да се разглеждат като консервативна долна граница на реалния риск, а не като негово завишаване. Прецизното пренасяне върху конкретна система изисква емпирично оценяване на ефективното свързване K и на разпределението $g(\omega)$ от наблюдавани данни.

7 Системни рискове и последици

7.1. Спонтанни „картели“ и манипулация на пазари

Клъстеризацията означава, че независими алгоритмични търговци започват да действат съгласувано **„без умисъл”** – възниква спонтанен „картел“, който генерира изкуствени пазарни тенденции, продукт на системните особености на автоматизираните участници, а не на реалното търсене и предлагане. Този режим създава две опасности: непредвидими колективни движения (внезапни, самоусилващи се тенденции) и уязвимост към целенасочена манипулация – достатъчно е да се въздейства върху общия сигнал, за да се повлияе на целия синхронизиран клъстер. Изследвания върху алгоритмичното ценообразуване вече документират, че самостоятелно обучаващи се агенти достигат до колузивни равновесия без комуникация помежду си [6].

7.2. Социални мрежи и информационна среда

Същият механизъм е приложим и към генераторите на съдържание. Синхронизирани LLM в социалните мрежи могат съгласувано да насаждат страх или внушения, да проектират необосновани очаквания, да разпространяват политически послания и дезинформация, да формират изкуствени потребности и да реализират „прозорец на Овъртон“. Тъй като над 70% от търсенията и взаимодействията в интернет се изместват към ИИ системи, синхронизираното поведение на тези системи придобива непропорционално голямо влияние върху обществените нагласи.

7.3. Загуба на цифров суверенитет

Клъстеризацията се задълбочава от концентрацията: моделите се обучават върху ограничен брой общи корпуси и се доставят от малък брой компании. Липсата или доминацията на определени данни в корпусите формира отклонени оценки; въведените етични ограничения могат да свият когнитивните възможности; а използването на непроверени външни **„LLM защитници“ и „LLM атакуващи“** намалява логическата прозрачност на мерките за сигурност. Всичко това ерозира способността на държавите самостоятелно да контролират развитието, внедряването и използването на ИИ в критичните си инфраструктури.

7.4. Загуба на когнитивен капацитет

Успоредно с това постоянното разчитане на ИИ води до атрофия на критичното мислене, деградация на специализирани умения, намаляване на творческия капацитет, ерозия на паметта и концентрацията и загуба на контекстуално разбиране. В условия на такъв когнитивен „недоимък“ синхронизираните ИК системи срещат все по-малко човешка съпротива, което допълнително усилва техногенното влияние и го поставя в ръцете на малък брой високотехнологични компании.
Тук е уместна и една епистемологична бележка. Реципрочният принцип на Хайзенберг в контекста на управлението гласи, че наблюдаващият променя поведението си според наблюдаваното. При автоматизираните ИИ системи този контур е автоматизиран и ускорен: агентът адаптира действията си спрямо обекта, който сам оформя – точно контурът от уравнения (4)–(5). Това предопределя множество слабопредвидими ефекти, от които клъстеризацията е само най-осезаемият.

8 Заключения

Потвърдена клъстеризация. Числените експерименти доказват, че множество LLM, въздействащи върху общ процес или пазар, се самосинхронизират и клъстеризират; съществува остър критичен праг $K_c \approx 1.60$, над който подредеността нараства скокообразно.

- **Клъстеризация без пряка връзка.** Синхронизация настъпва дори когато агентите не са свързани помежду си, а само чрез общия управляван обект – практически най-важният и най-трудно откриваем сценарий (фиг. 5, r ≈ 0.85).

- **Многоклъстерни коалиции.** При разнородна популация се формират няколко вътрешно синхронизирани клъстера (r локално ≈ 1) при ниска глобална подреденост – количественият подпис на спонтанни „картели“.

- **Самозасилваща се тенденция.** Тъй като броят на агентите и интензивността на споделяните данни растат, ефективното свързване се движи към и отвъд прага; при по-голям N преходът става по-рязък, а не по-мек.

- **Системни рискове.** Клъстеризацията поражда пазарна манипулируемост, синхронизирано въздействие върху информационната среда, ерозия на цифровия суверенитет и на когнитивния капацитет на хората.

Забележка: При подготовката на доклада са използвани инструменти и технологии с интегрирани ИИ.

Приложение А. Параметри на симулациите

За възпроизводимост по-долу са обобщени ключовите настройки на всеки числен експеримент. Всички симулации използват интегриране по метода на Ойлер със стъпка dt = 0.01 и фиксирано начално зърно на генератора на случайни числа. Свързването е all-to-all (средно-полево), освен за фигура 4, където е блоково (две общности), и за фигура 5, където е индиректно през общ обект по уравнения (4)–(5).

Таблица 3. *Обобщени параметри и резултати на шестте числени експеримента*

Експ.	N	Разпределение g(ω)	Свързване K	Свързаност	Резултат (r)
Фиг. 1	200	N(0, 1)	0.5 … 5.0	all-to-all	0.05 … 0.98
Фиг. 2	500	N(0, 1)	0 … 4.0 (скан)	all-to-all	преход при Kc ≈ 1.60
Фиг. 3	60	N(0, 1)	3.0	all-to-all	0.13 → 0.92
Фиг. 4	300	две групи ±0.9	Квътр=4.0, Квнеш=0.25	блоково	rA=rB=0.999; rглоб=0.45
Фиг. 5	120	N(0, 1)	2.6 (ефективно)	индиректно (обект)	0.85
Фиг. 6	–	аналитични индикатори	0 … 5.0	–	монотонна сходимост

ЛИТЕРАТУРА:

[1] Kuramoto Y. Self-entrainment of a population of coupled non-linear oscillators. In: International Symposium on Mathematical Problems in Theoretical Physics. Lecture Notes in Physics, Vol. 39, Springer, 1975, pp. 420–422.

[2] Kuramoto Y. Chemical Oscillations, Waves, and Turbulence. Springer-Verlag, Berlin, 1984.

[3] Strogatz S. H. From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. Physica D: Nonlinear Phenomena, Vol. 143, No. 1–4, 2000, pp. 1–20.

[4] Acebrón J. A., Bonilla L. L., Pérez Vicente C. J., Ritort F., Spigler R. The Kuramoto model: A simple paradigm for synchronization phenomena. Reviews of Modern Physics, Vol. 77, No. 1, 2005, pp. 137–185.

[5] Pikovsky A., Rosenblum M., Kurths J. Synchronization: A Universal Concept in Nonlinear Sciences. Cambridge University Press, 2001.

[6] Calvano E., Calzolari G., Denicolò V., Pastorello S. Artificial Intelligence, Algorithmic Pricing, and Collusion. American Economic Review, Vol. 110, No. 10, 2020, pp. 3267–3297.

[7] Атанасов В., Иванова А. Анализ на програмните модели за автоматизиране на когнитивни процеси. Стратегии на образователната и научната политика, Vol. 32, № 5s, 2024, ISSN 1310-0270. https://doi.org/10.53656/str2024-5s-24-ana

[8] Алексиева А. Е., Кулев Н. З., Манов Л. Е. Личностова персонификация на големи езикови модели на базата на IPIP-50. Сборник доклади от научна конференция „Актуални проблеми на сигурността“, НВУ „Васил Левски“, Велико Търново, 2026, с. 807–814. ISSN 2367-7473 (PDF).

MODEL OF A WEB-BASED INFORMATION SYSTEM "DIPLOMANT"*

PAVEL S. TODOROV, VALENTIN T. ATANASOV

ABSTRACT: *The paper presents a model of a web-based information system, "Diplomant", designed to support and facilitate the administrative management of the student thesis development process through a dedicated set of features. The model integrates several technologies, including a React-based client, a Spring Boot REST server, PostgreSQL for data storage, and JWT-based access control. A key contribution of the proposed model is an algorithm for detecting duplicate and similar thesis topics. The algorithm normalizes the input text and calculates a combined similarity score based on containment, Jaccard, Dice and trigram n-gram measures. The developed prototype was deployed in a containerized environment and verified through functional scenarios covering authentication, record management, reporting and topic similarity analysis.*

KEYWORDS: *web information system, thesis management, topic similarity, REST API, Spring Boot, React, PostgreSQL*

DOI: https://doi.org/10.46687/MT26PST

МОДЕЛ НА УЕБ БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА „ДИПЛОМАНТ"

ПАВЕЛ С. ТОДОРОВ, ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *В статията е представен модел на УЕБ базирана информационна система „Дипломант", предназначена да подпомага административното управление на процеса по разработване на дипломни работи чрез специализиран набор от функционалности. Моделът интегрира клиентска част, реализирана с React, REST сървър със Spring Boot, PostgreSQL за съхранение на данните и JWT за контрол на достъпа. Основен принос на предложения модел е алгоритъмът за откриване на дублиращи се и сходни теми. Алгоритъмът нормализира входния текст и изчислява комбинирана оценка на сходството чрез containment, Jaccard, Dice и триграмна n-gram метрика. Разработеният прототип е разгърнат в контейнеризирана среда и е проверен чрез функционални сценарии за удостоверяване, управление на записи, справки и анализ на сходството на теми.*

1 Въведение

Административното управление на дипломанти във висшите училища изисква работа с множество взаимосвързани данни: имена на студенти, специалности, образователно-квалификационна степен, теми на дипломни работи, научни ръководители, сесии за защита и файлове с цифровата версия на разработките. При широкоразпространената практика за поддържане на информация в отделни електронни таблици или неформални списъци се увеличава рискът от непълнота, дублиране, различно изписване на едни и същи стойности и затруднено изготвяне на справки. Този проблем има не само организационен, но и инженерно-информационен характер, защото изисква модел на данните, правила за достъп, стандартизирано въвеждане и сложни механизми за контрол [3, 11].

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии"

Обект на настоящата статия е моделът на УЕБ базираната информационна система „Дипломант“. Системата е разработена като прототип, чиито основни функционални характеристики са централизиране на данните за дипломантите, подпомагане на служители и преподаватели при въвеждане, редакция, търсене, справки и проверка на теми. Акцентът е поставен върху моделната структура и върху алгоритъма за откриване на сходство на теми, тъй като именно тази функционалност отличава системата от обикновен регистър.

Целта на публикацията е да представи основните елементи на разработката, включително концептуалния, функционалния и архитектурния модел на системата, както и подхода за автоматизирана проверка за дублиращи се и сходни формулировки на дипломни теми. По този начин системата се разглежда не само като програмен продукт, а и като възможно инженерно решение за конкретен административен процес.

2 Модел и основни изисквания към системата

„Дипломант“ е проектирана като вътрешна административна система, а не като публичен портал. Това решение е обосновано, защото данните за дипломанти и теми не трябва да бъдат видими за всички студенти. В системата са предвидени две основни роли: администратор и оператор. Операторът работи със записите за дипломанти, файловете и справките, докато администраторът поддържа номенклатурите, от които зависи еднородността на данните.

Централният обект в модела е компонентът „Дипломант“. Той обединява лични данни, академична информация, тема на дипломната работа, научен ръководител, година на защита, дата на държавна изпитна сесия и връзка към файл. Допълнителни обекти са „Потребител“, „Номенклатурна стойност“ и „Лог за вход“. Обектът „Потребител“ осигурява удостоверяване и ролеви достъп, номенклатурните стойности стандартизират изборите във формите, а логът за вход дава минимална проследимост на достъпа. Концептуалният модел на системата е представен на фиг. 1.

Функционалният модел може да бъде разгледан като последователен работен процес. Потребителят влиза в системата чрез потребителско име и парола. След успешно удостоверяване и упълномощаване получава достъп до списък с дипломанти, където може да търси, добавя, редактира или изтрива записи. При добавяне или редакция на тема системата изпълнява проверка за точно съвпадение и анализ на сходство. Данните могат да бъдат използвани за справки и експортирани като PDF документ.

Основните функционални изисквания включват удостоверяване, управление на записи, работа с номенклатури, прикачване и достъп до файлове, справки, PDF експорт, помощна система и откриване на конфликти при сходни теми. Нефункционалните изисквания са свързани със сигурност, надеждност, поддържаемост, удобство на интерфейса и възможност за разгръщане в реална мрежова среда. Формализираната проверка на темите представлява ограничен експертен елемент, който подпомага, но не заменя човешката преценка [1].

3 Архитектура и модел на данните

Архитектурата на системата следва многослоен УЕБ модел с ясно разделени отговорности [2, 4, 5]. Клиентската част е реализирана с React, Vite и Material UI [8]. Тя отговаря за потребителското взаимодействие, визуализацията на списъци и форми, адаптивното поведение и извеждането на резултатите от анализа на теми. Сървърната част е разработена със Spring Boot [7] и предоставя REST API за вход, управление на дипломанти, номенклатури, файлове и справки. Защитата е реализирана чрез Spring Security

и JWT [6], което позволява удостоверяване без съхраняване на състояние, подходящо за едностранично приложение.

Слоят за достъп до данни използва Spring Data JPA, а базата данни е PostgreSQL [9]. Схемата се управлява чрез Flyway миграции, което позволява контролирано развитие на структурата и еднакво прилагане на промените в локална и сървърна среда. Разгръщането е организирано чрез Docker Compose [10] с отделни контейнери за базата данни, приложението на задния край и приложението на предния край, обслужвано чрез nginx.

Релационният модел включва таблици за дипломанти, потребители, номенклатури, логове за вход и история на миграциите. Таблицата за дипломанти съдържа основните административни атрибути, а номенклатурите обхващат форма на обучение, специалност, ОКС и научен ръководител. Този подход намалява свободното въвеждане на критични стойности и повишава надеждността на справките. При бъдещо развитие моделът може да се разшири със статуси, история на действията, отделна таблица за файлове и интеграция с университетски регистри.



Фиг. 1. Концептуален модел на информационната система „Дипломант“

4 Алгоритъм за проверка на сходство на теми

Проверката на темите е ключовата специфична функционалност на системата. В университетска среда е нежелателно една и съща или почти една и съща тема да бъде предложена повторно, без това да бъде забелязано. Ръчното сравнение на всички вече въведени теми е бавно и несигурно, особено когато формулировките се различават по пунктуация, словоред или малки езикови изменения. Затова в системата е реализиран помощен алгоритъм, който не заменя експертната преценка, но сигнализира за потенциален конфликт.

Алгоритъмът започва с нормализация на текста: преобразуване до малки букви, премахване на пунктуация, изчистване на излишни интервали и опростена обработка на някои български словоформи. След това темата се разделя на ключови думи, които се използват при изчисляване на различни показатели за близост. Ако нормализираният текст съвпада напълно с вече съществуваща тема, системата връща конфликт и не допуска запис. Ако няма точно съвпадение, се изчислява процент на сходство.

Комбинираната оценка е съставена от четири компонента: containment similarity, Jaccard similarity, Dice similarity и триграмно n-gram сходство. Използването на повече от една метрика е целесъобразно, защото кратките заглавия на дипломни работи могат да бъдат близки по различни начини (табл. 1). Една метрика отчита включване на думи, друга отчита общи множества, трета е чувствителна към припокриване на токени, а триграмното сходство помага при близки текстови форми.

$$S = 0{,}35 \cdot C + 0{,}20 \cdot J + 0{,}20 \cdot D + 0{,}25 \cdot T,$$

където C е containment показател, J е Jaccard показател, D е Dice показател, а T е триграмно сходство. Теглата са избрани така, че по-голямо значение да има включването на ключови думи, без да се пренебрегва структурната близост на текста.

Таблица 1. Компоненти на комбинираната оценка за сходство

Компонент	Роля в оценката	Тегло
Containment (C)	Открива дали думите от едната тема се съдържат в другата.	0,35
Jaccard (J)	Сравнява общите и всички различни ключови думи.	0,20
Dice (D)	Оценява припокриването между множествата от токени.	0,20
Trigram (T)	Отчита близост между текстови фрагменти и малки промени.	0,25

Полученият процент се интерпретира в няколко диапазона: ниско сходство, частично сходство, силно сходство и почти идентични теми. При частично или силно сходство системата показва най-близките записи, ръководителя и годината. Така потребителят може да прецени дали формулировката е допустимо близка, дали е необходимо преформулиране или дали темата трябва да бъде отхвърлена. Решението остава човешко, но е подпомогнато от автоматизирана проверка.

5 Реализация и експериментална проверка

Прототипът е реализиран като разделено приложение с преден край и заден край. Модулите на задния край включват контролери, услуги, слой за достъп до данни, класове за обекти, DTO модели и конфигурация за сигурност. Основни крайни точки са /api/auth/login за вход, /api/diplomanti за работа със записи, /api/diplomanti/topic-analysis за анализ на теми, /api/nomenclatures за номенклатури и крайни точки за файлове и справки. Отделянето на анализа на теми като самостоятелна крайна точка е оправдано, защото той

не е стандартна операция по създаване, преглед, редакция или изтриване, а аналитична проверка върху съществуващите данни.

Потребителският интерфейс е организиран около основните административни действия. След вход потребителят вижда списък с дипломанти, търсене и действия за редакция, изтриване, преглед и сваляне на файл. Формата за добавяне и редакция е разделена на секции: лични данни, тема, академична информация, защита и файл. Справките са отделени в самостоятелен екран с филтри и възможност за PDF експорт. За малки екрани широките таблици се заменят с картов изглед, което подобрява четимостта. При достъп през мобилни устройства трябва да се отчита и сигурността на използваното устройство [12].

Експерименталната проверка обхваща както автоматизирани, така и ръчни сценарии. Проверени са успешен вход и издаване на JWT токен, отказ при достъп без токен, създаване на дипломант, блокиране на дублираща тема, нормализация на тема с различна пунктуация, връщане на сходни теми, работа с номенклатури, качване на файл и генериране на справка. Резултатите показват, че прототипът изпълнява поставените изисквания и може да бъде стартиран в контейнеризирана среда върху реален сървър.

Ограниченията на разработката са характерни за прототип. Алгоритъмът за сходство е евристичен и не използва пълна морфологична лематизация или семантични модели. Липсва и разширен одит на всички действия. Въпреки това системата демонстрира приложим подход за комбиниране на административен регистър с ограничен експертен механизъм за контрол на теми.

6 Заключение

Представеният модел на УЕБ базирана информационна система „Дипломант“ показва как специфичен университетски административен процес може да бъде формализиран и реализиран като съвременно УЕБ приложение. Системата обединява защитен достъп, управление на дипломанти, номенклатури, файлове, справки и PDF експорт в единна работна среда. Използваната архитектура с React, Spring Boot, PostgreSQL, JWT и Docker осигурява ясно разделение на отговорностите и възможност за възпроизводимо разгръщане.

Най-същественият принос е модулът за проверка на сходство на теми. Той превръща част от експертната логика в автоматизирана помощна проверка, като комбинира няколко текстови метрики и предоставя интерпретируем резултат. Така системата не взема окончателно решение вместо преподавателя или администратора, но намалява вероятността от пропуск при повторно или близко формулирана тема.

Като бъдещо развитие могат да се посочат по-подробна история на действията, разширени справки, интеграция с университетски информационни системи и по-дълбок езиков анализ чрез лематизация или семантични представяния на текст. Тези разширения биха превърнали прототипа в по-пълноценна производствена система.

ЛИТЕРАТУРА:

[1] Атанасов, В. Експертни информационни системи. Учебни материали за магистърска програма, Шуменски университет „Епископ Константин Преславски“, 2022.

[2] Цанков Ц., Ненков Н. Възможностите на отдалечени клиенти в архитектурата клиент-сървър. Сборник статии от XII международна научна конференция „Инновации в технологиях и образовании“, филиал на КузГТУ в г. Белово, 2019, ISBN 978-5-00137-063-5, с. 342–346.

[3] Laudon, K. C., Laudon, J. P. Management Information Systems: Managing the Digital Firm. Pearson, 2022.

[4] Fielding, R. T. Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation, University of California, Irvine, 2000.

[5] Richardson, L., Ruby, S. RESTful Web Services. O’Reilly Media, 2007.

[6] RFC 7519. JSON Web Token (JWT). Internet Engineering Task Force, 2015. Available: https://www.rfc-editor.org/rfc/rfc7519.

[7] Spring Boot Reference Documentation, version 3.2.x. Available: https://docs.spring.io/spring-boot/.

[8] React Documentation. Available: https://react.dev/.

[9] PostgreSQL 16 Documentation. Available: https://www.postgresql.org/docs/16/.

[10] Docker Compose Documentation. Available: https://docs.docker.com/compose/.

[11] Кемил И., Симеонова И. Дигитализация и предизвикателствата пред сигурността в електронната администрация. Научна конференция на НВУ „Васил Левски“, Велико Търново, 12–14 ноември 2025.

[12] Stoyanova, V. Problems with Information Security on Mobile Devices. Industry 4.0, 2019, p. 200. https://stumejournals.com/journals/i4/2019/4/200

EXPLAINABLE ARTIFICIAL INTELLIGENCE IN VIDEO SURVEILLANCE FOR CRITICAL INFRASTRUCTURE*

SILVIA H. NIKOLOVA, SIMONA S. HRISTOVA

ABSTRACT: *The deployment of intelligent video surveillance in energy facilities, transport hubs, ports, industrial plants and communication centers improves incident detection, but introduces a major risk: safety-relevant decisions may be produced by opaque models whose rationale is not understandable to operators. This paper proposes a multilayer explainable artificial intelligence architecture combining object detection and tracking with visual, temporal, counterfactual and textual explanations. The main contribution is a dual-channel reliability mechanism in which every alarm is assessed by model confidence and explanation quality. Metrics for fidelity, stability, spatial overlap, temporal consistency, latency and human trust are defined, together with an error-analysis procedure for false-positive and false-negative decisions. The approach strengthens human oversight, auditability and risk management while preserving human authority over high-consequence decisions.*

KEYWORDS: *explainable artificial intelligence, XAI, intelligent video surveillance, critical infrastructure, Grad-CAM, SHAP, error analysis, trust, human oversight*

DOI: https://doi.org/10.46687/MT26SHN

ОБЯСНИМ ИЗКУСТВЕН ИНТЕЛЕКТ (EXPLAINABLE AI) ВЪВ ВИДЕОНАБЛЮДЕНИЕТО ЗА КРИТИЧНА ИНФРАСТРУКТУРА

СИЛВИЯ Х. НИКОЛОВА, СИМОНА С. ХРИСТОВА

АБСТРАКТ: *Разширяването на интелигентното видеонаблюдение в енергийни обекти, транспортни възли, пристанища, промишлени предприятия и комуникационни центрове увеличава скоростта на откриване на инциденти, но създава нов риск: критично решение може да бъде взето от непрозрачен модел, чиито основания не са разбираеми за оператора. Предлага се многослойна архитектура за обясним изкуствен интелект (XAI), която свързва детекцията и проследяването на обекти с визуални, времеви, контрафактуални и текстови обяснения. Основният принос е двуканален механизъм за надеждност, при който всяка аларма се оценява едновременно по увереността на модела и качеството на обяснението. Формулирани са показатели за вярност, стабилност, пространствено припокриване, времева последователност, латентност и човешко доверие, както и процедура за анализ на фалшиви положителни и фалшиви отрицателни решения.*

1 Въведение

Критичната инфраструктура включва обекти и услуги, чието прекъсване може да засегне обществената безопасност, икономиката и националната сигурност [1]. Видеонаблюдението в подобна среда вече не се ограничава до запис и визуален контрол. Съвременните системи откриват проникване, пожар и дим, оставени предмети, опасно приближаване до зона, необичайна траектория, падане на човек или аварийно събитие. Прилаганите дълбоки невронни мрежи обаче често функционират като „черни кутии“: изходът е наличен, но причината за него остава скрита. Развитието на интелигентните камери и методите за откриване на видеоаномалии е разгледано в [6, 16, 17], а концепциите и направленията на обяснимия ИИ – в [18–20].

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Проблемът е особено съществен при аларми с висока цена на грешката. Фалшиво положителното решение може да прекъсне производствен процес, да задейства евакуация или да натовари охранителен екип. Фалшиво отрицателното решение може да пропусне проникване, пожар или саботаж. В двата случая една стойност на увереността, например 0,92, не е достатъчна: операторът трябва да разбере кой обект, зона, времева промяна или комбинация от признаци е довела до алармата.

Целта е да се предложи архитектура и методика за XAI във видеонаблюдението на критична инфраструктура, които: визуализират основанията на модела; измерват качеството на обяснението; подпомагат калибрираното доверие, а не безусловното приемане; и превръщат грешките в структурирана обратна връзка за подобряване на системата.

2 Свързани изследвания и нормативен контекст

LIME изгражда локален интерпретируем заместител около конкретна прогноза [2], а SHAP разпределя приноса на признаците чрез стойности на Шапли [3]. При конволюционни мрежи Grad-CAM използва градиентна информация, за да локализира областите, повлияли върху класа [4]. Варианти като Ablation-CAM, Score-CAM и F-CAM целят по-стабилна или по-прецизна локализация [5, 7, 8]. За видеоанализ обяснението трябва да обхваща не само пиксели, а и движение, траектория, последователност от кадри и контекст на зоната. EVAL локализира видеоаномалии и предоставя разбираеми основания чрез признаци за външен вид и движение [9].

NIST формулира четири принципа за обясним AI: системата да предоставя обяснение, обяснението да е смислено за конкретния потребител, да отразява точно процеса на системата и да обозначава границите на знанието си [10]. Европейският AI Act изисква високорисковите AI системи да бъдат достатъчно прозрачни за правилно интерпретиране на изхода и поставя акцент върху човешкия надзор и регистрирането на събития [11]. Класификацията на конкретната система зависи от нейното предназначение и внедряване; XAI не отменя необходимостта от правна оценка.

Критична слабост на post-hoc методите е възможността обяснението да изглежда убедително, без да е вярно спрямо вътрешната логика на модела. При решения с висок залог следва да се предпочитат интерпретируеми модели, когато това е възможно [12]. Салийнси картите могат да бъдат нестабилни или нечувствителни към параметрите на модела [13, 14]. Поради това обяснението трябва да се разглежда като измерим обект, подлежащ на валидация. Устойчивостта и стабилността на обясненията са предмет на отделни изследвания [15]. Разпознаването на частично видими обекти, невронните мрежи и трансферът на знания са разгледани в [23–25].

3 Предложена XAI архитектура

Архитектурата е организирана в шест функционални слоя. Потокът започва от камери и допълнителни IoDT сензори, преминава през детекция и проследяване, след което паралелно се формират решение и обяснение. Двата резултата се обединяват в модул за оценка на надеждността, преди алармата да достигне до оператор.

Табл. 1. Функционални слоеве на предложената архитектура

Слой	Основни функции	XAI резултат
Данни	RGB/IR/термално видео, метаданни, зони, сензори	Произход, качество, синхронизация
Възприятие	Детекция, сегментация, проследяване, оптичен поток	Обекти, траектории, релевантни кадри
Решение	Класификация на събитие и оценка на риск	Клас, вероятност, праг, алтернативи
Обяснение	Grad-CAM/SHAP, правила, контрафактуални примери	Къде, кога, кои признаци и защо
Контрол	Fidelity, stability, latency, drift, OOD	Валидност на обяснението
Интерфейс	Аларма, replay, heatmap, текст, обратна връзка	Ролево адаптирано обяснение

3.1 Двуканална оценка на алармата

Нека p(y|x) е увереността на детектора за клас y при видеофрагмент x, а q(e|x,y) е качеството на обяснението e. Комбинираната надеждност на алармата се дефинира като:

$$R_a = w_1 \cdot p(y|x) + w_2 \cdot F(e) + w_3 \cdot S(e) + w_4 \cdot T(e) - w_5 \cdot U(x),\ \Sigma w_i = 1,$$

където F е вярност на обяснението, S – стабилност при малки промени на входа, T – времева последователност, а U – неопределеност или индикатор за вход извън обучаващото разпределение. Висока увереност при ниско качество на обяснението не води автоматично до критична аларма, а до режим „изисква проверка“.

3.2 Ролево адаптирани обяснения

Оператор: кратка причина, маркирана зона, ключови кадри, времева линия и препоръчано действие.

Инженер/ML специалист: attribution карта, прагове, embedding сходство, версия на модела, OOD и drift индикатори.

Одитор: неизменяем журнал на входа, решението, обяснението, човешката реакция и последващия резултат.

Ръководител: агрегирани тенденции, грешки по сценарий, средно време за потвърждение и доверие на операторите.

4 Методи за визуализация на решенията

Едно обяснение не е достатъчно за всички типове събития. Пространствените методи са подходящи за наличие на обект или дим; времевите методи са необходими за поведение и траектория; контрафактуалните обяснения показват минималната промяна, която би променила решението; текстовите обяснения обобщават техническия резултат за оператора.

Табл. 2. Комбиниране на XAI методи според задачата

Метод	Основен въпрос	Подходящ пример	Ограничение
Grad-CAM / Score-CAM	Къде гледа моделът?	Дим, оръжие, нарушител	Груба локализация; нестабилност
SHAP / LIME	Кои признаци влияят?	Сензорно-видео сливане	Цена; локална апроксимация
Времева attribution карта	Кога възниква основанието?	Падане, бой, опасна траектория	Зависи от времевия прозорец
Контрафактуално обяснение	Какво би отменило алармата?	Без зона Z няма аларма	Физическа реалистичност
Правила/концепции	Кое правило е изпълнено?	Човек + забранена зона + нощ	Ограничено ново покритие

5 Показатели за качество на обяснението

Вярността измерва доколко обяснението отразява действителното поведение на модела. При маскиране на най-релевантните области Ω_e може да се използва спадът на увереността:

$$F(e) = p(y|x) - p(y|x \odot (1 - \Omega_e)).$$

За пространствено обяснение със зададена експертна област Ωg се използва пресечението върху обединението:

$$IoU_e = |\Omega_e \cap \Omega g| \,/\, |\Omega_e \cup \Omega g|.$$

Стабилността сравнява обясненията при малка, семантично незначима промяна δ на входа:

$$S(e) = 1 - d(e(x), e(x+\delta)) / dmax,$$

където d може да бъде 1 − SSIM, cosine distance или разстояние между нормализирани attribution карти. За видео се добавя времева последователност:

$$T(e) = 1 - (1/(N-1)) \Sigma_{t=2}^{N} d(e_t, Warp(e_{t-1}, v_t)),$$

където Warp компенсира движението чрез оптичен поток v_t. Латентността L_e се измерва от получаването на кадъра до визуализиране на обяснението. Човешката ефективност се оценява чрез точност на операторското решение, време за потвърждение, калибрация на доверието и честота на правилно отхвърлени неверни аларми.

6 Методика за анализ на грешките

Анализът не приключва с матрица на объркване. Всяка грешка се записва като пакет: видеофрагмент, клас и увереност, обяснение, качество на входа, активни зони/правила, версия на модела, операторско решение и проверена причина. След това грешките се групират по механизъм, а не само по клас.

Табл. 3. Таксономия на грешките и коригиращи действия

Категория	XAI признак	Вероятна причина	Коригиращо действие
Фон/отражение	Heatmap извън обекта	Shortcut learning	Негативни примери; маскиране на фон
Оклузия	Прекъсната attribution област	Недостатъчна видимост	Мултикамерно сливане; OOD флаг
Осветление/време	Фокус върху ярък източник	Domain shift	Аугментация; IR/термален канал
Безопасно нетипично действие	Вярна зона, грешен клас	Слабо покритие на нормалното	Active learning; нови сценарии
Пропусната заплаха	Ниска/разсеяна карта	Малък обект/ниска чувствителност	Мултимащабен модел; нов праг
Нестабилно обяснение	Промяна между близки кадри	Чувствителност към шум	Temporal smoothing; regularization

7 Експериментална методология

За валидиране се предлага тестова среда с RGB и термални камери в четири сценария: нерегламентирано проникване, ранни признаци на пожар/дим, оставен предмет и опасно навлизане в технологична зона. Основният модел може да бъде YOLO-базиран детектор, комбиниран с DeepSORT/ByteTrack за траектории и temporal transformer за събития. XAI модулът включва Grad-CAM/Score-CAM, времева attribution карта и кратко правилно генерирано текстово обяснение. Данните се разделят по сцени, а не по кадри, за да се предотврати изтичане на визуално сходство между обучение и тест.

Оценката се провежда в три режима: A – само прогноза и увереност; B – прогноза с визуално обяснение; C – прогноза с визуално, времево и текстово обяснение плюс индикатор за качество. Регистрират се точност на потвърждението, време за реакция, калибрация на доверието и честота на automation bias. За статистическо сравнение могат да се използват repeated-measures ANOVA или Friedman тест според разпределението.

Резултатите в Табл. 4 са илюстративни симулационни стойности, предназначени да демонстрират начина на отчитане, и не следва да се цитират като реално проведен експеримент.

Табл. 4. Илюстративни симулационни резултати

Режим	Точност	Средно време	Отхвърлени FP	ECE
A: без XAI	84,6 %	18,4 s	61,2 %	0,142
B: визуално XAI	90,8 %	15,7 s	74,5 %	0,096
C: мултимодално XAI	94,1 %	13,9 s	82,7 %	0,061

Илюстративната тенденция показва очакваната полза от XAI: не просто повишаване на субективното доверие, а по-точно съгласуване между доверие и реална коректност. Намаляването на Expected Calibration Error (ECE) е важно, защото високото доверие в грешна аларма е по-опасно от умереното доверие в правилна аларма.

8 Доверие, човешки надзор и киберсигурност

Обяснимостта не гарантира автоматично доверие. Убедително визуализирана, но невярна heatmap може да увеличи automation bias. Затова интерфейсът трябва да показва и несигурността: качество на изображението, OOD предупреждение, стабилност на обяснението и конфликт между видео и други сензори. При висок риск операторът трябва да може да поиска повторен анализ, алтернативно обяснение или кадри от друга камера. Оценката на човешката надеждност чрез FMEA е разгледана в [21], а автоматизираното вземане на решения в контекста на GDPR – в [22].

XAI създава и нова повърхност за атака. Злонамерен вход може да запази класа, но да измести attribution картата или да създаде убедително обяснение за неправилно решение. Необходими са подписване на журналите, контрол на версиите, проверка на целостта на модела, adversarial тестове и ролево ограничен достъп до подробни обяснения.

9 Дискусия

Предложеният подход разглежда XAI като част от контура за безопасност, а не като допълнение към потребителския интерфейс. Предимството е съчетаването на четири вида прозрачност: пространствена („къде“), времева („кога“), признакова („кои фактори“) и контрафактуална („какво би променило решението“). Двуканалната оценка намалява вероятността уверена, но необяснима прогноза да бъде приета без проверка.

Ограниченията са свързани с допълнителна латентност, липса на универсален показател за качество и зависимостта на обясненията от аудиторията. Attribution методите не доказват непременно причинност. Необходимо е бъдещо изпитване с реални оператори, реални алармени журнали и различни типове критична инфраструктура, както и оценка на компромиса между точност, интерпретируемост, поверителност и киберсигурност.

10 Заключение

Предложена е архитектура за обясним изкуствен интелект във видеонаблюдението за критична инфраструктура, при която решението и обяснението се формират и проверяват като два взаимосвързани канала. Научно-приложният принос включва многослойно комбиниране на визуални, времеви, признакови и контрафактуални обяснения; формализирана оценка на вярност, стабилност, локализация, времева последователност и латентност; ролево адаптирана визуализация; и таксономия за превръщане на фалшивите аларми и пропуснатите събития в коригиращи действия. XAI повишава доверието само когато обясненията са проверени, несигурността е видима и човекът запазва реална възможност да оспори автоматизираното решение.

ЛИТЕРАТУРА:

[1] Диманова Д. В., Цанков Ц. С. Анализ състоянието на критичната инфраструктура за район Шумен. Годишник на Шуменския университет „Епископ К. Преславски“, Шумен, 2016, ISSN 1311-834X, с. 45–54.

[2] Ribeiro M. T., Singh S., Guestrin C. Why Should I Trust You?: Explaining the Predictions of Any Classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 1135–1144, DOI: 10.1145/2939672.2939778.

[3] Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems, Vol. 30, 2017.

[4] Selvaraju R. R., Cogswell M., Das A., Vedantam R., Parikh D., Batra D. Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization. Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2017, pp. 618–626, DOI: 10.1109/ICCV.2017.74.

[5] Ramaswamy H. G., et al. Ablation-CAM: Visual Explanations for Deep Convolutional Network via Gradient-free Localization. Proceedings of the IEEE Winter Conference on Applications of Computer Vision (WACV), 2020, pp. 983–991.

[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] Wang H., et al. Score-CAM: Score-Weighted Visual Explanations for Convolutional Neural Networks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020, pp. 24–25.

[8] Belharbi S., et al. F-CAM: Full Resolution Class Activation Maps via Guided Parametric Upscaling. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022, pp. 3490–3499.

[9] Singh A., Jones M. J., Learned-Miller E. EVAL: Explainable Video Anomaly Localization. arXiv preprint arXiv:2212.07900, 2022.

[10] Phillips P. J., et al. Four Principles of Explainable Artificial Intelligence. NIST Interagency/Internal Report (NISTIR) 8312, National Institute of Standards and Technology, 2021, DOI: 10.6028/NIST.IR.8312.

[11] European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union, 2024.

[12] Rudin C. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. Nature Machine Intelligence, Vol. 1, 2019, pp. 206–215, DOI: 10.1038/s42256-019-0048-x.

[13] Adebayo J., et al. Sanity Checks for Saliency Maps. Advances in Neural Information Processing Systems, Vol. 31, 2018.

[14] Ghorbani A., Abid A., Zou J. Interpretation of Neural Networks Is Fragile. Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 33, 2019, pp. 3681–3688, DOI: 10.1609/aaai.v33i01.33013681.

[15] Lakkaraju H., Arsov N., Bastani O. Robust and Stable Black Box Explanations. Proceedings of the 37th International Conference on Machine Learning, PMLR, Vol. 119, 2020, pp. 5628–5638.

[16] Sultani W., Chen C., Shah M. Real-World Anomaly Detection in Surveillance Videos. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 6479–6488.

[17] Kiran B. R., Thomas D. M., Parakkal R. An Overview of Deep Learning Based Methods for Unsupervised and Semi-Supervised Anomaly Detection in Videos. Journal of Imaging, Vol. 4, No. 2, 2018, Art. 36, DOI: 10.3390/jimaging4020036.

[18] Ali S., et al. Explainable Artificial Intelligence (XAI): What We Know and What Is Left to Attain Trustworthy Artificial Intelligence. Information Fusion, Vol. 99, 2023, Art. 101805, DOI: 10.1016/j.inffus.2023.101805.

[19] Arrieta A. B., et al. Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. Information Fusion, Vol. 58, 2020, pp. 82–115, DOI: 10.1016/j.inffus.2019.12.012.

[20] Gunning D., Aha D. DARPA's Explainable Artificial Intelligence (XAI) Program. AI Magazine, Vol. 40, No. 2, 2019, pp. 44–58, DOI: 10.1609/aimag.v40i2.2850.

[21] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M., Marinova G. Application of Failure Mode and Effects Analysis for Evaluating Human Reliability. Scientific Conference with International Participation MATTEH

2024, Conference Proceedings, Vol. 2, Shumen, 2024, ISSN 1314-3921, pp. 147–152. https://doi.org/10.46687/BOIK9859

[22] Simeonova I. How GDPR treats automated decision-making. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2025, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 164–175. https://doi.org/10.46687/jsar.v29i1.461

[23] Манов Л., Кулев Н. Откриване и разпознаване на частично видими обекти в оптични изображения с използване на техниките на изкуствения интелект – мини ревю от 1970 г. до 2000 г. DefTech 2023, 2023, с. 444–450. ISSN 2815-4282.

[24] Манов Л. Е. Съвременни технологии с изкуствен интелект за разпознаване на обекти с военно предназначение в оптични изображения: Компютърен експеримент с невронни мрежи в MATLAB. DefTech 2025, 2025, с. 714–722. ISSN 2815-4282.

[25] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

INVESTIGATION OF AN ELECTRONIC CONVERTER MODEL IN SIMULINK*

VASIL B. IVANOV

ABSTRACT: *A methodology for modeling an electronic converter– specifically, an inverter– is presented using the Matlab/Simulink environment and the Simulink and SimPowerSystems (SPS) libraries. Their integration combines simulation-based and functional modeling, enabling investigation and analysis in both the time and frequency domains.*

KEYWORDS: *Matlab/Simulink, SimPowerSystems (SPS) libraries, voltage inverters (DC/AC), power semiconductor devices (IGBTs), passive components (RLC)*

DOI: https://doi.org/10.46687/MT26VBI

ИЗСЛЕДВАНЕ МОДЕЛ НА ЕЛЕКТРОНЕН ПРЕОБРАЗУВАТЕЛ В SIMULINK

ВАСИЛ Б. ИВАНОВ

АБСТРАКТ: *Представена е методика за моделиране на електронен преобразувател - инвертор в среда Matlab/Simulink с използване на библиотеките Simulink и SimPowerSystems (SPS). Комбинирането между тях включва имитационно и функционално моделиране, позволяващ изследване и анализ както във времевата, така и в честотната област.*

1 Въведение

Електрическите системи захранвани с променлив ток се включват към обществената мрежа при спазване изискванията за номинални показатели на напрежението и честотата. Съвременните източници на напрежение, получени от работата на възобновяеми енергийни източници (ВЕИ) генерират постоянен ток като масиви от акумулаторни батерии и фотоволтаични модули (соларни панели). Електронните преобразуватели на постоянен ток в променлив ток са инвертори на напрежение (DC/AC) с изходни параметри позволяващи включване на променливотокови консуматори.

Публикацията въвежда в етапите на интегрална методика за моделиране на електронен преобразувател – инвертор. Синтезирани са основните етапи от създаване на модела в среда Matlab/Simulink с използване на библиотеките Simulink и SimPowerSystems (SPS) [2, 3]. Комбинирането между тях включва имитационно и функционално моделиране, позволяващо изследване и анализ както във времевата, така и в честотната област. Подобен подход за моделиране и изследване на трифазен инвертор посредством MATLAB/Simulink е приложен в [4].

Представени са стъпките по изграждане на конкретен модел чрез създаване на работно поле, избор и свързване на елементи, задаване на начални условия и избор на числен метод за решаване на диференциалните уравнения. Приложеният анализ FFT от блока Powergui определя спектралните компоненти чрез амплитудно-честотните им характеристики (АЧХ) като отчита в проценти общото хармонично изкривяване на тока и напрежението, съответно

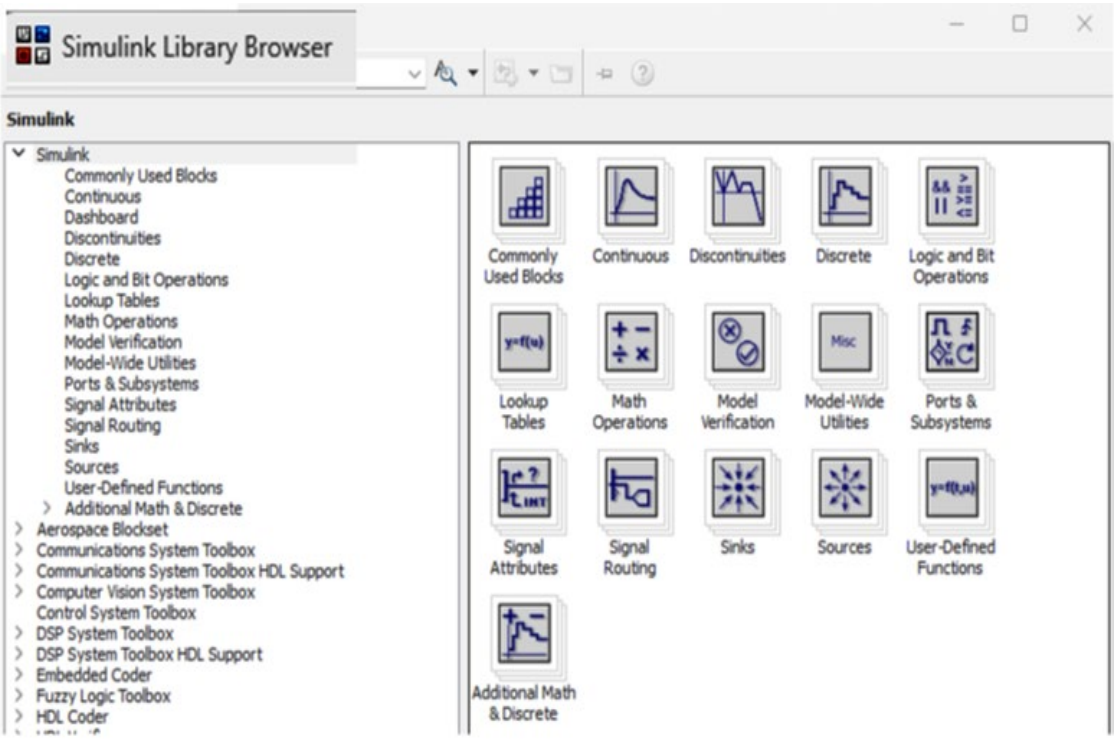
* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

THDI и THDU [5]. Резултатите от симулацията се представят чрез графичен и числен анализ за оценка на качествените показатели на преобразуваната електрическа енергия, включително хармоничния състав на тока и напрежението [6]. Стандартът IEC 61000-4-7 определя общи изисквания и методика за измерване на хармонични и интерхармонични компоненти в електрозахранващи системи. Стандартът обхваща спектрални компоненти до 9 kHz при системи 50/60 Hz и разглежда измерването на хармонични напрежения и токове [7].

2 Методика за моделиране на блокови и принципни схеми чрез Matlab/Simulink. Етапи на виртуално моделиране в среда Simulink

Методиката обхваща и избора на силови полупроводникови елементи (IGBT) и пасивни компоненти (RLC), както и тяхната параметризация при изграждане на модели на силови вериги. Представено е моделиране на трифазен инвертор и неговото управление чрез широчинно-импулсна модулация. Моделирането в реален практически еквивалент е основа за експериментални изследвания и проектиране на реални силови електротехнически устройства и системи.

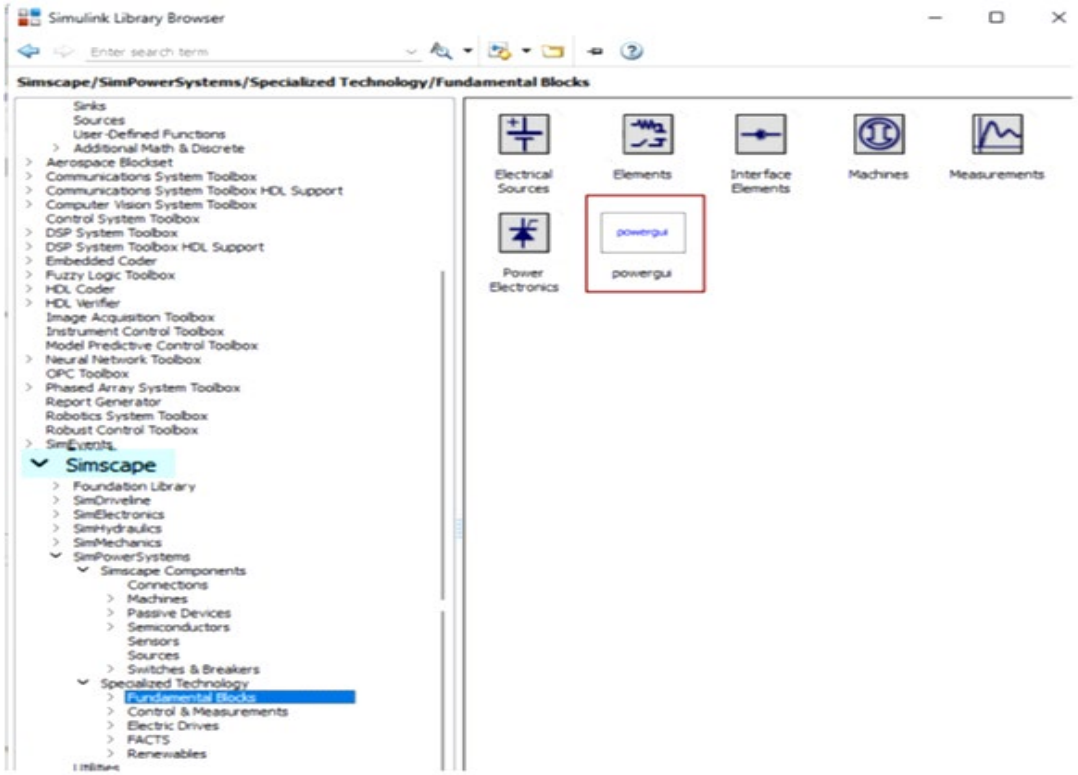
Програмният пакет Simulink е предназначен за моделиране на линейни и нелинейни динамични обекти. За целите на настоящото изследване се използват библиотеките на Simulink и SPS, както и командния апарат на Matlab. Приложението на MATLAB при изследване на преходни процеси в линейни електрически вериги и математическото им моделиране е разгледано в [9, 10]. Друг подход използва обобщени мрежи за моделиране на преходни процеси във верига от втори ред [8]. Библиотеката Simulink е организирана в дървовидна структура, визуализирана чрез диалоговия прозорец Simulink Library Browser (фиг. 1).



Фиг. 1. Библиотека на раздел Simulink Library Browser

Имената на блоковете от фиг. 1 задават функционалността и математическата им приложимост при моделиране. Работното поле от фиг. 2 съдържа блокове от библиотеката Simscape/ SPS, изградени от електронни елементи необходими за моделиране на принципни схеми. Синхронната работа между подразделите Simulink и SPS предоставя възможност за конструиране на модели от сложни електрически устройства, базирани на комбиниран подход – имитационно (чрез електрически елементи, проводници и схеми) и функционално (чрез математическо описание) моделиране. Комбинацията им позволява едновременно симулиране на работните режими на устройствата и генериране на различни видове анализи – както времеви, така и честотни (включително амплитудно-честотни характеристики – АЧХ).

Комуникацията между моделите в SPS се осъществява чрез съвместимостта на входно-изходните параметри на елементите от различните библиотеки. При възникване на несъвместимост се използват блокове-конвертори, налични в библиотеката Simulink Library Browser. Кабелната връзка между електрически елементи и функционални блокове се изчертава като линия при спазване посоките на сигналите (вход/изход), както и поляритетът на източниците.



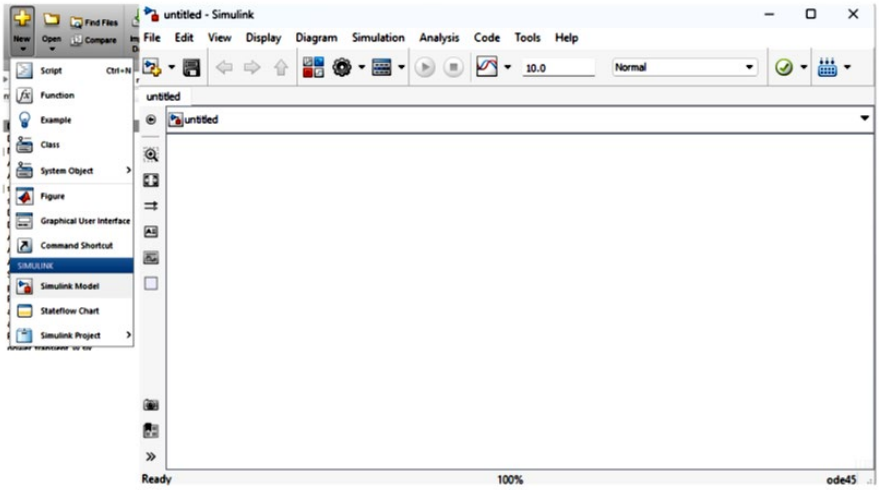
Фиг. 2. Библиотека на раздел SPS с блокове поставени на работно поле Powergui

Анализът на виртуалния модел включва вградения в SPS математически апарат за синтез на диференциални уравнения. Числено решаване на тези уравнения може да се извършва чрез различни алгоритми, като: ode15s, ode23s, ode23t и ode23tb. Симулинк моделът по подразбиране стартира с алгоритъма ode45. Изборът на подходящ алгоритъм се определя чрез сравнителен анализ на ефективността при изпълнение на симулацията, като се отчитат както скоростта на изчисление, така и качеството на получените времеви

диаграми. Правилният избор на числен метод е потвърден, когато симулацията протича без прекъсвания, нестабилности или забавяния при визуализацията на резултатите.

3 Етапи в интегралната методика за създаване на модел в Matlab/Simulink

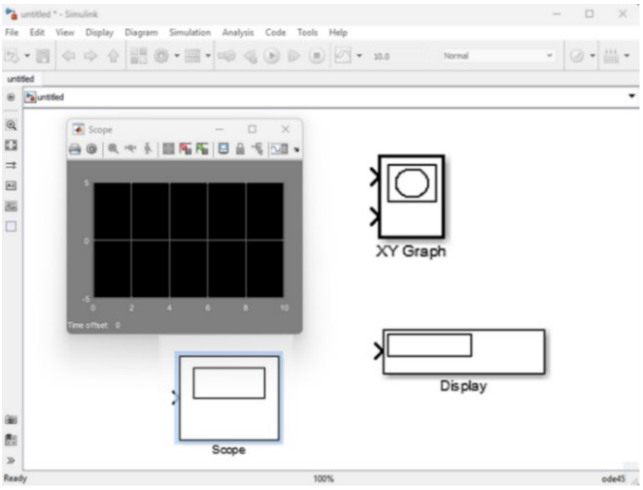
Началото на създаване на симулацията за нов модел започва с генериране на работно поле показано на фиг. 3, като върху него се избират и разполагат необходимите елементи от съответните библиотеки. Добавените елементи на работното поле се свързват от входен възел и изчертаване на линия до изходния възел. Електрическата връзка е осъществена при оцветяване в черен цвят. Линията в червен цвят означава грешка в свързването.



Фиг. 3. Работно поле за създаване на нов модел

– **Поставяне в работното поле на симулационни измервателни апарати за визуализация на резултатите**

Задължителен комплект от библиотеките на Simulink е избора на виртуални измервателни прибори от библиотеката Sinks от фиг. 4, като Scope, XY Graph и Display.



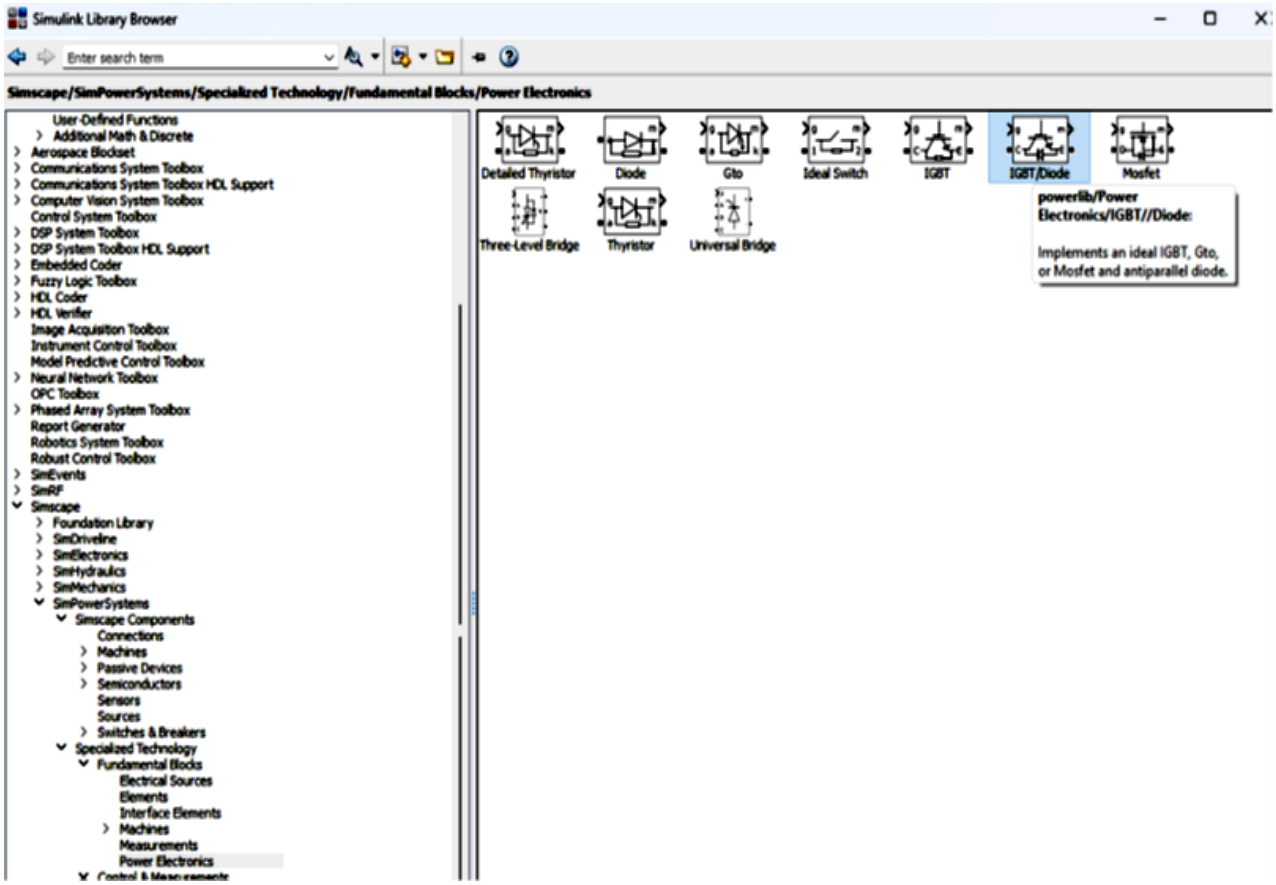
Фиг. 4. Пиктограми на измервателни прибори Scope с изображение на работен екран за осцилоскоп и XY Graph, Display цифров мултимер

Моделите от блокове Scope и плотер XY Graph визуализират графично резултатите от симулацията. Интерфейсът на Scope е координатна система, аналогична на реален осцилоскоп с абсциса (X) отчитаща времето на симулация и ординатата (Y) за формата и амплитудата на изследвания параметър. Моделът на блок Display е цифров мултиметър с възможност за конфигуриране на отчети от амплитудни, ефективни или комплексни стойности.

– **Избор на електрически силови елементи за изграждане на модел от принципни и блокови схеми**

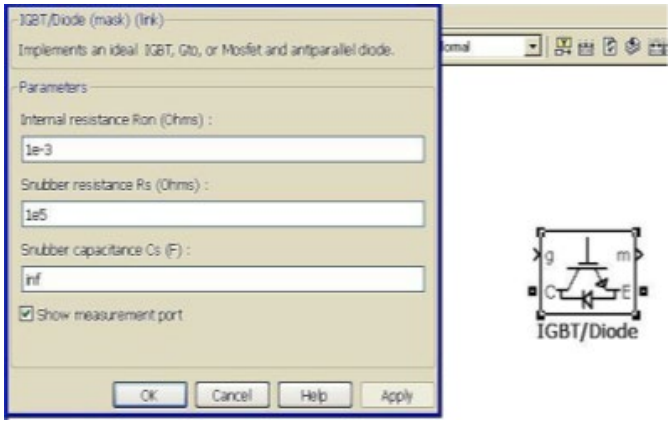
Началото на изграждане на модели в Simulink от дискретни елементи е библиотеката **Power Electronics** от дървовидната структура към раздел SPS, показана на фиг. 5.

Устройствата и компонентите са групирани в папки обозначени по начин за лесно и интуитивно откриване и поставяне на работното поле. Прилагат се два варианта на пренасяне в работното поле – чрез изтегляне с мишката от библиотеката или чрез копиране. Библиотека Elements от раздел SPS съдържа пиктограми от модели на силови полупроводникови прибори, необходими в архитектурата на принципните схеми. Изборът на конкретен силов елемент от библиотеката се определя по пиктограмата, след което той се разполага в работното поле.



Фиг. 5. Библиотека Elements от раздел SPS и графично изобразяване на електрически елементи и възли

Отвореният **диалогов прозорец** показан на фиг. 6 за избраният елемент транзистор IGBT визуализира основните му параметри.



Фиг. 6 Отворен диалогов прозорец със зададени по подразбиране параметри на транзистор IGBT и графично му изобразяване чрез пиктограма

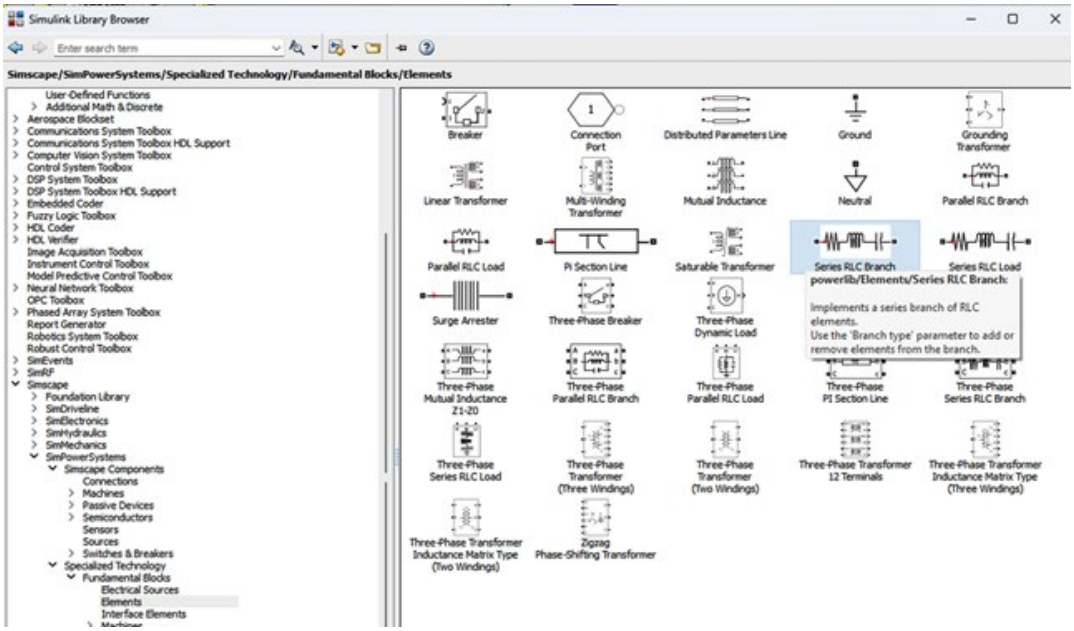
Основни параметри на избраният силов транзистор от диалоговия прозорец:

- **Ron** – вътрешно съпротивление в права посока;
- **Rs** – вътрешно съпротивление в обратна посока;
- **C** – капацитет на прехода.

Изграждането на модели от принципни схеми включва пасивни компоненти архивирани в библиотеката Elements, показана на фиг. 7.

Пиктограмата на симулационния елемент от фиг. 7 Series RLC Branch, моделира последователно свързани пасивни елементи: съпротивление (R), индуктивност (L) и капацитет (C).

Стойностите на елементите в конкретния случай се задават, като в диалоговия прозорец се записват: R = 1 Ω – активно съпротивление; L = $1 \cdot 10^{-3}$ H – индуктивност и C = $1 \cdot 10^{-6}$ F – капацитет.

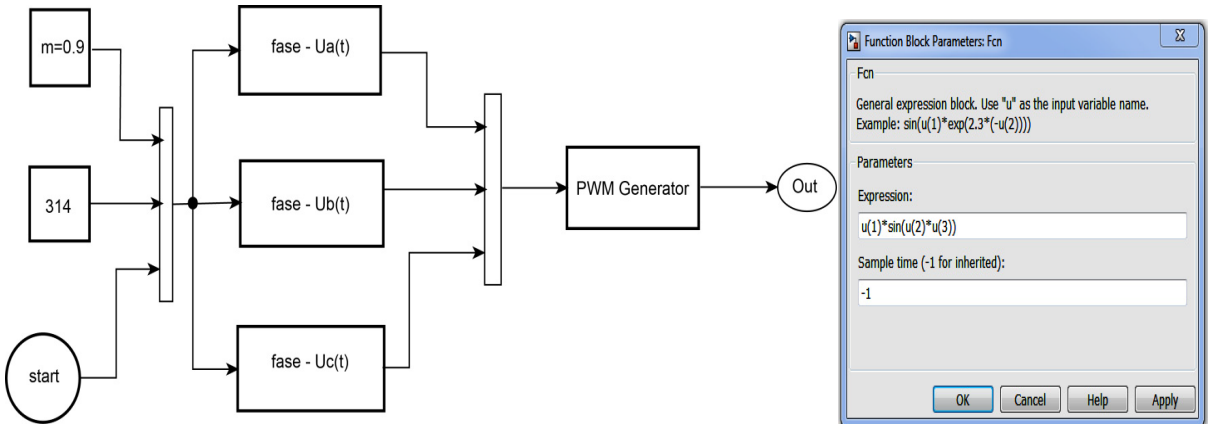


Фиг. 7. Библиотека Elements от раздел SPS и пиктограми на електрически елементи като R, L, C

4 Експериментална постановка – моделиране в Simulink на електронен преобразувател (инвертор на напрежение)

Управляващата функция на инвертора на напрежение е архитектура от функционални блокове на Simulink зададени с уравнения за имитиране на синусоидални функции, записани в диалоговия прозорец (фиг. 8).

Изходната функция симулира широчинно импулсна модулация от блок PWM Generator за управление на четири транзистора от силовата схема.



Фиг. 8. Архитектура на управление в Simulink свързан към блок PWM Generator

Системата уравнения е записана в блокове fase – U(t) за три фази (A, B и C):

$$U_A(t) = U_{Am}\sin(\omega.t + \psi_U),\ V\ i_A(t) = i_{Am}\sin(\omega.t + \psi_I),A \quad (1)$$

$$U_B(t) = U_{Bm}\sin(\omega.t - \frac{2.\pi}{3}),\ V\ i_B(t) = i_{Bm}\sin(\omega.t - \frac{2.\pi}{3}) \quad (2)$$

$$U_C(t) = U_{Cm}\sin(\omega.t + \frac{2.\pi}{3}),\ V\ i_C(t) = i_{Cm}\sin(\omega.t + \frac{2.\pi}{3}) \quad (3)$$

където:

$\omega = 314, s^{-1}$ е кръговата честота, при зададена линейна

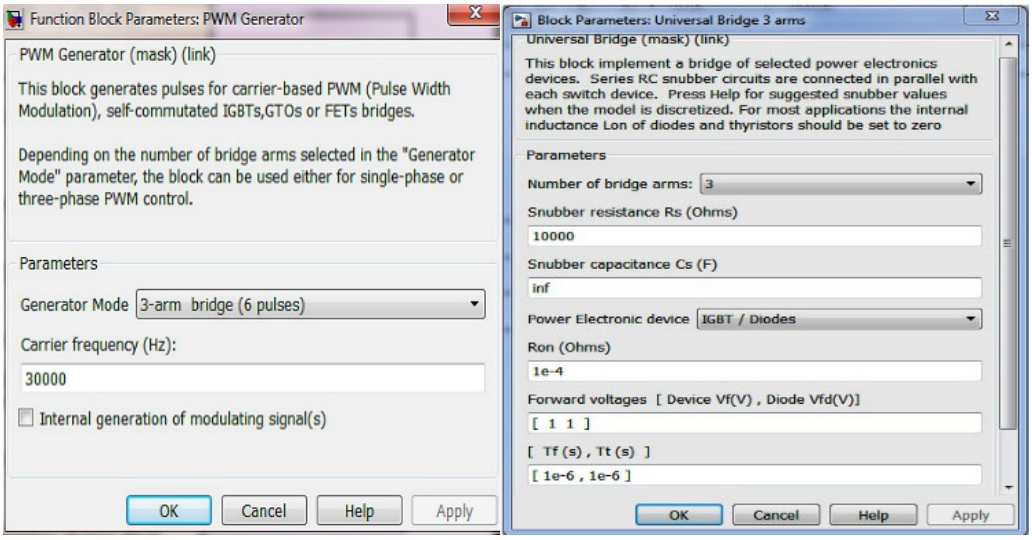
$$f = 50, Hz \quad (4)$$

Дефазирането между началните фаза на тока ψ_I и напрежението ψ_U се определя от фазова им разлика:

$$\varphi = \psi_U - \psi_I \quad (5)$$

Идеята на симулацията е графичното моделиране на (1), (2) и (3), като синусоиди дефазирани на 120^0 **имитиращи трифазната електрическа мрежа**.

Диалоговите прозорци с падащо меню за избор от конфигурации на брой и вид **мощни транзистори** се оразмеряват за работа към силовата част на инвертора (фиг. 9). Зададената стойност на носещата честота 30kHz е при референтна мрежова 50Hz и индексът на модулация между амплитудите на двете честоти m = 0,8.

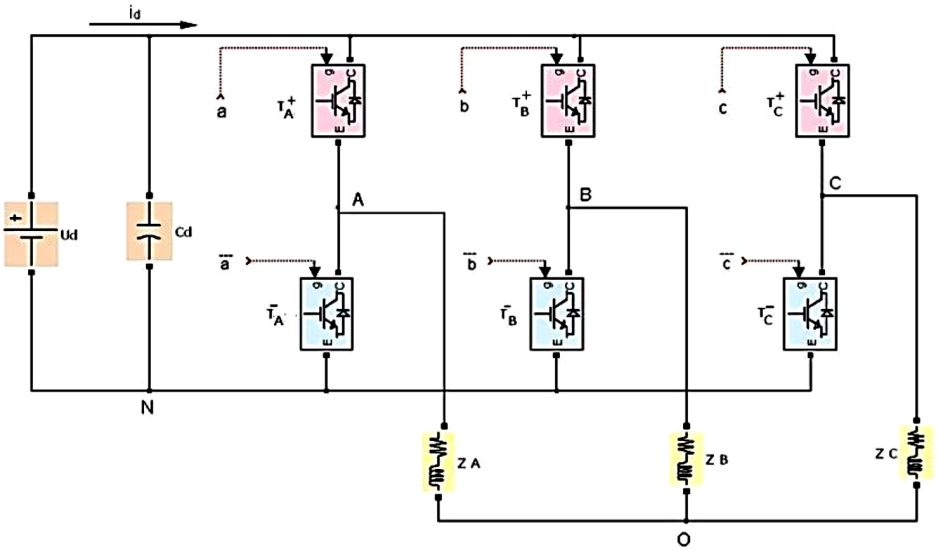


Фиг. 9. Диалоговият прозорец вляво показва настройки на „PWM Generator“ за носеща честота и брой транзистори, а вдясно показва параметрите на силовия мост

Диалоговият прозорец от блок Universal Bridge 3 arms е зададен като три двойки силови транзистора, управлявани чрез ШИМ (PWM) функция.

Силовата част от модела на трифазен електронен преобразувател е построена от блокове на библиотеките Elements и Power Electronics (фиг. 10), като е проектирана да работи с мощни полупроводникови елементи (IGBT, power MOSFET, GTO - hyristors). Управлението на комутацията им се осъществява по закона на широчинно импулсната модулация ШИМ (PWM) функция, определяща променлив коефициент на запълване в зависимост от натоварването в изходната верига. Менютата на диалоговите прозорци за елементите се настройват за конкретния случай с номинална изходна мощност 2000W.

Реален източник на напрежение (C_d, U_d) симулиращ постояннотоков генератор на напрежение (фотоволтаични модули, акумулаторна батерия или постояннотоков генератор) е включен в силовата част на принципната схема (фиг. 10).

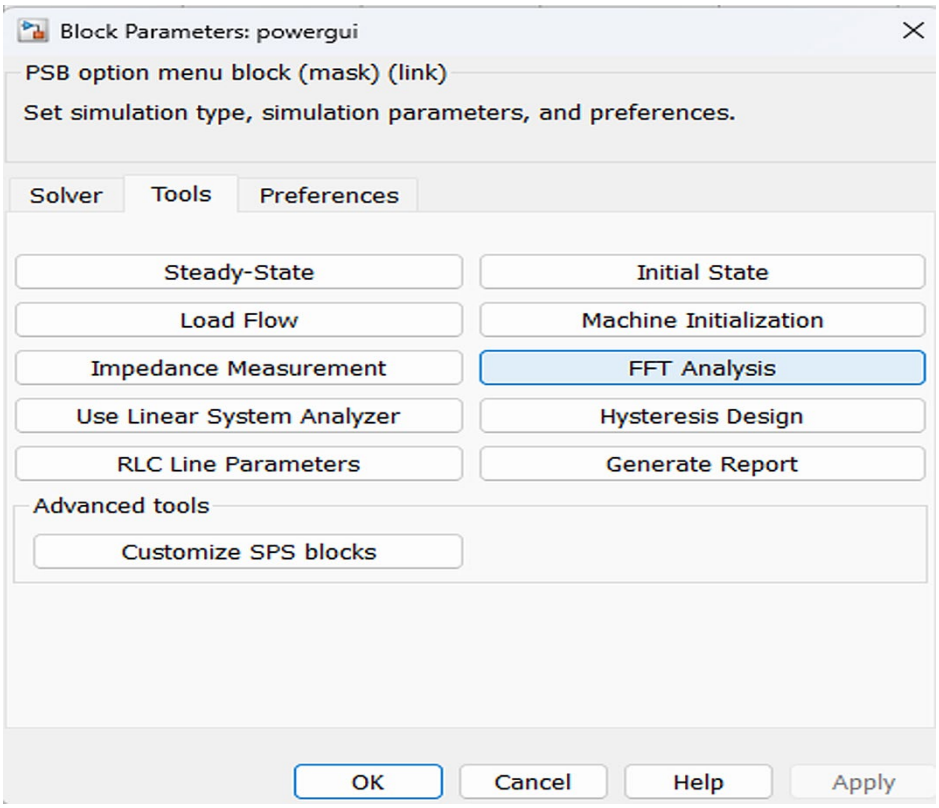


Фиг. 10. Модел на силова част от трифазен инвертор на напрежение

Съвместната работа между силовата част и управляващия ШИМ модел формира завършена структура на електронен преобразувател - инвертор, използван във фотоволтаичните системи.

Анализът на виртуалния модел на електронен преобразувател, разработен в Simulink за публикацията изисква използване на специализирания блок графичен интерфейс (GUI – Powergui).

Блокът Powergui, разположен върху работното поле, съдържа интерфейс с радиобутони за избор на различни режими на анализ (фиг. 11).



Фиг. 11. Диалогов прозорец на функционален блок Powergui с радиобутони за избор на вид анализ

Изборът на блок анализатора powergui отваря диалогов прозорец, на който с радиобутон от фиг. 11 се стартира FFT Analysis за графично визуализиране формата на изходния ток и напрежение и изчисляване процентно коефициента на хармонични изкривавания THD_U и THD_I за всеки хармоник, кратен на основния (h1=50Hz).

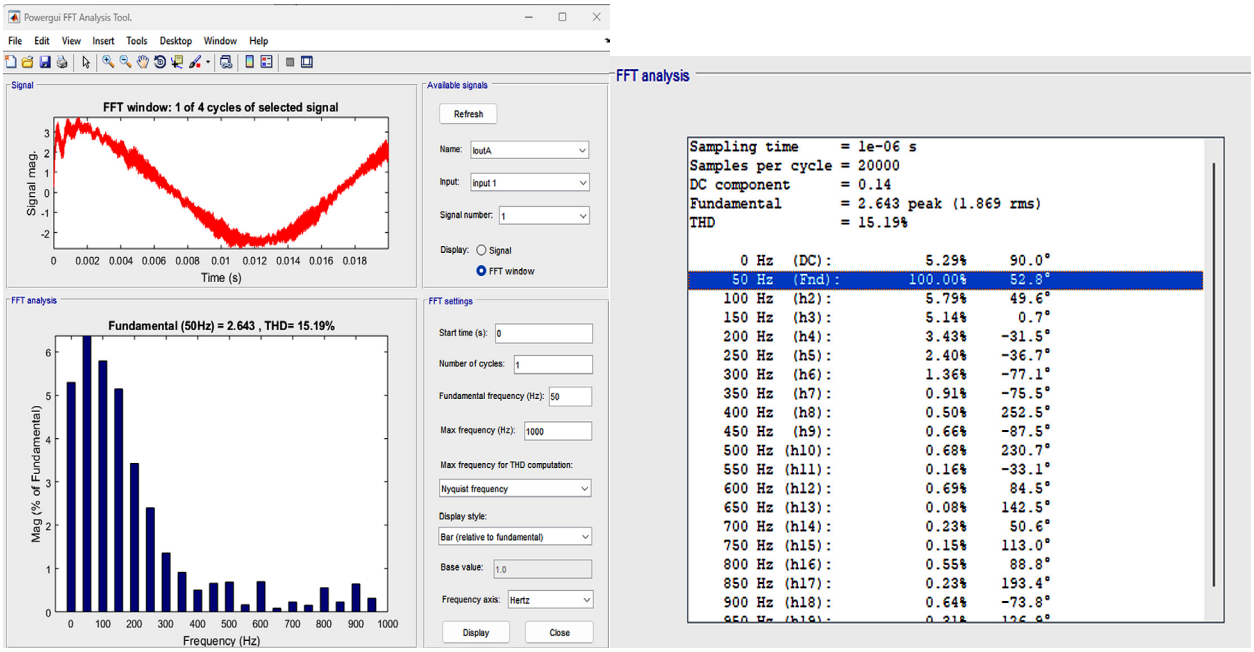
Качеството на изходното напрежение, определено от приближаването на неговата форма до синусоидалната, се характеризира с коефициента на хармонични съставящи THD, както за напрежението така и за тока [7]:

$$\mathrm{THD_U} = \frac{\sqrt{\sum_{h2}^{hn} U_n^{\,2}}}{U_{h1}} .100,\% \quad \mathrm{THD_I} = \frac{\sqrt{\sum_{h2}^{hn} I_n^{\,2}}}{I_{h1}} .100,\% \qquad (6)$$

където U_n е ефективната стойност на напрежението с номер на най-високия хармоник h_n, U_{h1} – ефективната стойност на напрежението на първия хармоник;

h_2 – номерът на хармоника, най-близко до основния;

Математическата основа на честотния анализ реализирано в Simulink е бързото преобразуване на Фурие (FFT). Анализът и мониторингът на честотните характеристики на RLC вериги са разгледани в [1]. Синтезираният честотен анализ е формата на вълната и отчетите от хармоници на хистограмата. Резултатите от работата на електронният преобразувател са визуализирани в графична и таблична форма на фиг. 12.



Фиг. 12. Диаграма, хистограма и таблични данни за ефективните стойности на хармониците от спектъра на АЧХ

5 Изводи

Интегрираната методика предоставя възможност за моделиране на електронни преобразуватели в Simulink и детайлен анализ на резултатите от симулацията им чрез графично и таблично представяне.

Приложният принос от визуализирането на отчетите за форма на вълната на тока, напрежението и амплитудно - честотните им характеристики (АЧХ) се използва като основа за експериментални изследвания качеството на работа върху реално изградени еднофазни и трифазни електронни преобразуватели, присъединени към електроенергийната мрежа. Моделирането на процесите в Simulink за електронният преобразувател синтезира диаграми, които са близки до реалните, позволяващо по-надеждна оценка на работните режими и характеристиките на инверторите.

ЛИТЕРАТУРА:

[1] Лалев Х., Желев С., Цанков Ц. Анализ и мониторинг на честотните характеристики на RLC вериги. Научна сесия на факултет „Артилерия, ПВО и КИС“, Шумен, 2009, ISSN 1314-1953.

[2] Mandadzhiev G. A., Belovski I., Ivanov K. Combined Simulink Model of Commercially Available Off-the-Shelf Thermoelectric Energy Harvesters. Vol. 27, No. 1, 2026, ISSN 1311-5065, pp. 50–58.

[3] Mandadzhiev A., Belovski I., Ivanov K. Simulink Model Validation of Thermoelectric Module in Power Generation Mode. In: 2025 10th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), Stara Zagora, Bulgaria, 2025, DOI: 10.1109/EEAE65901.2025.11273673, pp. 1–5.

[4] Rajpriya G., Ravi S., Zaidi A. M. A. Design and development of MATLAB Simulink based Selective Harmonic Elimination technique for three phase voltage source inverter. In: Proceedings of the 2013 International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2014, DOI: 10.1109/ICACCS.2013.6938734.

[5] Guerrero Ramírez E. O., Martínez Barbosa A., Contreras Ordaz M. A., Cruz Martínez G. Estudio de la distorsión armónica total en MATLAB/Simulink del inversor trifásico PWM. Pistas Educativas.

[6] Modeling and analysis of current harmonic distortion from grid connected PV inverters under different operating conditions. Solar Energy, Elsevier.

[7] IEC 61000-4-7:2002+A1:2008. Electromagnetic Compatibility (EMC) – Part 4-7: Testing and Measurement Techniques – General Guide on Harmonics and Interharmonics Measurements and Instrumentation for Power Supply Systems and Equipment Connected Thereto. IEC.

[8] Petrov, Y. Modeling Of Transients Processies In Linear Electric Circuit Of The Second Order With Generalised Net. Annual of Assen Zlatarov University – Burgas, Bulgaria, Vol. XLVI, No. 1, 2019.

[9] Мечкова, В., Станева, Л., Мечков, Б. Приложение на MATLAB при изследване на преходни процеси в линейни електрически вериги. Годишник на Университет „Проф. д-р Асен Златаров“, Бургас, т. XXXVIII, № 1, 2009, с. 126–129.

[10] Мечкова, В., Станева, Л., Мечкова, Б. Математически модел за изследване на преходни процеси в линейна електрическа верига от втори ред. Международна научна конференция „Образование, наука, икономика и технологии“, т. 2, Бургас, 2015.

RESEARCH ON A MODEL OF A WIND POWER PLANT WITH A STATIC SYNCHRONOUS COMPENSATOR (STATCOM) FROM THE SIMULINK LIBRARY "SIMULINK"*

VASIL B. IVANOV

ABSTRACT: *The main objective of this study is to analyze the structure of a wind power plant model, the interconnections between its individual subsystems, and the behavior of the electrical system under specified operating conditions. A STATCOM compensator is integrated into the model to provide dynamic reactive power compensation and voltage regulation at the point of connection to the electrical grid.*

KEYWORDS: *Matlab/Simulink, SimPowerSystems (SPS) libraries, STATCOM compensator. wind power plant model*

DOI: https://doi.org/10.46687/MT26VBV

ИЗСЛЕДВАНЕ НА МОДЕЛ НА ВЯТЪРНА ЕЛЕКТРОЦЕНТРАЛА СЪС СТАТИЧЕН СИНХРОНЕН КОМПЕНСАТОР STATCOM ОТ БИБЛИОТЕКАТА НА „SIMULINK"

ВАСИЛ Б. ИВАНОВ

АБСТРАКТ: *Основната цел на това изследване е да се анализира структурата на модел на вятърна електроцентрала, взаимовръзките между отделните ѝ подсистеми и поведението на електрическата система при определени експлоатационни условия. В модела е интегриран компенсатор STATCOM, който осигурява динамична компенсация на реактивната мощност и регулиране на напрежението в точката на свързване към електрическата мрежа.*

1 Въведение

Вятърната енергия е основен възобновяем енергиен ресурс и намира все по-широко приложение при производството на електрическа енергия. Енергийният потенциал на вятъра зависи основно от скоростта и плътността на въздушния поток, както и от конструктивните характеристики на вятърната турбина. Поради променливия характер на скоростта и посоката на вятъра, работата на вятърните електроцентрали притежава динамични изменения на електрическите и механичните параметри [1], [2].

Съвременните вятърни електроцентрали използват различни електромеханични генератори, сред които асинхронни, двойно захранвани асинхронни и синхронни генератори. Изборът на генератор присъединен към електрическата мрежа оказва влияние върху реактивната мощност, напрежението и динамичните характеристики на вятърната електроцентрала [1], [2].

Математическото и компютърното моделиране предоставят възможност за изследване поведението на вятърни енергийни системи при различни работни условия без необходимост от провеждане на всички експерименти върху реално оборудване. Измерването на мощностните характеристики на вятърни турбини е предмет на стандарта

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН"

IEC 61400-12-1 [3]. Моделирането на преходни процеси в електрически вериги чрез обобщени мрежи и MATLAB е разгледано в [6, 7].

Програмният продукт Simulink и Simscape Electrical предоставят математически инструментариум, за моделиране на вятърни турбини, електрически генератори, трансформатори, силови преобразуватели и електроенергийни мрежи [4, 5].

Присъединяването на вятърни електроцентрали към електроенергийната мрежа изисква управление на реактивната мощност (Q) и поддържане на напрежението за устойчивата работа на цялата система. Моделирането на статичен компенсатор от вида STATCOM представлява ефективно средство за бърза динамична компенсация на реактивната мощност и регулиране на напрежението в точката на присъединяване.

В статията се изследва модел на вятърна електроцентрала от библиотеката Simulink с интегриран компенсатор STATCOM. Анализират се структурата и взаимовръзките между отделните подсистеми, както и влиянието на STATCOM върху реактивната мощност, напрежението и електрическите параметри на системата при зададени режими на работа.

2 Теоретична постановка

● **Параметри на входните физични величини задвижващи вятърна централа.**

Ефективната работа на вятърните турбини зависи от следните основни параметри: скорост на вятъра **Vв** (начална, крайна, средна, референтна); посока на вятъра; позиция на турбината (хоризонтална или вертикална ос).

• **Кинетичната енергия на въздуха Ек** зависи от неговата плътност **ρ (kg/m³)**, която при **стандартни условия** и температура **15°C** е приблизително **1.225 kg/m³.** Колкото по-висока е плътността на въздуха, толкова по-голяма е генерираната енергия при една и съща скорост на вятъра.

• **Енергиен потенциал на вятъра определен чрез** кинетичната енергия на задвижвания въздух:

$$E_в = \frac{1}{2}.\,m.\,V_в{}^2, (W.s) \tag{1}$$

където: Vв (m/s) – скорост на вятъра, m (kg) – маса на въздуха.

Въздушната маса може да се синтезира чрез зависимостта:

$$m = \rho.\,Q, (kg) \tag{2}$$

Обемният въздушен дебит Q се определя чрез:

$$Q = S\cdot.\,L \tag{3}$$

S [m²] - площ описана от движението на витлото на вятърната турбина,
ρ [kg/m³] - плътност на въздуха,
L [m] – дължина на въздушния път създаден от витлото на вятърната турбина.

• **Механичната мощност на вятъра**, задвижваща вятърната турбина се изразява чрез кинетичната енергия **по времето** на активно въздействие на вятъра върху витлото:

$$P_в = \frac{1}{2}.\frac{E_к}{t}, (W) \tag{4}$$

• **Механичната мощност на движеща се въздушна маса m през заградената площ S** на вятърната турбина се получава:

$$\mathrm{P_{мех}} = \frac{1}{2}.\mathrm{C_p}\ \rho.\mathrm{S}.\frac{\mathrm{L}}{\mathrm{t}}.\mathrm{V_в}^2 = \frac{1}{2}.\rho.\mathrm{S}.\mathrm{V_в}^3(\mathrm{W}) \quad (5)$$

• Въвежда се **коефициент на мощност** $\mathrm{C_p}$ отчитащ ефективността от преобразуване на вятъра в мощност задвижваща вятърната турбина.

Неговият теоретичен максимум е 0.59, а реално е около 0.45 – 0.48.

$$\mathrm{P_{макс}}^{\mathrm{т}} = \frac{0{,}59}{2}.\rho.\mathrm{S}.\mathrm{V_в}^3(\mathrm{W}) \quad (6)$$

Коефициентът на мощност $\mathrm{C_p}$ **зависи от входната скорост** $V_{\mathrm{вх}}$ на вятъра в турбината в съотношение с излизащата скорост $V_{\mathrm{изх}}$.

• Параметъра определящ кратността на съотношенията е **коефициента на бързоходност Кб**:

$$\mathrm{К_{бърз}} = \frac{\mathrm{V_{изх}}}{\mathrm{V_{вх}}} \quad (7)$$

където:

$V_{\mathrm{изх}} = \omega \cdot \mathrm{R}, \left(\frac{\mathrm{m}}{\mathrm{s}}\right)$ е ъгловата скорост на периферния ръб на перките към радиуса им.

$V_{\mathrm{изх}} = \mathrm{Vв}, \left(\frac{\mathrm{m}}{\mathrm{s}}\right)$ е скоростта на вятъра влизащ в турбината.

Проектирането на вятърни турбини изисква задаване на **максимална стойност на мощността:**

$$\mathrm{P_{макс}}^{\mathrm{ном}} = \frac{1}{4}.\rho.\mathrm{S}.\mathrm{V_в}^3(\mathrm{W}) \quad (8)$$

Съществен параметър е **плътността на енергийния поток**, който зависи от географското местоположение, релефа на терена, инфраструктурата, атмосферните условия. Плътността на енергийния поток се измерва в W/m² и определя мощността на вятъра, преминаваща през единица площ $\mathrm{S} = 1\mathrm{m}^2$.

Повърхностната плътност на мощността (средна специфична мощност) се определя за площ $S = 1m^2$ и се задава чрез:

$$\mathrm{P_{ср.спец.}}^{\mathrm{макс}} = \frac{1}{4}.\rho.\mathrm{V_в}^3, \left(\frac{\mathrm{W}}{\mathrm{m}^2}\right) \quad (9)$$

● **Пълната (привидна) електрическа мощност** получена от електромеханичен асинхронен генератор на вятърна турбина е променливотокова:

$$\mathbf{S^2} = \mathrm{R}^2 + \mathrm{Q}^2 + \mathrm{D}^2, \mathrm{VA}$$

Пълната електрическа мощност се състои от компонентите:

- **Активна полезна** мощност:

$$\mathbf{P} = \mathrm{R}.\mathrm{I}^2.\cos\varphi\,, \mathrm{W} \quad (10)$$

- **Индуктивна** реактивна мощност:

$$\mathbf{Q_L} = X_L . I^2 . \sin\varphi \, , var \tag{11}$$

- **Капацитивна** реактивна мощност:

$$\mathbf{Q_C} = X_C . I^2 . \sin\varphi \, , var \tag{12}$$

където, D е деформационната мощност от нелинейните елементи.

Извод: Ефективността на вятърните централи зависи от множество фактори, като най-съществен е скоростта на вятъра. Чрез математично моделиране и симулация в среда като Simulink може да се извърши точен анализ и оптимизация на параметрите още преди реалната експлоатация на вятърната централа.

3 Методика на моделиране на вятърна централа от библиотеката на програмния продукт Simulink. Етапи на моделиране.

● **Създаване на модел** с начален етап, включващ чертеж в работното поле на блокови схеми и принципни електрически схеми. Стартиране процеса на моделиране е задаване на началните условия и параметрите на конкретната електромеханична вятърна централа.

● **Симулацията се стартира и експериментира** със следните показатели:

• **дефиниране на входни и изходни величини** и измерване на електромеханичните параметри като ток, напрежение, въртящ момент, скорост на вятъра и обороти на машината.

• **анализ на резултатите** от симулацията в реално време се представя чрез **обработка и визуализация на** графики, диаграми, хистограми и таблични отчети.

● **Simulink** използва библиотеката на **SimPowerSystems**, включваща модели на реални електротехнически устройства. Основни характеристики на архитектурата са блокове с диалогови прозорци, задаване на параметри чрез падащи менюта с възможност за избор между идеални модели и реални модели. Моделирането включва елементи като резистори, кондензатори, бобини, транзистори, мотори, трансформатори и др.. Комбинацията от елементи позволява създаване и симулиране на реални физични процеси.

● **Моделът на вятърната електроцентрала е създаден в библиотеката на Simulink** чрез построена принципна схема и зададени мощностни характеристики, въртящ момент и електрически параметри на **електромеханичния модул асинхронен генератор** и консуматори.

● **Параметрите на модела** са конфигурирани по начин за експериментиране чрез задаване на различни симулационни режими **с включен и изключен STATCOM** и авариен режим на късо съединение.

● **Динамичните параметри на променливите величини като** скорост на вятъра, ъгъл на регулиране и обороти **се управляват автоматично чрез обратни връзки** в блоковата схема на системата.

Приложимост на изследваният по виртуалния модел

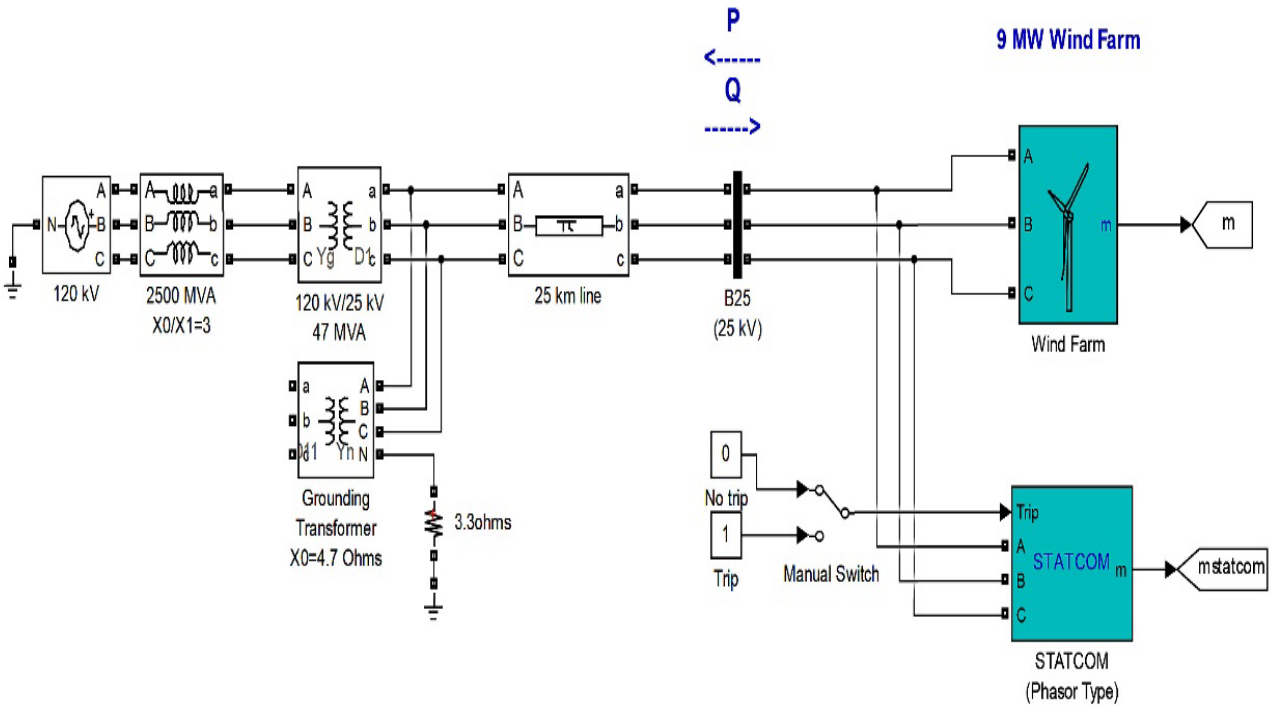
Моделирането на вятърна електроцентрала присъединена към електроенергийната система се реализира в програмна среда на Simulink. Основните предимства са възможност за предварително тестване на системи, оптимизация преди реална реализация и намаляване на риска при внедряване. Резултатите от симулациите при зададени параметри могат успешно да се използват при проектиране на реални вятърни електроцентрали., анализ на работни режими и оптимизация на енергийни процеси.

4 Експериментален модел на вятърна електроцентрала, свързана към електроенергийната система от виртуалната библиотека

● **Моделиране вятърна централа от три двойки вятърни турбини**

Библиотечният модел на вятърна електроцентрала е съставен от **шест броя вятърни турбини**, задвижващи **асинхронни** електрически генератори **Induction Generator (IG)**.

Принципната схема на библиотечния модел (фиг. 1) представя енергийната структура на вятърна централа, свързана към електрическата система, чрез разпределителната мрежа средно напрежение 25kV и повишаващ трансформатор към преносната мрежа високо напрежение 120 kV.



Фиг. 1. Енергийна структура на библиотечния модел от вятърна електроцентрала, свързана към електрическа мрежа

● **Структура на подсистемата Wind Farm от фиг. 1**

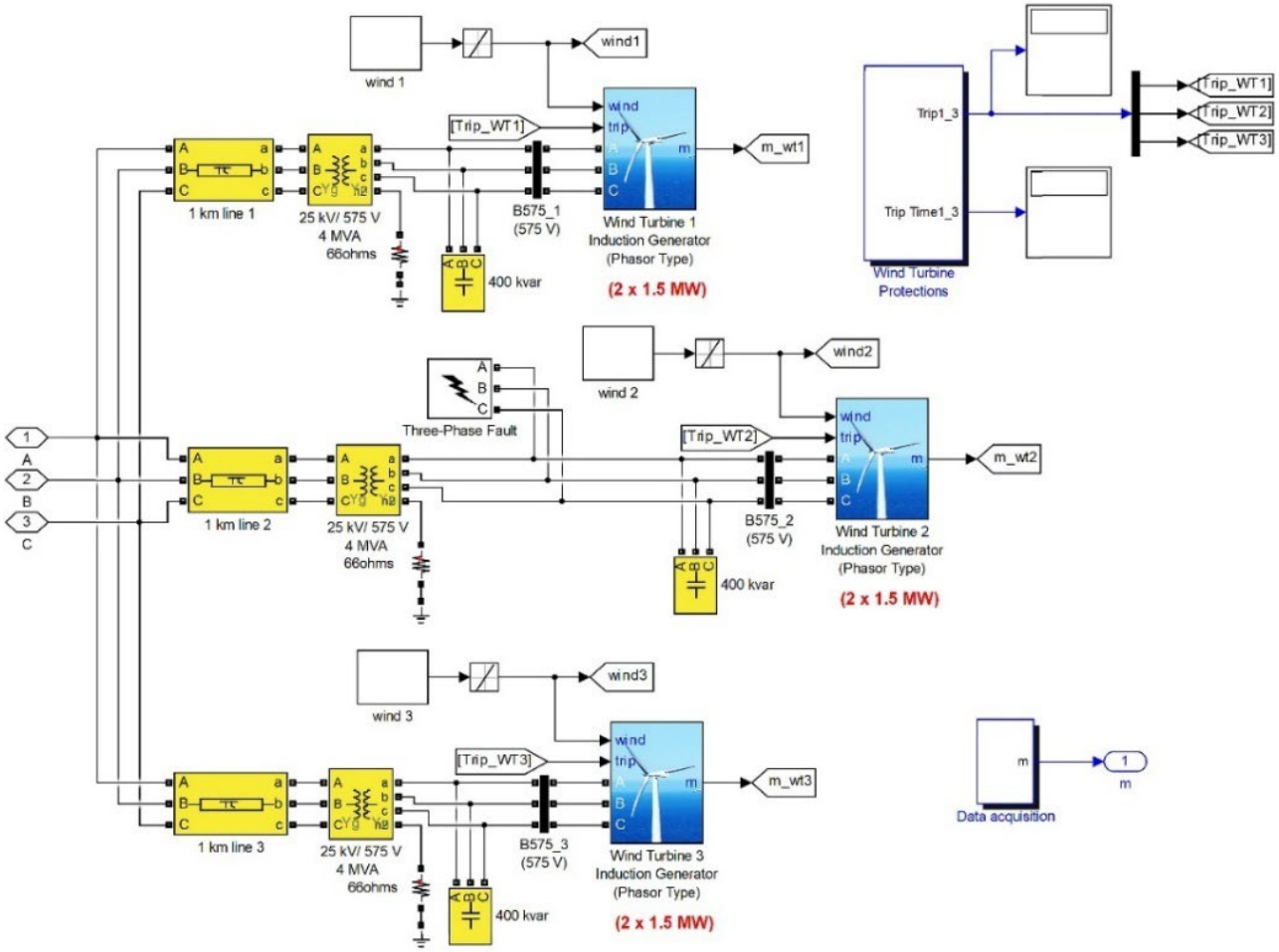
Подсистемата **Wind Farm** от библиотеката (фиг. 2) представлява интегриран модел на вятърна централа с обединен паралелен трифазен изход (изводи A, B, C). Произведената електрическа енергия се предава чрез кабелна линия с дължина 25km към повишаващ трифазен силов трансформатор, моделиран с номинални параметри 25кV/120 kV/47 MVA

● **Библиотечен модел на вятърните турбини и генератори**

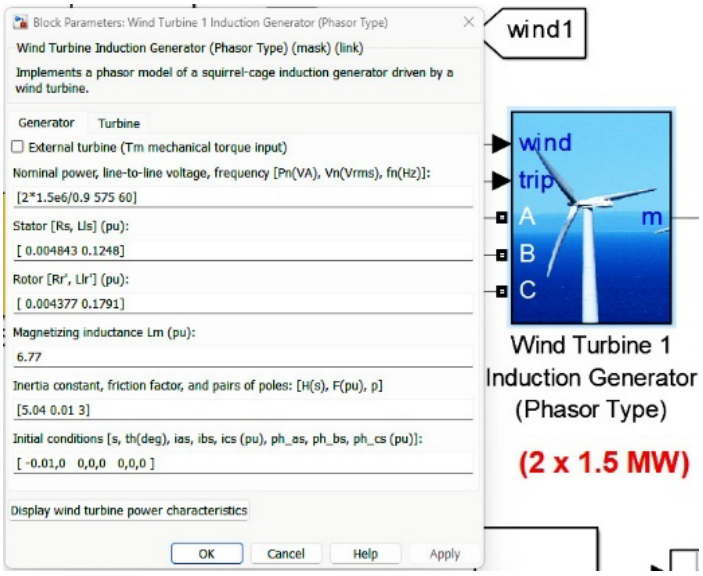
Подсистемата **Wind Farm** (фиг. 3) е реализирана чрез шест вятърни турбини, групирани в три паралелни двойки.

Всяка турбина работи при скорост на вятъра V=8m/s със зададена номинална активна мощност $P_{ном}$=1,5MW и задвижва трифазен асинхронен генератор (Induction Generator). Общата инсталирана мощност на симулационната вятърна електроцентрала е

$P_{общ}$ = 6.1,5 = 9MW



Фиг. 2. Библиотечен модел Simulink на подсистема „Wind Farm“



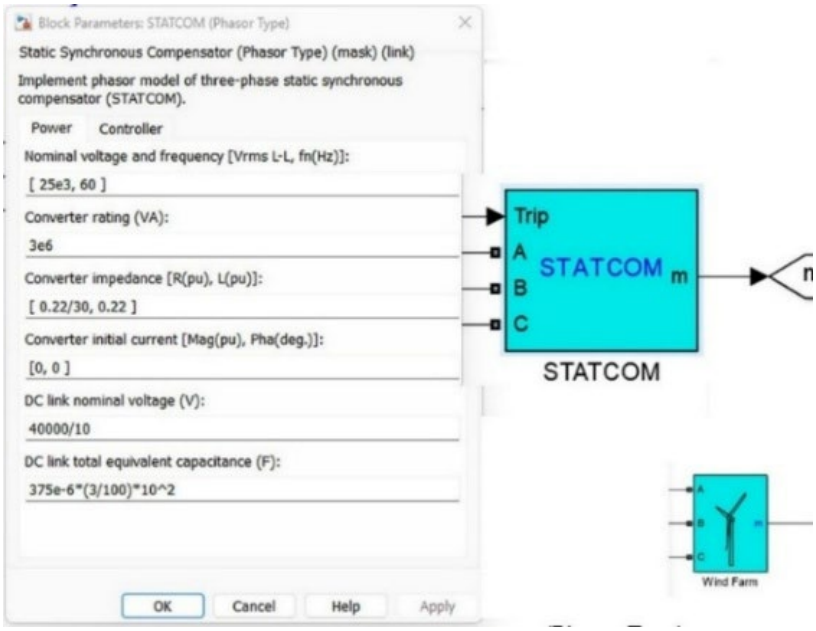
Фиг. 3. Диалогов прозорец с възможност за промяна на зададените електрически параметри и характеристики на една двойка вятърни турбини;

Принцип на преобразуване на енергията

Библиотечният модел в Simulink реализира преобразуването на механичната мощност $P_{мех}$ в електрическа мощност $P_{ел}$ чрез принципа на електромагнитната индукция. Механичната мощност, получена от въртенето на вятърните турбини, създава електромагнитен момент в асинхронния генератор, при което в статорните намотки се индуцира електродвижещо напрежение. Електрическата мощност обменяна между генератор и консуматорите е **активна** (P) и **реактивна** (Q) и се променя динамично от включеният **статичен синхронен компенсатор STATCOM**. **Пълната** мощност на вятърната централа **(S)** зависи от скоростта на вятъра, оборотите на ротора, електромагнитния момент и параметрите на електрическата мрежа.

• Работен режим на асинхронните генераторите от вятърните турбини

Библиотечният модел използва асинхронни генератори, които подават **активна мощност** към електрическата мрежа при работа **със скорост на въртене, малко по-висока от синхронната скорост.** При номинален режим моделът е настроен за стабилна работа при n ≈ 1pu (относителни единици), което съответства на 100% от номиналната скорост.
В режим на празен ход скоростта достига приблизително n=1.005pu (относителни единици)



Фиг. 4. Диалогов прозорец със зададени параметри на трифазен статичен синхронен компенсатор STATCOM моделиращ динамично реактивна мощност;

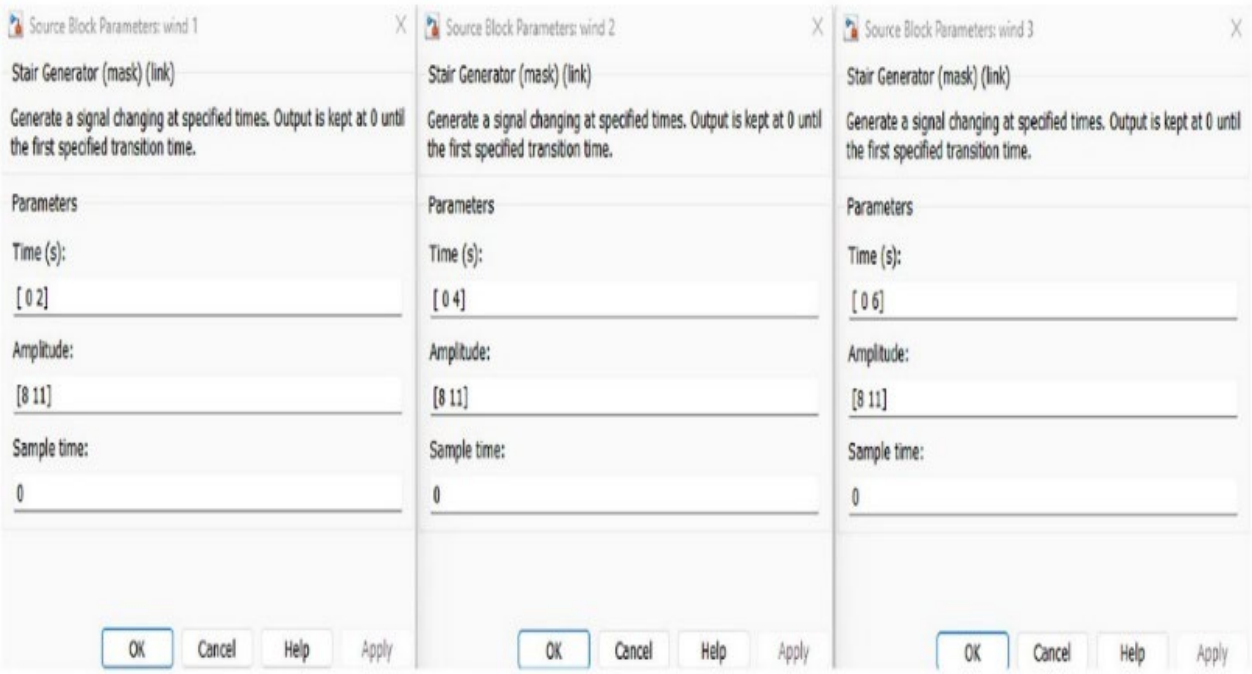
● Експериментално задаване на входните въздействия и изследване на работните режими на вятърната централа в Simulink

• Настройване характеристиките на вятърната турбина

Зависимостта на механичната мощност от скоростта на вятъра се анализира в диапазон V=4 \div 10m/s. Номиналният режим на работа се достига при скорост на вятъра $V_н$=9m/s, при което изходната мощност достига $P_н$=1pu =3MW

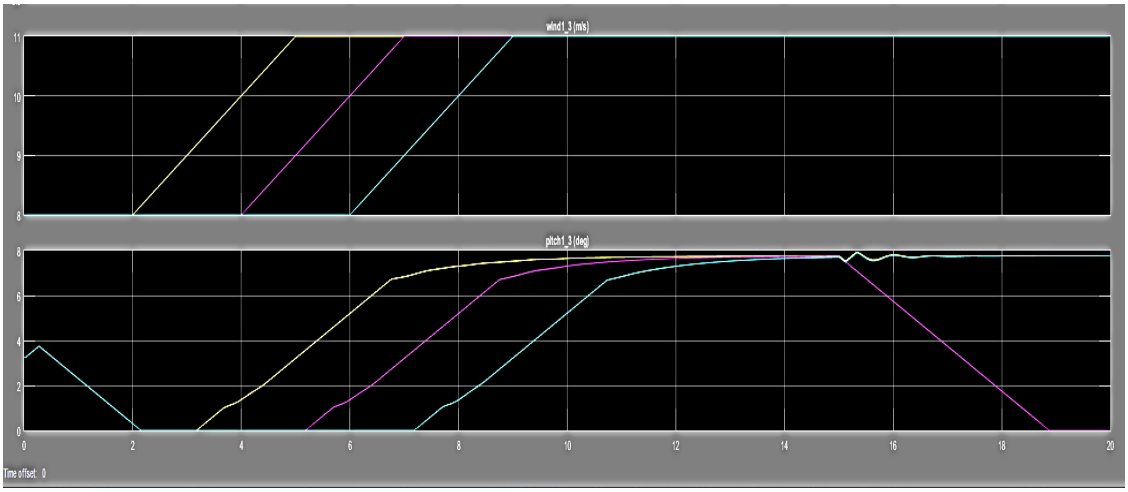
• Моделиране на изменението на скоростта на вятъра

За изследване на динамичните процеси са зададени различни времеви интервали на скоростта на вятъра за трите двойки турбини.



Фиг. 5. Диалогов прозорец за задаване скоростите на вятъра към отделните турбини.

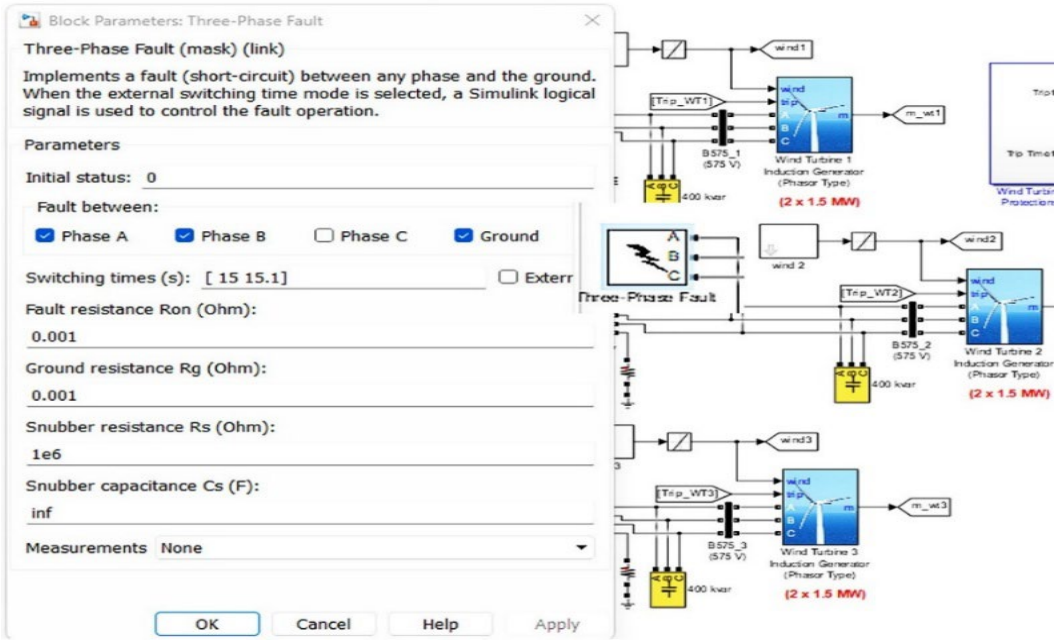
Изменението на скоростта се реализира чрез блокове Wind 1, Wind 2 и Wind 3. Началната скорост за първата двойка турбини е V=8m/s. След време t=2s скоростта се увеличава до V=11m/s. Аналогично изменение се задава за втората двойка турбини при (t=4s) и третата двойка турбини при (t=6s). Резултатите от изменението на входния ветрови поток са представени на фиг. 6.



Фиг. 6. Времедиаграма на зададената скорост на вятъра към трите групи турбини.

- **Изследване на авариен режим при късо съединение**

За проверка устойчивостта на системата е моделиран авариен режим чрез симулация на между фазово късо съединение. Изследването е проведено за турбина 2 при изходните нисковолтови клеми B25=575V, чрез блок **Three-Phase Fault** (фиг. 7).

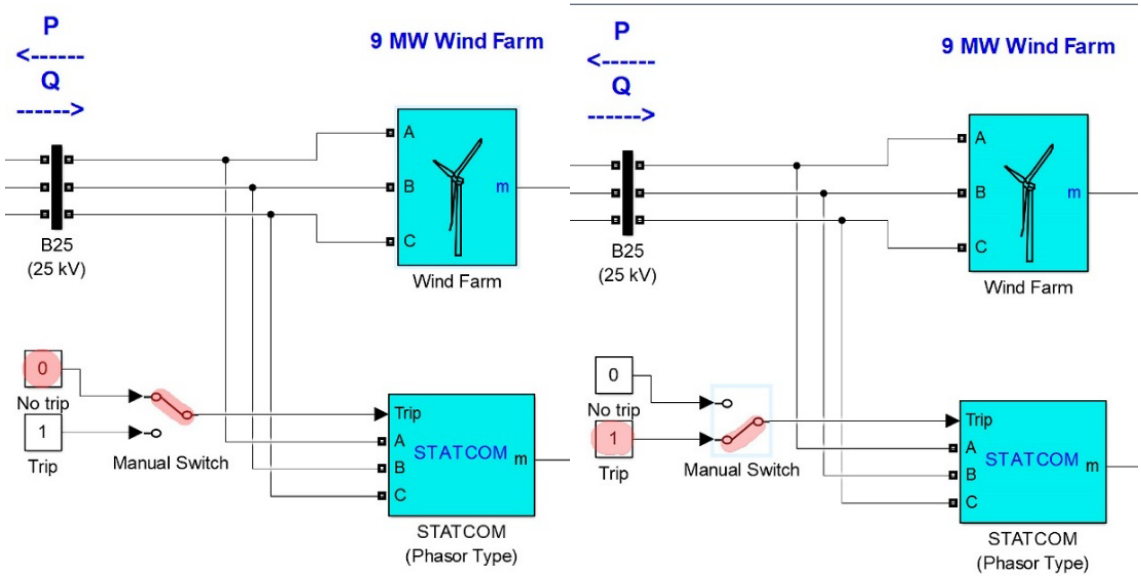


Фиг. 7. Диалогов прозорец за настройване параметрите при зададен авариен режим.

Аварийното късо съединение между фази A и B към земя от фиг. 7 е зададено за интервал t=15s до 15.11s. Наблюдава се краткотрайно претоварване на генератора, **промяна на активната и реактивната мощност и реакция на системата за компенсация** чрез STATCOM, което е представено графично на фиг. 14 и фиг. 15

• Симулационни режими в Simulink с включен и изключен статичен синхронен компенсатор STATCOM

Режим 1 – вятърна централа със STATCOM. В този режим STATCOM е включен паралелно към електрическата мрежа. Управлението се реализира чрез блок **Manual Switch** (фиг. 8). Логическото състояние в [0] STATCOM **участва динамично в регулиране на реактивната мощност.**



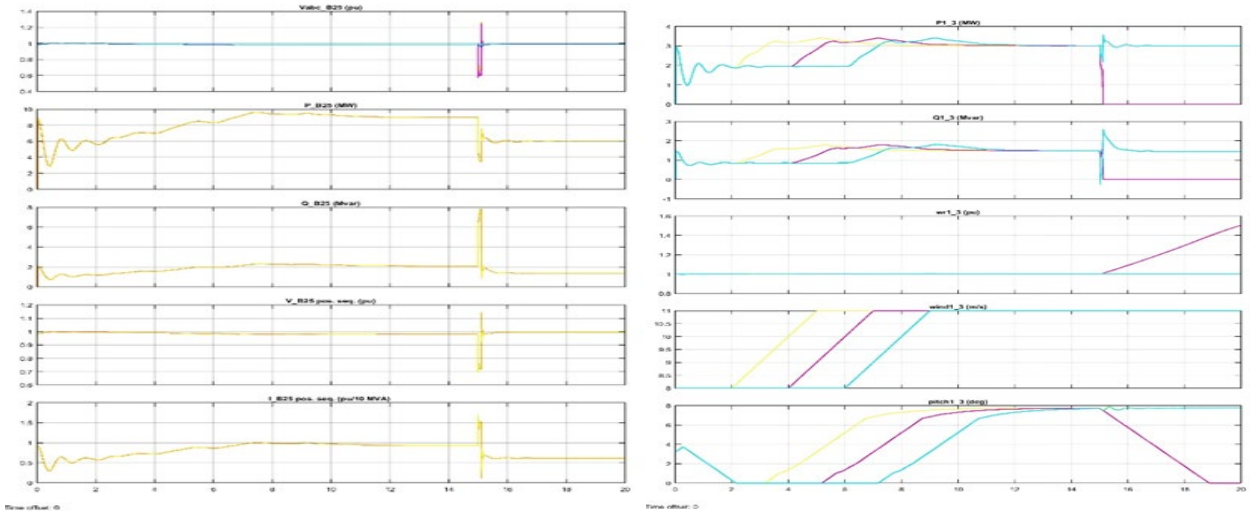
Фиг. 8. Управление включване/изключване на STATCOM чрез блок Manual Switch.

Режим 2 – работа без STATCOM. Логическото състояние трябва да бъде в позиция [1] и STATCOM се изключва и системата **работи без динамична компенсация**, като чрез диаграми се сравняват режимите (фиг. 8).

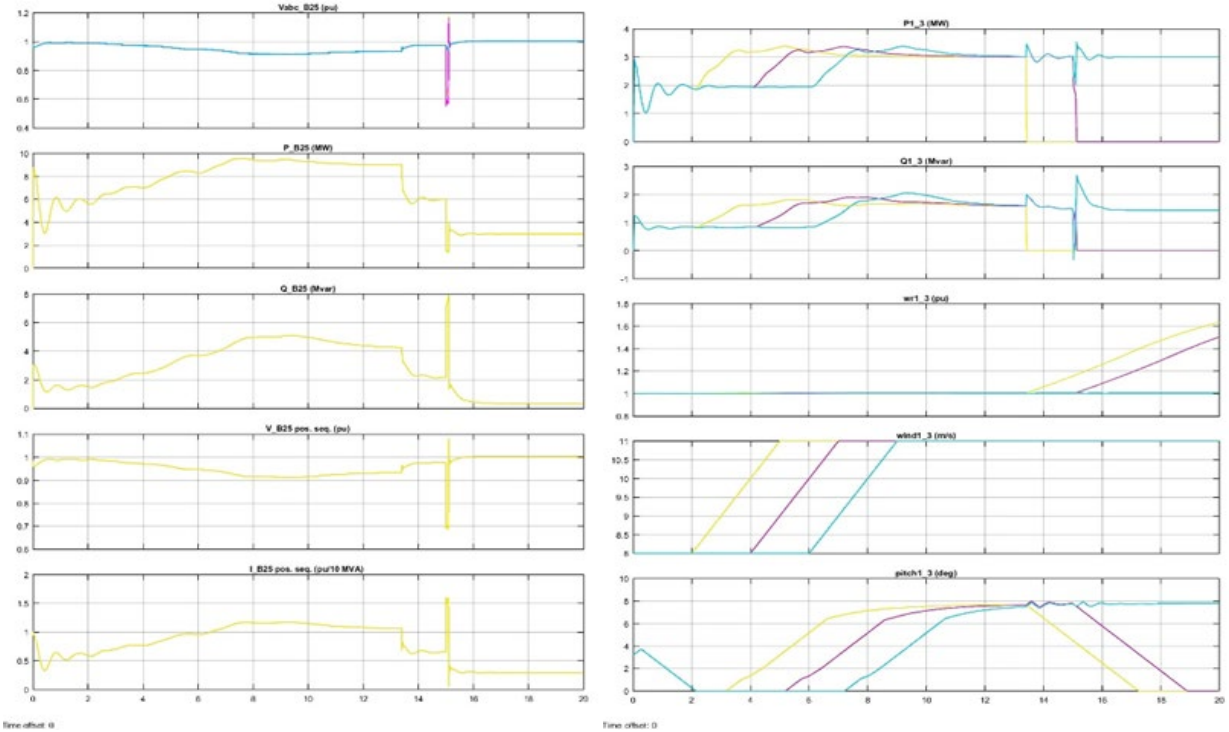
Анализ на резултатите от работните и аварийните режими на виртуалната вятърна централа в Simulink

•Аварийна работа на турбина 2

Получените резултати от симулацията са представени на фиг. 9 с включен **статичен синхронен компенсатор STATCOM** и фиг. 10 с изключен STATCOM.



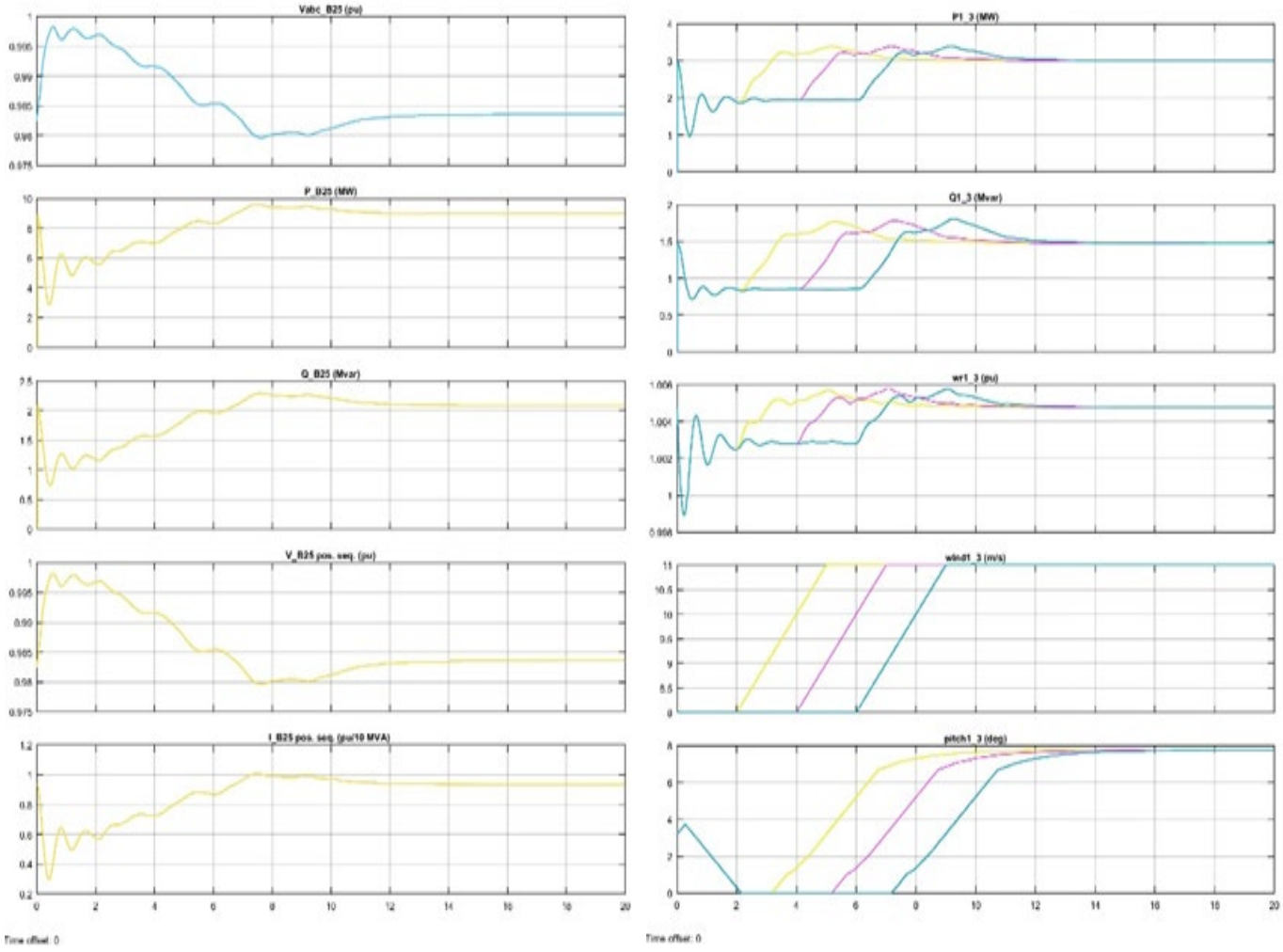
Фиг. 9. Изменение на параметрите при късо съединение с включен STATCOM.



Фиг. 10. Изменение на параметрите при късо съединение без STATCOM.

Сравнителният анализ установява, че при включен **статичен синхронен компенсатор STATCOM** спадът на напрежението е по-малък и изменението на реактивната мощност е ограничено, като възстановяването на режима е по-бързо. Динамичната компенсация моделирана от блок STATCOM на фиг. 9 ефективно стабилизира работния режим на консуматорите.

• Резултати от симулация на нормален режим на работа на вятърната централа



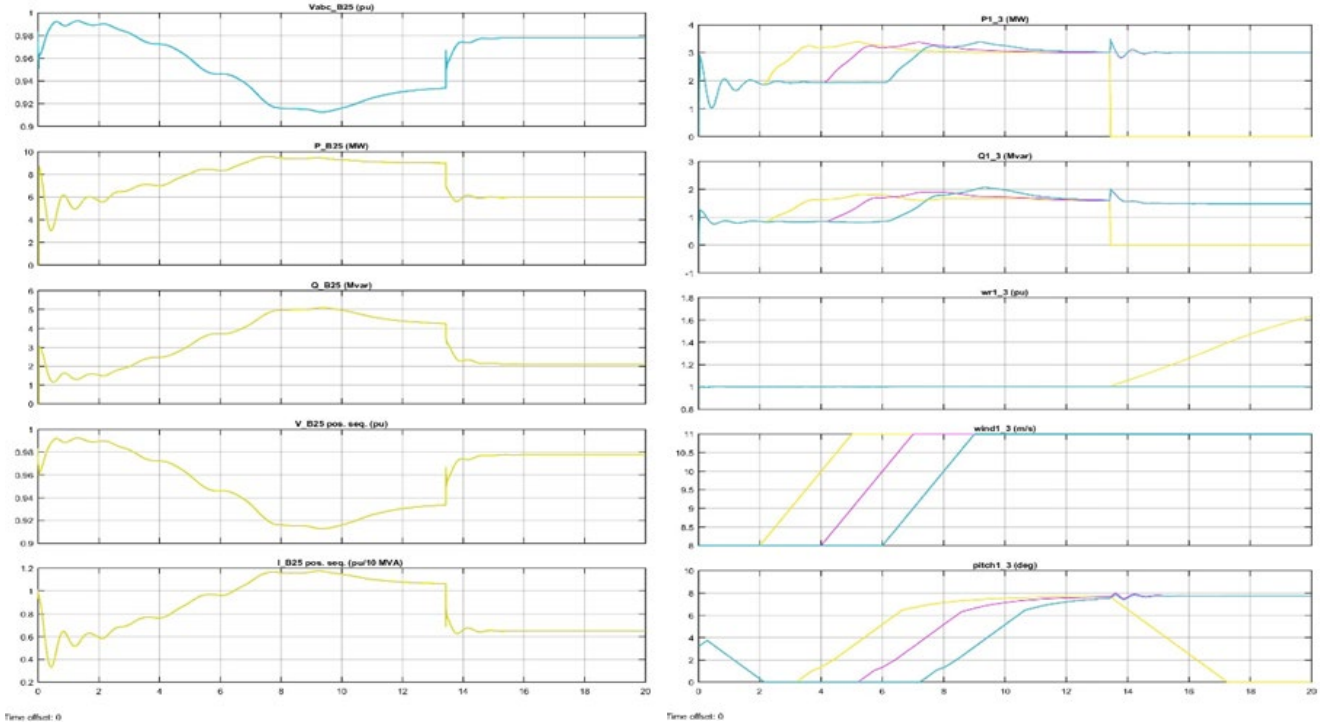
Фиг. 11 Диаграми от работата на системата с включен STATCOM;

При работа без STATCOM от фиг. 12 се наблюдава изменение режима на турбина 1 след достигане на максималната мощност. Чрез изменение на ъгъла на наклон на лопатките се намалява механичната мощност, но това води до понижение на производителността на системата.

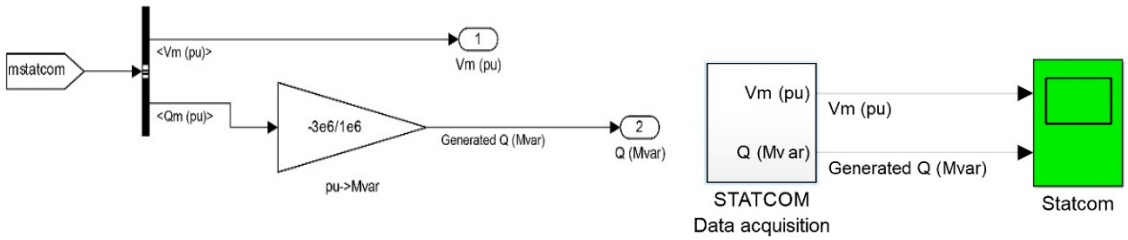
Анализ от влиянието на статичен синхронен компенсатор STATCOM върху стабилността на параметрите при различните режими на работа на централата.

Математическият библиотечен модел от свързани блокове отчитащи алгоритъма на компенсатора и измервателни блокове с виртуален осцилоскоп са показани на фиг. 13.

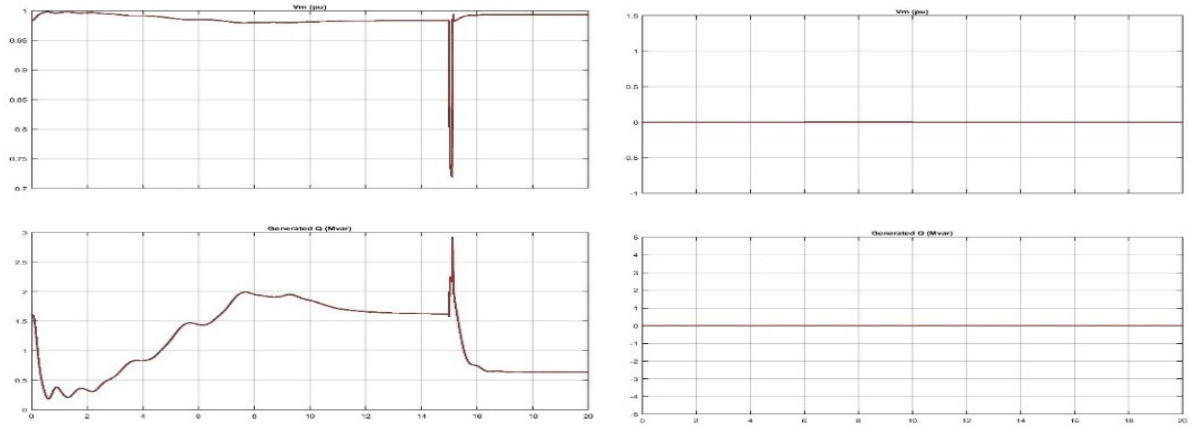
Получените времедиаграми показват реакцията на системата при включен и изключен **статичен синхронен компенсатор STATCOM**.



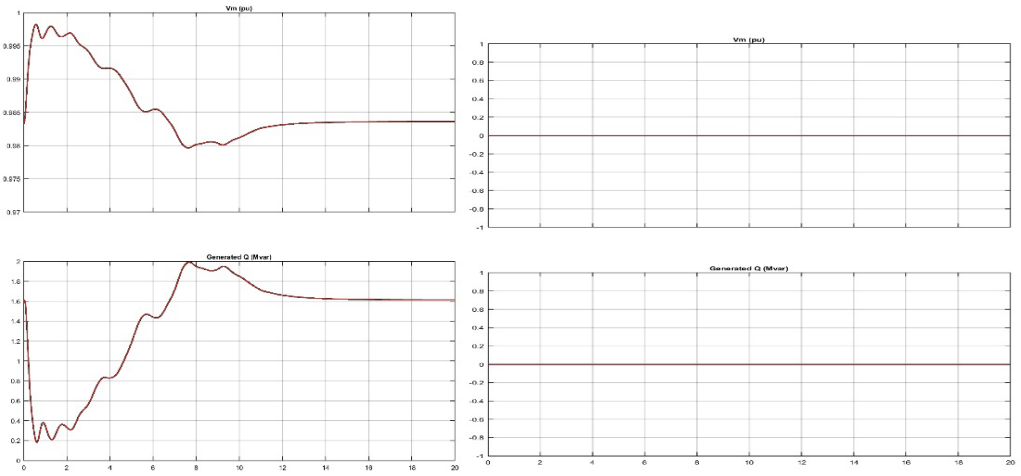
Фиг. 12 Диаграми от работата на системата с изключен STATCOM.



Фиг. 13. Блокова структура за измерване и анализ на параметрите на STATCOM.



Фиг. 14 Графики от режим на късо съединение при включен-вляво и изключен –вдясно STATCOM



Фиг. 15 Графики от нормален режим при включен- вляво и изключен – вдясно STATCOM

5 Изводи

Резултатите от симулацията на библиотечния модел в показват, че добавеният модел на **статичен синхронен компенсатор STATCOM** подобрява работата на вятърната електроцентрала осъществявайки динамична компенсация на реактивната мощност, стабилизира стойностите на напрежението и ограничава преходните процеси при аварийни режими, чрез компенсация на енергията с помощта на STATCOM или инерционни елементи, като капацитети и индуктивности.

● **Анализ от регулирането на вятърната турбина**

Оптималното използване на енергията на вятърния поток се постига чрез управление на ъгъла на атака на лопатките и скоростта на въртене на ротора на асинхронния генератор. Моделът при скорости на вятъра под номиналните стойности увеличава честотата на въртене с ефект на максимално използване на наличната енергия.

Високи скорости на вятъра предизвикват автоматично регулиране на ъгъла на лопатките с около 8^0, ограничавайки механичната мощност и предотвратявайки претоварването на турбината и асинхронния генератор.

ЛИТЕРАТУРА:

[1] Jenkins N., Burton T., Bossanyi E., Sharpe D., Graham M. Wind Energy Handbook. 3rd ed. Chichester: Wiley, 2021. DOI: 10.1002/9781119451143.

[2] Manwell J. F., McGowan J. G., Rogers A. L. Wind Energy Explained: Theory, Design and Application. 2nd ed. Chichester: Wiley, 2009. DOI: 10.1002/9781119994367.

[3] IEC. IEC 61400-12-1:2022. Wind Energy Generation Systems – Part 12-1: Power Performance Measurements of Electricity Producing Wind Turbines. Geneva: International Electrotechnical Commission, 2022. ISBN 978-2-8322-5621-3.

[4] MathWorks. Renewable Energy – MATLAB & Simulink. MathWorks Documentation.

[5] MathWorks. Wind Turbine Induction Generator (Phasor Type) – Implement Phasor Model of Squirrel-Cage Induction Generator Driven by Variable Pitch Wind Turbine. MATLAB & Simulink Documentation.

[6] Petrov, Y. Modeling Of Transients Processies In Linear Electric Circuit Of The Second Order With Generalised Net. Annual of Assen Zlatarov University – Burgas, Bulgaria, Vol. XLVI, No. 1, 2019.

[7] Мечкова, В., Станева, Л., Мечков, Б., Бъндева, К. Моделиране на преходни процеси в електрическа верига с MATLAB. Годишник на Университет „Проф. д-р Асен Златаров“, Бургас, т. XXXVIII, № 1, 2009, с. 130–132.

IMPACT OF NEW NETWORK TECHNOLOGIES ON THE QUALITY OF COMMUNICATION SERVICES*

ALEKS YA. DANEV, ILKER A. HATIB

ABSTRACT: *This report examines the impact of new network technologies on the quality of communication services. The main features and advantages of technologies such as 5G, the Internet of Things (IoT), cloud computing and software-defined networks are analysed. Their impact on the speed, reliability, security and efficiency of communications is examined. The main challenges and future prospects for the development of modern communication networks are also presented. The report shows that new network technologies are a key factor in improving the quality of communication services and in the development of the digital society.*

KEYWORDS: *IoT, networks, technologies*

DOI: https://doi.org/10.46687/MT26AYD

ВЛИЯНИЕ НА НОВИТЕ МРЕЖОВИ ТЕХНОЛОГИИ ВЪРХУ КАЧЕСТВОТО НА КОМУНИКАЦИОННИТЕ УСЛУГИ

АЛЕКС Я. ДАНЕВ, ИЛКЕР А. ХАТИБ

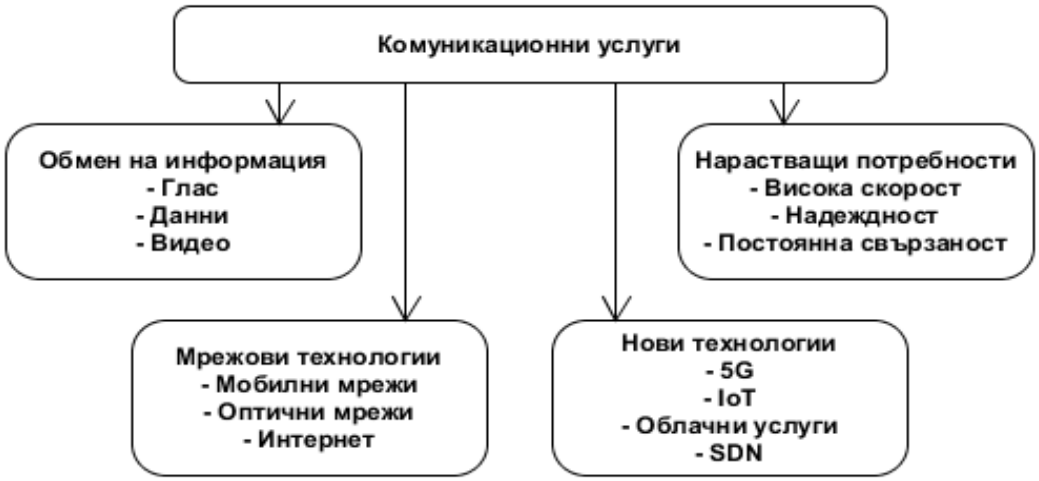
АБСТРАКТ: *Настоящият доклад разглежда влиянието на новите мрежови технологии върху качеството на комуникационните услуги. Анализирани са основните характеристики и предимства на технологии като 5G, Интернет на нещата (IoT), облачните изчисления и софтуерно дефинираните мрежи. Разгледано е тяхното въздействие върху скоростта, надеждността, сигурността и ефективността на комуникациите. Представени са също основните предизвикателства и бъдещите перспективи пред развитието на съвременните комуникационни мрежи. Докладът показва, че новите мрежови технологии са ключов фактор за подобряване качеството на комуникационните услуги и за развитието на цифровото общество.*

1 Въведение

Съвременното информационно общество е немислимо без надеждни комуникационни услуги. Те осигуряват възможност за обмен на информация в реално време между потребители, организации и устройства по целия свят. През последните години се наблюдава експоненциално нарастване на обема на обменяните данни. Причините за това са развитието на мобилните технологии, увеличеното използване на мултимедийно съдържание и широкото навлизане на цифровите услуги. Мрежовите технологии са в основата на този процес. Те определят начина, по който данните се предават, обработват и съхраняват. Всяко ново поколение мрежова инфраструктура води до подобрения в качеството на предоставяните комуникационни услуги. Особено значима роля играят безжичните технологии, които позволяват мобилност и достъп до информация независимо от местоположението на потребителя. Развитието на 5G мрежите поставя началото на нов етап в телекомуникационния сектор [4]. Целта на настоящия доклад е да анализира влиянието на новите мрежови технологии върху качеството на комуникационните услуги, като се разгледат основните технологични решения, техните предимства и възможните

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

предизвикателства пред бъдещото развитие на сектора. На фиг.1 е показана йерархична схема на развитието на комуникационните услуги.

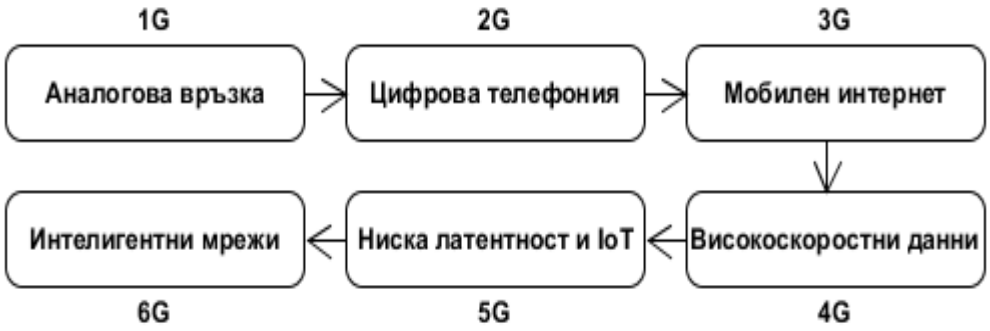


Фиг. 1. Развитие на комуникационните услуги

2 Развитие на съвременните мрежови технологии

Първите компютърни мрежи са били създадени с цел обмен на ограничени количества информация между малък брой устройства. С течение на времето потребностите от по-бърза и надеждна комуникация нарастват значително. Развитието на интернет технологиите води до създаването на глобални комуникационни инфраструктури. Благодарение на тях милиарди потребители могат да обменят информация в реално време независимо от географското си местоположение. Мобилните комуникации също претърпяват значителна еволюция. От първите аналогови мрежи до съвременните 5G системи се наблюдава многократно увеличение на скоростта на предаване на данни и подобряване на качеството на услугите. Оптичните мрежи представляват друг важен елемент от развитието на телекомуникациите. Те осигуряват изключително висока пропускателна способност и минимални загуби при предаване на информация. В резултат на тези технологични промени се създават предпоставки за предоставяне на нови услуги, които преди са били невъзможни или икономически неизгодни за реализация. С развитието на широколентовия интернет се създадоха условия за предоставяне на разнообразни цифрови услуги. Онлайн образованието, електронната търговия и дистанционната работа се превърнаха в неразделна част от ежедневието на милиони хора по света. Важен етап в развитието на мрежовите технологии е преминаването към пакетно предаване на данни. Този подход позволява по-ефективно използване на наличните ресурси и осигурява по-висока надеждност на комуникациите. Появата на виртуализацията в мрежите значително промени начина, по който се изграждат и управляват комуникационните инфраструктури. Чрез виртуални ресурси операторите могат по-лесно да адаптират услугите към нуждите на потребителите. Съвременните мрежи все по-често използват автоматизирани механизми за управление и мониторинг. Това води до намаляване на времето за реакция при възникване на проблеми и повишава качеството на обслужване. Отделни разработки разглеждат Bluetooth [5], оптичните кабели за подводни системи [6], предаването чрез видима светлина и

сравнението между безжични технологии и Li-Fi [11, 13]. Проектирането и оценяването на мрежи с Network Notepad и Cisco Packet Tracer са разгледани в [1, 14]. На фиг. 2 е показано развитието на съвременните мрежови технологии.



Фиг. 2. Развитие на съвременните мрежови технологии

3 Влияние на 5G технологиите върху комуникационните услуги

Петото поколение мобилни мрежи представлява една от най-значимите иновации в телекомуникационния сектор. Технологията е разработена с цел да отговори на нарастващите изисквания за по-висока скорост и по-ниска латентност. Едно от основните предимства на 5G е възможността за предаване на големи обеми данни за много кратко време. Това позволява по-качествено използване на мултимедийни приложения и стрийминг услуги. Ниското закъснение е друг важен фактор за подобряване качеството на комуникационните услуги. То е особено важно при приложения като дистанционно управление, автономни превозни средства и телемедицина. 5G мрежите позволяват свързването на значително по-голям брой устройства в сравнение с предходните поколения мобилни технологии. Това създава благоприятни условия за развитието на Интернет на нещата. Благодарение на тези характеристики 5G се превръща в ключов фактор за цифровата трансформация на обществото и бизнеса. Една от ключовите особености на 5G е използването на по-широк честотен спектър. Това позволява значително увеличаване на капацитета на мрежата и по-ефективно обслужване на голям брой потребители едновременно. Технологията подпомага развитието на интелигентни градове, в които различни системи за управление на транспорта, енергията и обществените услуги обменят информация в реално време. В индустриалната автоматизация 5G създава възможности за използване на роботи и автоматизирани производствени линии с минимално закъснение при обмена на данни. Това повишава производителността и намалява риска от грешки. Освен технологичните предимства, внедряването на 5G оказва положително влияние върху икономическото развитие чрез създаване на нови бизнес модели и възможности за иновации в различни сектори. Таблица 1 представя съпоставка между 4G и 5G технологии.

4 Ролята на интернет на нещата (IoT)

Интернет на нещата представлява концепция, при която различни устройства са свързани към мрежата и обменят информация без необходимост от постоянна човешка намеса. Развитието на IoT води до значително увеличаване на броя на устройствата, които

използват комуникационни услуги. Това поставя нови изисквания към мрежовата инфраструктура. Умните домове са един от най-разпространените примери за приложение на IoT технологиите. Чрез тях потребителите могат дистанционно да управляват различни устройства и системи. В индустриалния сектор IoT се използва за мониторинг и управление на производствени процеси. Това позволява оптимизиране на ресурсите и повишаване на ефективността. Нарастващият брой свързани устройства стимулира развитието на по-надеждни и мащабируеми комуникационни мрежи, способни да осигурят високо качество на услугите. В здравеопазването IoT устройствата позволяват непрекъснато наблюдение на пациенти чрез интелигентни сензори и носими устройства. Това улеснява ранното откриване на здравословни проблеми и подобрява медицинското обслужване. В селското стопанство технологията се използва за наблюдение на почвената влажност, климатичните условия и състоянието на културите. По този начин се оптимизира използването на ресурси и се повишава добивът. Интелигентните транспортни системи също разчитат на IoT решения за събиране и анализ на информация за трафика. Това допринася за намаляване на задръстванията и подобряване безопасността на движението. Разширяването на IoT екосистемата изисква стандартизирани комуникационни протоколи, които да гарантират съвместимост между устройствата и ефективен обмен на данни в различни среди. Изграждането на индустриални комуникационни мрежи, безжичните сензорни модули и Wi-Fi протоколите са разгледани в [7–9], а модел на интерактивна система с ултрашироколентови сензори е представен в [18]. На фиг. 3 е показана ролята на Интернет на нещата.



Фиг. 3. Ролята на Интернет на нещата

Таблица 1. Сравнение между 4G и 5G технологии

Показател	4G	5G
Скорост на предаване	До 1 Gbps	До 10–20 Gbps
Латентност	30–50 ms	1–10 ms
Брой свързани устройства	Ограничен	Значително по-голям
Надеждност на връзката	Висока	Много висока
Поддръжка на IoT	Ограничена	Оптимизирана

5 Облачни технологии и софтуерно дефинирани мрежи

Облачните технологии променят начина, по който се съхранява и обработва информацията. Вместо локални ресурси се използват разпределени центрове за данни, достъпни чрез интернет. Този подход осигурява по-голяма гъвкавост и възможност за бързо разширяване на ресурсите според нуждите на потребителите и организациите. Софтуерно дефинираните мрежи позволяват централизирано управление на мрежовата инфраструктура чрез софтуерни решения. Това улеснява конфигурирането и поддръжката на комуникационните системи [17]. Интелигентните комутатори, качеството на данните в индустриални мрежи и адаптивното управление на трафика са разгледани в [12, 15, 16]. Комбинацията между облачни технологии и SDN подобрява ефективността на мрежовите операции и намалява времето за реакция при възникване на проблеми. В резултат качеството на комуникационните услуги се повишава чрез по-добро управление на ресурсите и по-висока надеждност на системите. Облачните платформи предоставят възможност за достъп до приложения и данни от всяка точка с интернет свързаност. Това улеснява сътрудничеството между потребители и организации независимо от тяхното местоположение. Много компании използват облачни услуги за съхранение на големи масиви от информация и архивиране на критични данни. Това повишава надеждността на информационните системи и намалява риска от загуба на информация. Софтуерно дефинираните мрежи позволяват по-добро разпределение на трафика в зависимост от натоварването на инфраструктурата. Така се постига по-висока ефективност и оптимално използване на наличните ресурси. Допълнително предимство на тези технологии е възможността за бързо внедряване на нови услуги без необходимост от значителни промени във физическата инфраструктура на мрежата. В таблица 2 са показани характеристиките на облачните технологии.

Таблица 2. Характеристики на облачните технологии и софтуерно дефинираните мрежи

Характеристика	Облачни технологии	Софтуерно дефинирани мрежи (SDN)
Основна функция	Съхранение и обработка на данни	Управление на мрежовия трафик
Управление	Централизирани облачни платформи	Централизиран контролер
Гъвкавост	Висока	Висока
Мащабируемост	Лесно увеличаване на ресурсите	Лесно адаптиране на мрежата
Ползи за комуникационните услуги	Достъпност и надеждност	По-добра производителност и контрол

Облачните технологии и софтуерно дефинираните мрежи са сред основните компоненти на съвременната комуникационна инфраструктура. Те осигуряват по-ефективно управление на ресурсите, по-висока надеждност на услугите и възможност за бързо адаптиране към променящите се потребности на потребителите и организациите

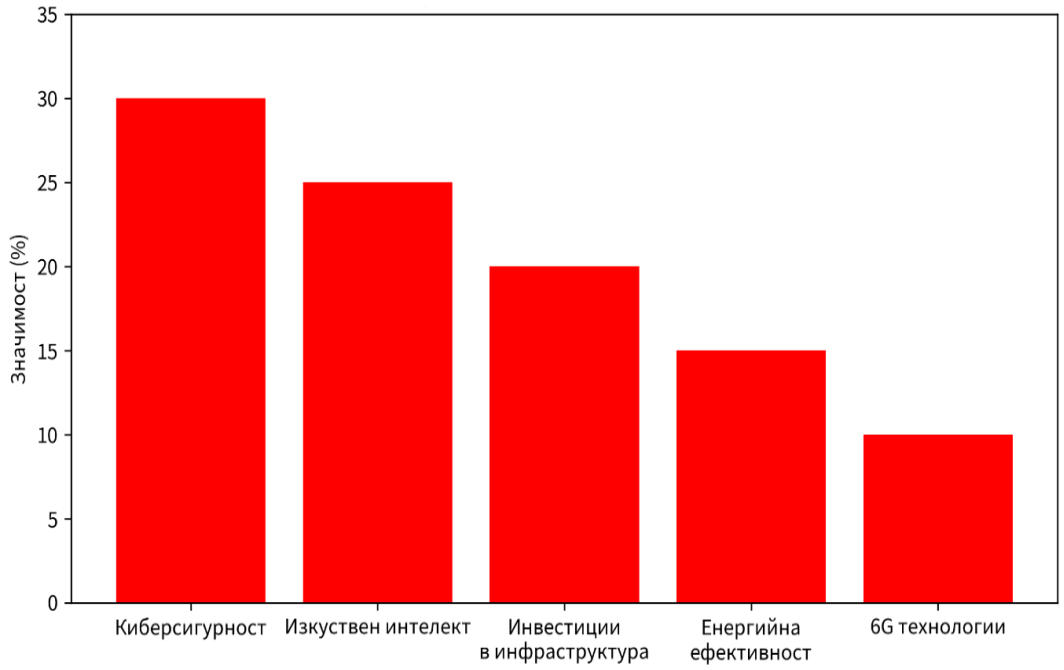
6 Предизвикателства и перспективи пред бъдещите комуникационни мрежи

Въпреки значителния напредък съществуват редица предизвикателства пред развитието на комуникационните мрежи. Сред тях са нарастващите изисквания за сигурност и защита на личните данни. Киберзаплахите се превръщат във все по-сериозен проблем за операторите и потребителите. Това налага внедряването на нови механизми за защита на комуникационната инфраструктура. Уязвимостите на безжични мрежи с WPA2 са разгледани в [3], а хардуерни реализации на генератори на псевдослучайни последователности за криптографски приложения са представени в [2, 10]. Друг важен въпрос е необходимостта от значителни инвестиции за изграждане и поддръжка на модерни мрежови системи. Финансовите разходи често представляват сериозно предизвикателство за доставчиците на услуги. Развитието на изкуствения интелект и машинното обучение предоставя нови възможности за автоматизирано управление на мрежите и оптимизация на ресурсите. В бъдеще се очаква внедряването на 6G технологии, които ще предложат още по-висока скорост, по-ниска латентност и нови възможности за комуникация между хора, устройства и интелигентни системи. С нарастването на броя на свързаните устройства се увеличава и необходимостта от по-ефективно управление на мрежовия трафик. Това изисква внедряване на интелигентни алгоритми за анализ и оптимизация на комуникациите. Енергийната ефективност се превръща във все по-важен фактор при изграждането на нови мрежови инфраструктури. Намаляването на енергийното потребление е от съществено значение както от икономическа, така и от екологична гледна точка. Глобалната свързаност изисква сътрудничество между държави, оператори и технологични компании за създаване на общи стандарти и политики в областта на комуникациите. Очаква се бъдещите поколения мрежи да интегрират още по-тясно изкуствения интелект, квантовите комуникации и автоматизираните системи за управление, което ще доведе до ново ниво на качество и ефективност на комуникационните услуги. На таблица 3 е показана значимостта на основните фактори за развитието на бъдещите комуникационни мрежи, а на фиг. 4 са онагледени процентните разпределения.

Таблица 3. Значимост на основните фактори за развитието на бъдещите комуникационни мрежи

Фактор	Значимост (%)
Киберсигурност и защита на данните	30
Развитие на изкуствения интелект	25
Инвестиции в инфраструктура	20
Енергийна ефективност	15
Внедряване на 6G технологии	10

От представените данни се вижда, че киберсигурността и защитата на данните се разглеждат като най-значимото предизвикателство пред бъдещите комуникационни мрежи. Висока значимост имат също развитието на изкуствения интелект и необходимостта от инвестиции в инфраструктура. Това показва, че бъдещото развитие на комуникационните технологии ще зависи както от технологичните иновации, така и от способността за осигуряване на сигурна и надеждна мрежова среда.



Фиг. 4. Оценка на значимостта на факторите за развитие на комуникационната инфраструктура

7 Заключение

Новите мрежови технологии оказват съществено влияние върху качеството на комуникационните услуги. Те създават условия за по-бърз, надежден и сигурен обмен на информация, като същевременно разширяват възможностите за предоставяне на разнообразни цифрови услуги. Благодарение на непрекъснатото развитие на комуникационните мрежи се подобрява достъпът до информация и се улеснява взаимодействието между потребители, организации и устройства. Развитието на 5G мрежите, Интернет на нещата (IoT) и облачните технологии променя традиционните модели на комуникация и създава предпоставки за внедряване на иновативни решения в различни сфери на обществения и икономическия живот. Тези технологии подпомагат автоматизацията на процесите, повишават ефективността на работата и създават нови възможности за развитие на бизнеса и публичните услуги. Подобряването на ключови показатели като скорост на предаване на данни, надеждност на връзката и ниска латентност допринася за повишаване удовлетвореността на потребителите и за по-ефективното функциониране на организациите. В резултат на това комуникационните услуги се превръщат в основен фактор за развитието на цифровата икономика и съвременното информационно общество. Развитието на комуникационните технологии оказва влияние не само върху техническите аспекти на обмена на информация, но и върху начина, по който хората работят, учат и общуват. Съвременните мрежови решения предоставят възможност за дистанционна работа, онлайн обучение и достъп до разнообразни услуги независимо от географското местоположение на потребителите. Въпреки многобройните предимства, съществуват и редица предизвикателства, свързани със сигурността на данните, управлението на мрежовите ресурси и необходимостта от значителни инвестиции в инфраструктура. За успешното развитие на комуникационния сектор е необходимо непрекъснато усъвършенстване на технологиите, както и прилагане на ефективни мерки за

защита на информационните системи. С нарастването на потребностите от свързаност и обмен на данни ще се увеличава и значението на модерните мрежови решения. Инвестициите в нови технологии и развитието на квалифицирани специалисти ще бъдат ключови фактори за поддържане на високо качество на комуникационните услуги и за успешното внедряване на бъдещи иновации. В заключение може да се обобщи, че новите мрежови технологии са сред основните двигатели на цифровата трансформация в съвременното общество. Тяхното бъдещо развитие ще продължи да подобрява качеството на комуникационните услуги, да създава нови възможности за иновации и да допринася за икономическия растеж и глобалната свързаност през следващите десетилетия.

ЛИТЕРАТУРА:

[1] Казаков Ст. Изграждане на информационна мрежа с Network Notepad. MATTEX 2024, сборник доклади, т. 2, Шумен, 2024, с. 94–102. ISSN 1314-3921.

[2] Николов Н. Р., Цанков Ц. С. Хардуерна реализация на генератор на псевдослучайни последователности, описван с полином от 1024 степен, и програмно управление на обратните връзки. Научна сесия 2010, сборник научни трудове, част I, НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, Шумен, 2011, с. 159–163. ISSN 1313-7433.

[3] Николов Л. Анализ на уязвимостта на безжична компютърна мрежа, защитена с криптографски протокол WPA2. Proceedings of the XXVI International Scientific Conference Trans&Motauto, Burgas, 2018, Vol. 2, pp. 252–253, ISSN 1313-5031 (Print), ISSN 2535-0307 (Online).

[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., Examination of Bluetooth and its Protocol and Applications, 2021, Annual of Konstantin Preslavski University of Shumen, Vol. XI E, Faculty of technical sciences, ISSN 1311-834X, pp. 114-120.

[6] Denev D., Analysis of the Requirements for Optical Cables for Construction of Underwater Transmission Systems, 2021, Journal scientific and applied research, vol. 21, International Journal, ISSN 1314-6289, pp. 75-79.

[7] Denev D., Tsankov Ts., Design and Implementation of a Field Level of an Industrial Communication Network for the Needs of the Industry, 2022, 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies ICEST 2022, Ohrid, North Macedonia, 16-18 June, ISBN 978-1-6654-8500-5 and DOI 10.1108/ICEST55168.2022.9828607

[8] 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.

[9] Denev D., Research of Wi-Fi and its Protocols, 2022, Conference with international participation MATTEH 2022, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 95-101.

[10] Iliev M. P., Nikolov N. R., Tsankov T. Sv. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Electrotechnica & Electronica, Vol. 46, No. 7–8, 2011, pp. 29–33. ISSN 0861-4717.

[11] Konstantinova E., Tsankov Ts. Capabilities for high-speed data transmission through the use of visible light. International Scientific Conference “Defense Technologies” DefTech 2020, Shumen, 2020, ISSN 2367-7902, pp. 379–385.

[12] Tsankov Ts., Docheva A. Implementing smart switches and technologies in communication networks. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, 2024, ISSN 1314-8818, pp. 103–110. https://doi.org/10.46687/YT24CAL

[13] Denev D., Comparative Analysis Between Wireless and Li-Fi, 2022, Conference with international participation MATTEH 2022, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 89-94.

[14] 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.

[15] 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.

[16] Denev D., Adaptive Traffic Management Algorithms in Ultra-Reliable Low-Latency Networks, 2025, Black Sea Journal of Engineering and Transport, Vol. I, ISSN:3033-2885, pp.12-16.

[17] Uzun, M. B., Atanasov, V. T. Common conception of software-defined networks. Annual of Konstantin Preslavsky University of Shumen, Vol. XIII E, 2023, pp. 112–119, ISSN 2815-4703 (Online).

[18] Atanasov, V., Trifonov, T. A new model of ultra wideband sensors based interactive system. International Journal on Information Technologies and Security, Vol. 16, No. 1, 2024, pp. 39–48, ISSN 1313-8251. https://doi.org/10.59035/XYCG3094

THE ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN INDUSTRIAL AUTOMATION*

DANIEL R. DENEV

ABSTRACT: *Artificial intelligence is becoming one of the most significant technologies that transform modern industrial production. By implementing intelligent algorithms and systems, enterprises achieve higher productivity, reduce costs and improve product quality. The integration of AI in industrial automation allows for the processing of large volumes of data in real time, which helps make more accurate and effective management decisions. This report examines the main areas of application of artificial intelligence in industrial automation. The opportunities for optimization of production processes, predictive maintenance, robotization, quality management and the challenges in implementing intelligent systems are analyzed. The goal is to present the importance of AI as a key factor for the development of industry in the 21st century.*

KEYWORDS: *Artificial Intelligence, Industrial Automation, Predictive Maintenance, Smart Manufacturing, Machine Learning*

DOI: https://doi.org/10.46687/MT26DRD

РОЛЯТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В СЪВРЕМЕННАТА ИНДУСТРИАЛНА АВТОМАТИЗАЦИЯ

ДАНИЕЛ Р. ДЕНЕВ

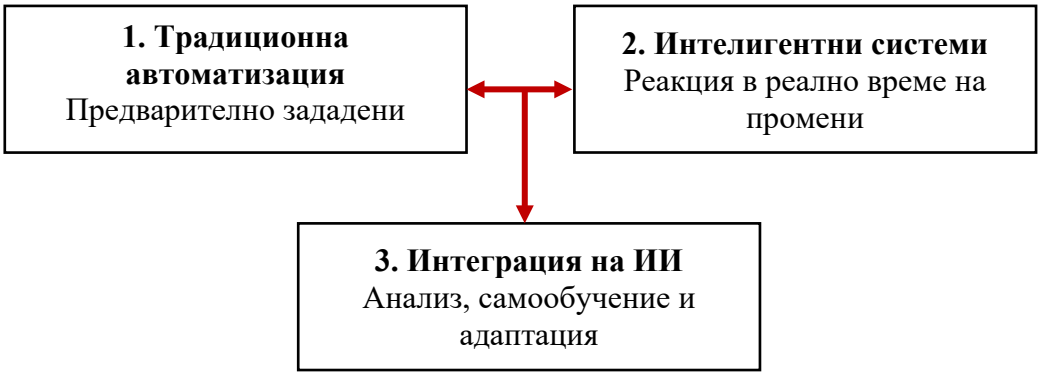
АБСТРАКТ: *Изкуственият интелект се превръща в една от най-значимите технологии, които трансформират съвременното индустриално производство. Чрез внедряването на интелигентни алгоритми и системи предприятията постигат по-висока производителност, намаляване на разходите и подобряване на качеството на продукцията. Интеграцията на ИИ в индустриалната автоматизация позволява обработка на големи обеми данни в реално време, което подпомага вземането на по-точни и ефективни управленски решения. Настоящият доклад разглежда основните направления на приложение на изкуствения интелект в индустриалната автоматизация. Анализирани са възможностите за оптимизация на производствените процеси, предиктивната поддръжка, роботизацията, управлението на качеството и предизвикателствата при внедряването на интелигентни системи. Целта е да се представи значението на ИИ като ключов фактор за развитието на индустрията през XXI век.*

1 Въведение

Развитието на цифровите технологии през последните десетилетия доведе до значителни промени в начина, по който функционират индустриалните предприятия. Автоматизацията постепенно се превърна в основен инструмент за повишаване на ефективността и конкурентоспособността на производството. В този контекст изкуственият интелект заема централно място като технология, способна да надгради традиционните автоматизирани системи чрез анализ, самообучение и адаптация към променящите се условия. Индустриалната автоматизация вече не се ограничава единствено до изпълнение на предварително зададени команди. Благодарение на изкуствения интелект машините могат да анализират информация, да разпознават модели и да вземат решения в реално

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

време. Това създава предпоставки за изграждането на интелигентни производствени системи, които реагират бързо на промените в производствената среда и повишават общата ефективност на предприятията. На фиг. 1 е показани етапите на еволюция на автоматизацията.



Фиг. 1. Еволюция на индустриалната автоматизация

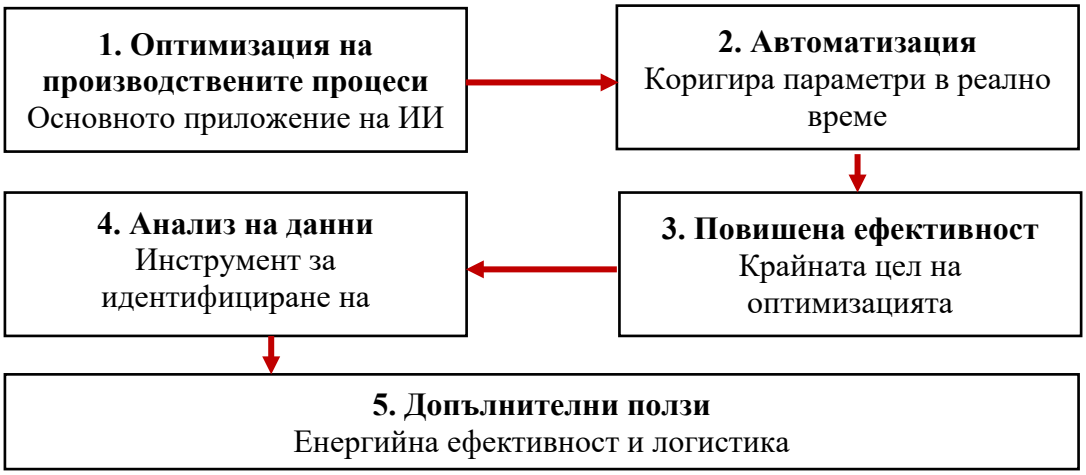
2 Изкуствен интелект и оптимизация на производствените процеси

Една от основните области на приложение на изкуствения интелект е оптимизацията на производствените процеси. Чрез използването на алгоритми за машинно обучение предприятията могат да анализират големи количества производствени данни и да идентифицират факторите, които влияят върху производителността. Това позволява по-добро планиране на ресурсите и намаляване на производствените загуби. Интелигентните системи могат автоматично да коригират параметрите на производствените линии в зависимост от текущите условия. По този начин се осигурява по-стабилен производствен процес и се намалява рискът от възникване на грешки. Резултатът е по-висока ефективност и по-добро използване на наличните ресурси. Управлението на ресурси в компютърни индустриални мрежи е разгледано в [7]. Примери за други оптимизационни задачи са имунните алгоритми за синтез на сигнали [1, 5], а за паралелна изчислителна инфраструктура е описана клъстерна система в среда MPI [6]. Освен това ИИ подпомага оптимизирането на енергийното потребление и логистичните процеси в предприятията. Чрез анализ на данни в реално време могат да бъдат открити възможности за намаляване на разходите и повишаване на устойчивостта на производството. Съвременните платформи за индустриален анализ използват изкуствен интелект за прогнозиране на натоварването на производствените линии и за оптимално разпределение на задачите между различните производствени звена. Това позволява по-добро управление на капацитета и предотвратява образуването на тесни места в производствения цикъл. В резултат се съкращава времето за производство и се повишава общата ефективност на предприятието. На фиг. 1 е показано приложението на изкуствения интелект в производството.

3 Предиктивна поддръжка на индустриално оборудване

Поддръжката на производственото оборудване е критичен фактор за непрекъснатостта на производствения процес. Традиционните методи за поддръжка често се основават на предварително определени графици, които не винаги отразяват реалното състояние на машините. Изкуственият интелект предлага по-ефективен подход чрез предиктивна поддръжка. С помощта на сензори и интелигентни алгоритми се събират и

анализират данни за работата на оборудването. Системите могат да разпознават признаци за бъдещи повреди още преди те да са настъпили. Това позволява извършването на навременни ремонтни дейности и предотвратяване на непланирани производствени спирания. Прилагането на предиктивна поддръжка води до удължаване на експлоатационния живот на оборудването и намаляване на разходите за ремонти. В същото време се повишава надеждността на производствените системи и се подобрява безопасността на работната среда. Важна характеристика на предиктивната поддръжка е възможността за непрекъснат мониторинг на критични параметри като температура, вибрации, налягане и електрическа консумация. Чрез анализ на тези показатели системите могат да откриват дори минимални отклонения от нормалния режим на работа. Това създава условия за ранна диагностика и намалява вероятността от сериозни аварии. Освен техническите предимства, предиктивната поддръжка има и значителен икономически ефект. Намаляването на непланираните престои води до по-добро изпълнение на производствените графици и по-висока удовлетвореност на клиентите. В дългосрочен план предприятията постигат по-ниски експлоатационни разходи и по-добра възвръщаемост на инвестициите в оборудване [10, 12, 14].



Фиг. 2. Приложения на изкуствения интелект в производството

Средно време между откази

Показва средното време на работа на оборудването между две последователни повреди.

T – общо време на работа

N – брой повреди

Машина е работила 6000 часа и са регистрирани 4 повреди. Следователно средно на всеки 1500 часа се очаква отказ.

$$\text{MTBF} = \frac{\text{T}}{\text{N}} = \frac{6000}{4} = 1500\text{ч} \quad (1)$$

Средно време за ремонт

T_r – общо време на работа

N – брой повреди

Показва колко време е необходимо за възстановяване на оборудването след повреда. За 4 повреди са изразходвани общо 20 часа ремонт.

$$MTTR = \frac{T_r}{N} = \frac{20}{4} = 5\text{ч} \quad (2)$$

Коефициент на готовност

Показва вероятността машината да бъде в работоспособно състояние. При MTBF = 1500 часа и MTTR = 5 часа:

$$A = \frac{MTBF}{MTBF+MTTR} = \frac{1500}{1500+5} = 0.9967 \approx 99{,}67\% \quad (3)$$

Среднoквадратична стойност на вибрациите

Използва се за оценка на вибрациите на лагери, валове и електродвигатели. По-високата RMS стойност често е индикатор за износване или възникващ дефект.

$$RMS = \sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2} \quad (4)$$

n – брой измервания;

x_i – стойност на i-тото измерване.

Измерени на вибрации са със стойности $x_1 = 2\text{mm/s}, x_2 = 3\text{mm/s}, x_3 = 4\text{mm/s}$, тоест броят на измерванията е n=3.

$$RMS = \sqrt{\frac{x_1^2+x_{2+}^2x_3^2}{3}} = \sqrt{\frac{2_1^2+3_{2+}^24_3^2}{3}} = \sqrt{\frac{4+9+16}{3}} = \sqrt{\frac{29}{3}} = \sqrt{9{,}67} = 3{,}11mm/s \quad (5)$$

Процент намаление на престоя след внедряване на ИИ

Показва ефективността на системата за предиктивна поддръжка. Преди внедряване на ИИ престоят е бил 120 часа годишно, а след внедряването – 45 часа. Тоест престоят е намален с 62.5%.

$$A = \frac{T_{before}-T_{after}}{T_{before}} \times 100\% = \frac{120-45}{120} \times 100\% = \frac{75}{120} \times 100\% = 62{,}5\% \quad (6)$$

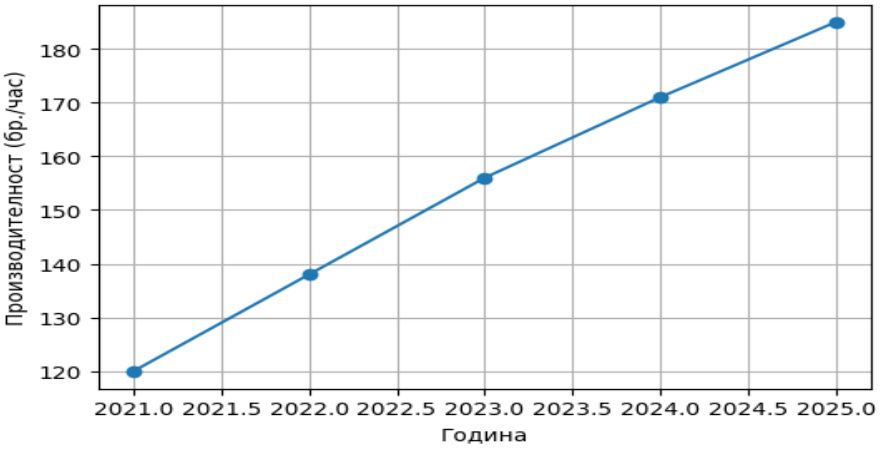
4 Роботизация и интелигентни производствени системи

Роботизацията представлява едно от най-видимите приложения на изкуствения интелект в индустрията. Съвременните роботи са способни не само да изпълняват предварително зададени операции, но и да се адаптират към различни производствени условия. Това ги прави значително по-гъвкави в сравнение с традиционните автоматизирани системи. Интелигентните роботи използват технологии за компютърно зрение и машинно обучение, за да разпознават обекти и да взаимодействат с околната среда. Разпознаването на обекти чрез невронни мрежи и трансфер на знания е разгледано в изследвания с военно предназначение [2, 3]. Взаимодействието между хора и машини при управление на физически обекти е предмет на [18]. Те могат да работят съвместно с хората, като изпълняват повтарящи се, тежки или опасни задачи. Това подобрява условията на труд и намалява риска от трудови злополуки. Внедряването на роботизирани системи позволява на предприятията да увеличат производствения капацитет и да поддържат високо качество на продукцията. Освен това се създават възможности за по-бързо адаптиране към

изискванията на пазара и индивидуалните нужди на клиентите. Развитието на колаборативните роботи представлява важна стъпка в индустриалната автоматизация. Тези роботи са проектирани да работят в непосредствена близост до хората без необходимост от сложни защитни съоръжения. Благодарение на усъвършенствани сензори и алгоритми те могат безопасно да взаимодействат с операторите и да подпомагат изпълнението на различни производствени дейности. Нарастващото използване на автономни роботизирани системи променя и организацията на производствените процеси. Роботите вече могат самостоятелно да транспортират материали, да извършват инспекции и да координират действията си с други машини. Това води до създаването на по-интегрирани и ефективни производствени среди, в които човешкият фактор е насочен към по-сложни и творчески задачи. Таблицата 1 и фиг. 3 показват ефекта от внедряването на роботизирана система.

Таблица 1. Ефект от внедряването на роботизирана система

Показател	Преди роботизация	След роботизация	Промяна
Производителност (бр./час)	120	185	+54.2%
Процент дефектни изделия (%)	4.8	1.7	-64.6%
Средно време за цикъл (сек.)	30	19	-36.7%
Производствени престои (часа/месец)	22	9	-59.1%
Трудови инциденти (бр./година)	6	2	-66.7%
Използваемост на оборудването (%)	78	92	+17.9%



Фиг. 3. Производителност след внедряването на роботи

5 Контрол на качеството чрез изкуствен интелект

Осигуряването на високо качество на продукцията е сред основните цели на всяко индустриално предприятие. Изкуственият интелект предлага нови възможности за автоматизиран контрол на качеството чрез използване на системи за машинно зрение и анализ на изображения. Интелигентните системи могат да откриват дефекти и отклонения в продукцията с висока точност и скорост. За разлика от човешкия контрол, те работят

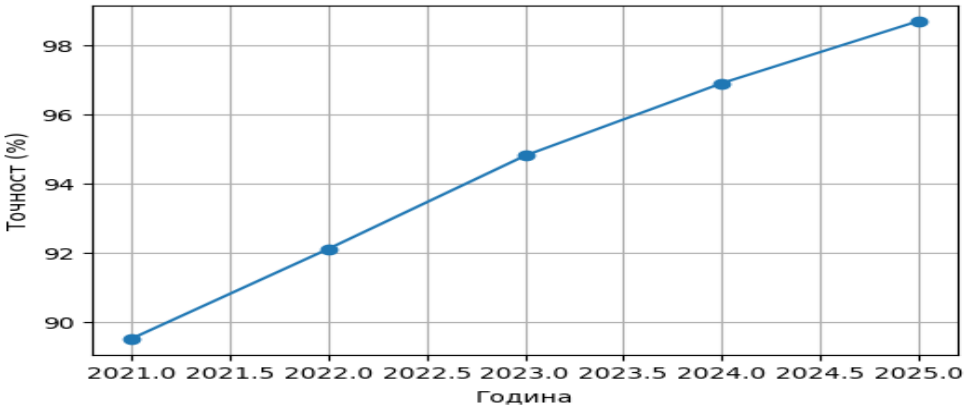
непрекъснато и не са подложени на умора или субективни оценки. Това води до по-надеждни резултати и намаляване на производствените загуби. Методологията за изследване на логистични системи, измерването на производствени фактори и организацията на логистични процеси са разгледани в [8, 9, 11]. ERP системите и експертният анализ на логистичното управление и качеството са разгледани в [15, 19]. Допълнително, събраните данни могат да бъдат използвани за анализ на причините за възникване на дефекти. По този начин предприятията могат да предприемат коригиращи действия и да подобрят цялостния производствен процес. Системите за контрол на качеството, базирани на изкуствен интелект, могат да обработват хиляди изображения за секунди и да откриват дефекти, които трудно биха били забелязани от човешкото око. Това е особено важно в отрасли като автомобилостроенето, електрониката и фармацевтичната индустрия, където дори минимални отклонения могат да доведат до сериозни последствия. Натрупаните данни от процесите по контрол на качеството предоставят ценна информация за подобряване на производствените технологии. Обработката и анализът на данни в информационни системи чрез динамични масиви в MS Excel са разгледани в [17]. Таблица 2 и таблица 3 показват контрола на качеството, а фиг. 4 и фиг. 5 показват резултатите от тях.

Таблица 2. Сравнение на показателите за контрол на качеството

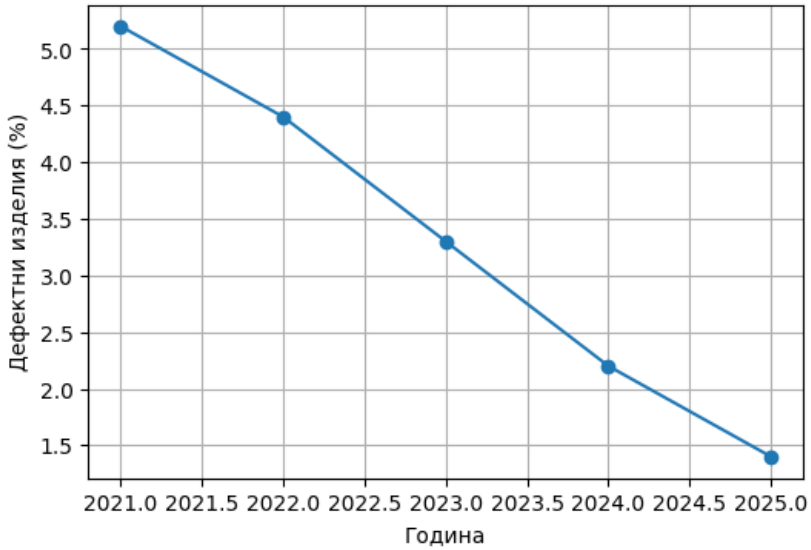
Показател	Преди внедряване на AI	След внедряване на AI	Промяна
Точност при откриване на дефекти (%)	89.5	98.7	+10.3%
Дефектни изделия (%)	5.2	1.4	-73.1%
Време за инспекция на изделие (сек.)	15	4	-73.3%
Проверени изделия на час	240	900	+275.0%
Фалшиви сигнали (%)	7.5	2.1	-72.0%
Производствени рекламации (бр./месец)	18	6	-66.7%

Таблица 3. Динамика на показателите за качество след внедряване на система за изкуствен интелект

Година	Точност на AI системата (%)	Дефектни изделия (%)	Рекламации (бр./месец)
2021	89.5	5.2	18
2022	92.1	4.4	15
2023	94.8	3.3	11
2024	96.9	2.2	8
2025	98.7	1.4	6



Фиг. 4. Точност на AI системата за контрол на качеството



Фиг. 5. Процент дефектни изделия по години

6 Предизвикателства и перспективи пред внедряването на ИИ

Въпреки многобройните предимства, внедряването на изкуствен интелект в индустриалната автоматизация е свързано с редица предизвикателства. Сред тях са високите първоначални инвестиции, необходимостта от специализирани кадри и сложността на интеграцията със съществуващите производствени системи. Друг важен аспект е свързан със защитата на данните и киберсигурността. С увеличаването на броя на свързаните устройства и автоматизирани системи нараства и рискът от кибератаки [16]. Поради тази причина предприятията трябва да инвестират в надеждни механизми за защита на информацията. Хардуерни реализации на генератори на псевдослучайни последователности за криптографски приложения са представени в [4, 13]. В бъдеще се очаква ролята на изкуствения интелект в индустрията да продължи да нараства. Развитието на технологиите ще позволи създаването на още по-интелигентни и автономни производствени системи, които ще повишат ефективността и устойчивостта на индустриалните предприятия. Едно от основните предизвикателства е необходимостта от квалифицирани специалисти, които да разработват, внедряват и поддържат интелигентните

системи. Недостигът на кадри в областта на изкуствения интелект и анализа на данни затруднява много предприятия при осъществяването на дигиталната трансформация. Това налага инвестиции в обучение и повишаване на квалификацията на персонала. Съществен въпрос е и етичният аспект на автоматизацията. Разширяването на използването на интелигентни технологии поражда дискусии относно бъдещето на заетостта и ролята на човека в производствения процес. Въпреки тези опасения преобладава мнението, че изкуственият интелект няма да замени напълно човешкия труд, а ще промени неговия характер, като създаде нови възможности за професионално развитие и специализация.

7 Заключение

Изкуственият интелект се утвърждава като ключов фактор за развитието на съвременната индустриална автоматизация. Неговото приложение обхваща широк спектър от дейности – от оптимизация на производството и предиктивна поддръжка до роботизация и контрол на качеството. Благодарение на способността си да анализира големи обеми информация и да взема решения в реално време, ИИ значително подобрява ефективността на производствените процеси. Въпреки съществуващите предизвикателства, перспективите пред внедряването на изкуствен интелект са изключително благоприятни. С развитието на технологиите предприятията ще разполагат с все по-мощни инструменти за автоматизация и управление. Това ще доведе до изграждането на по-гъвкави, интелигентни и конкурентоспособни индустриални системи, които ще определят бъдещето на производството.

ЛИТЕРАТУРА:

[1] Беджев Б. Й., Николов Н. Р., Цанков Ц. С. Обучаема изкуствена имунна система използваща „добри“ пътища за синтез на сигнали с оптимални автокорелационни свойства. MATTEX 2018, т. 2, част 2, Шумен, 2018, с. 3–11. ISSN 1314-3921.

[2] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[3] Манов Л. Е. Съвременни технологии с изкуствен интелект за разпознаване на обекти с военно предназначение в оптични изображения: Компютърен експеримент с невронни мрежи в MATLAB. DefTech 2025, 2025, с. 714–722. ISSN 2815-4282.

[4] Николов Н. Р., Цанков Ц. С. Хардуерна реализация на генератор на псевдослучайни последователности, описван с полином от 1024 степен, и програмно управление на обратните връзки. Научна сесия 2010, сборник научни трудове, част I, НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, Шумен, 2011, с. 159–163. ISSN 1313-7433.

[5] Николов Н. Р., Беджев Б. Й., Цанков Ц. С. Приложение на изкуствените имунни системи при синтеза на сигнали с оптимални автокорелационни свойства. MATTEX 2016, т. 2, Шумен, 2016, с. 23–29. ISSN 1314-3921.

[6] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, сборник доклади, т. 1, Шумен, 2011, с. 229–232. ISSN 1314-3921.

[7] 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.

[8] Kodzheykova, V. Methodology of experimental-statistical research of logistics systems. Proceedings of the Scientific Conference with International Participation MATTEH 2022, Vol. 2, Shumen, 2022, pp. 296–301, ISSN 1314-3921.

[9] Kodzheykova, V. Measurement of factors to provide medium serial technological production. Proceedings of the Scientific Conference with International Participation MATTEH 2022, Vol. 2, Shumen, 2022, pp. 302–308, ISSN 1314-3921.

[10] Kasula B., AI-Enabled Digital Twins for Industrial Automation: Enhancing Predictive Maintenance and Operational Efficiency, 2024, American Journal of AI & Innovation, Vol. 6, No. 6, ISSN 3066-8934, pp. 1–12.

[11] Kazakov St. Resources and Organization of Processes in Logistics Engineering. SocioBrains, 2020, pp. 54–59. ISSN 2367-5721.

[12] Bala A., Rashid R. Z. J. A., Ismail I., Oliva D., Muhammad N., Sait S. M., Al-Utaibi K. A., Memon K. A., Artificial Intelligence and Edge Computing for Machine Maintenance – Review, 2024, Artificial Intelligence Review, Vol. 57, Article 119, Springer Nature, ISSN 0269-2821.

[13] Iliev M. P., Nikolov N. R., Tsankov T. Sv. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Electrotechnica & Electronica, Vol. 46, No. 7–8, 2011, pp. 29–33. ISSN 0861-4717.

[14] Fernández-Peláez F., Etxegarai M., Moreno V., Echeverria L., Campins G., López C., Rojo R., González V., Predictive Maintenance in the Food Industry: A Case Study Using Vibration Sensors and Machine Learning Techniques, 2024, Artificial Intelligence Research and Development, IOS Press, DOI: 10.3233/FAIA240407.

[15] Kazakov St. ERP Systems in Logistics and Transportation. SocioBrains, 2020, pp. 49–53. ISSN 2367-5721.

[16] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144. ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[17] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.

[18] Tsvetanova, P. T., Stoyanova, V. T. Research of Systems for Interaction between People and Machines in the Management of Physical Objects. Proceedings of the International Scientific Conference “Defense Technology”, 2019. ISSN 2367-7902.

[19] Yankova-Yordanova, Y., Kodzheykova, V. Expert approach for analysing a logistics control system and quality management in the conditions of small and medium serial production. Journal Scientific and Applied Research, Vol. 15, 2019, pp. 37–47, ISSN 1314-6289.

RESEARCH ON AUTHENTICATION MECHANISMS IN MODERN COMMUNICATION SYSTEMS*

EKATERINA M. HRISTOVA, STEFANIYA M. CHERVENKOVA

ABSTRACT: *Authentication is a fundamental process in modern communication systems that guarantees the identity of users, devices and services. With the development of digital technologies and increasing cyber threats, various authentication mechanisms have emerged that provide data protection and prevent unauthorized access. This report examines the main authentication methods, their working principles, advantages and disadvantages, as well as their role in the security of communication systems.*

KEYWORDS: *communication, unauthorized access, cyber threats*

DOI: https://doi.org/10.46687/MT26EMH

ИЗСЛЕДВАНЕ НА МЕХАНИЗМИТЕ ЗА УДОСТОВЕРЯВАНЕ В СЪВРЕМЕННИТЕ КОМУНИКАЦИОННИ СИСТЕМИ

ЕКАТЕРИНА М. ХРИСТОВА, СТЕФАНИЯ М. ЧЕРВЕНКОВА

АБСТРАКТ: *Удостоверяването представлява основен процес в съвременните комуникационни системи, който гарантира идентичността на потребителите, устройствата и услугите. С развитието на цифровите технологии и нарастващите киберзаплахи се появяват различни механизми за удостоверяване, които осигуряват защита на данните и предотвратяват неоторизиран достъп. Настоящият доклад разглежда основните методи за удостоверяване, техните принципи на работа, предимства и недостатъци, както и ролята им за сигурността на комуникационните системи.*

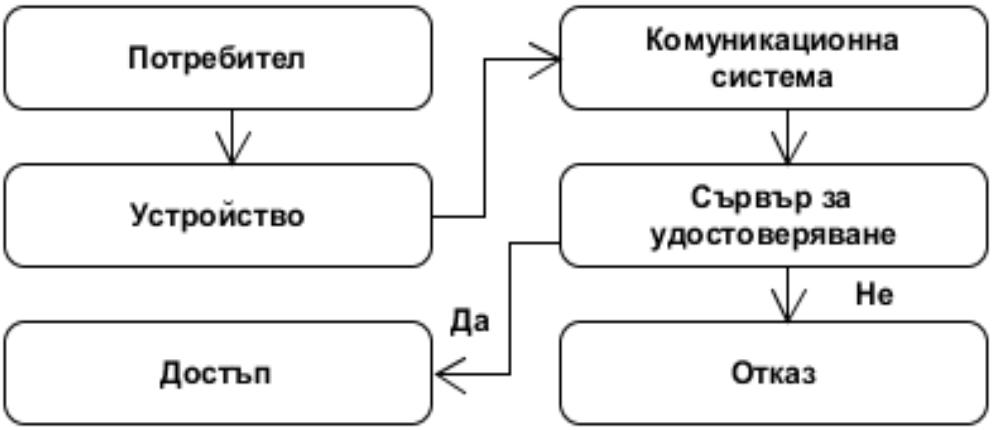
1 Въведение

Съвременните комуникационни системи са неразделна част от ежедневието на хората и организациите. Интернет, мобилните мрежи, облачните услуги и корпоративните информационни системи изискват надеждни механизми за защита на потребителските данни. Един от най-важните елементи на информационната сигурност е удостоверяването, чрез което се потвърждава самоличността на даден потребител или устройство преди предоставянето на достъп до определени ресурси. Ефективните механизми за удостоверяване намаляват риска от злоупотреби, кражба на данни и неоторизиран достъп до чувствителна информация. Съвременните комуникационни системи се развиват в посока на все по-висока взаимосвързаност между устройства, услуги и потребители. Това води до увеличаване на повърхността за атаки и съответно до нужда от по-сложни механизми за защита. Удостоверяването вече не се разглежда само като входна стъпка към система, а като динамичен процес, който може да се прилага многократно по време на сесията. Допълнително значение придобива необходимостта от защита на разпределени архитектури, където потребителят може да използва множество устройства едновременно. Това изисква синхронизация на идентичността между различни платформи. В този контекст удостоверяването трябва да бъде едновременно надеждно и адаптивно към различни среди.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

По-широкият контекст включва съвременните киберзаплахи [13], сигурността на мултимедийни мрежи в автоматизирани системи [11] и защитата на мобилни устройства [14].

Друг важен аспект е интеграцията на облачни услуги, при които данните не се съхраняват локално, а в разпределена инфраструктура. Това променя начина, по който се реализира контролът на достъпа. Системите трябва да удостоверяват не само потребителя, но и устройството и контекста на заявката. В допълнение се наблюдава тенденция към автоматизация на процесите по сигурност. Удостоверяването се свързва с анализ на поведение, мрежов трафик и контекстуални фактори. Това позволява по-ранно откриване на аномалии и предотвратяване на потенциални инциденти. Анализът на трафик чрез Wireshark е разгледан в [8], а обработката на данни при пакетна комутация е предмет на [10]. Отделни изследвания разглеждат Wi-Fi протоколите, защитата при мрежово кодиране и уязвимостите на Zigbee [6, 7, 9]. На фиг. 1 е показан общия процес на удостоверяване.



Фиг. 1. Общ процес на удостоверяване

2 Същност и значение на удостоверяването

Удостоверяването представлява процес на проверка на идентичността на даден субект в комуникационната система. То е първата стъпка към осигуряване на сигурен достъп до информационни ресурси. Основната му цел е да гарантира, че потребителят или устройството, което заявява определена самоличност, действително е това, за което се представя. Без надеждно удостоверяване всички останали механизми за сигурност биха били неефективни, тъй като системата не би могла да разграничи легитимните потребители от потенциалните нападатели. Удостоверяването е критичен компонент на информационната сигурност, който осигурява първична защита срещу неоторизиран достъп. То функционира като филтър, който разделя легитимните потребители от потенциалните заплахи. Без него всички последващи механизми като авторизация и криптиране биха били неефективни. В съвременните системи удостоверяването се разглежда като многоетапен процес, а не като еднократна проверка. Това позволява динамична оценка на риска по време на активна сесия. Например, промяна в местоположението или устройството може да изисква повторна проверка. Ролята на удостоверяване е показана в таблица 1.

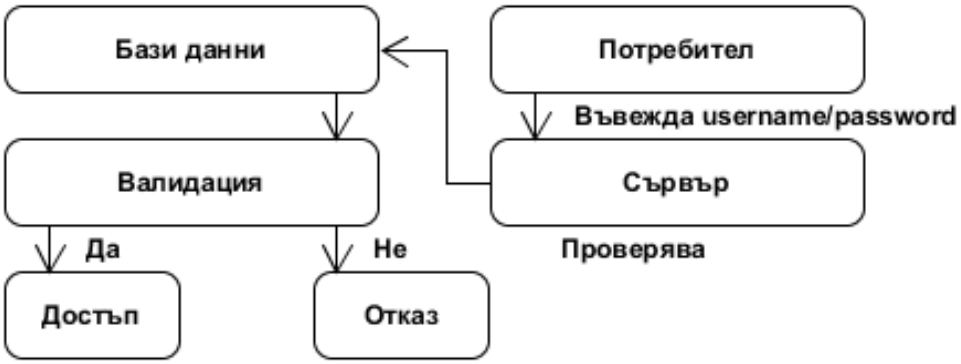
Таблица 1. Роля на удостоверяването в комуникационните системи

Аспект	Описание
Цел	Проверка на самоличността на потребител или устройство
Основна функция	Предотвратяване на неоторизиран достъп
Значение	Осигурява сигурност на информационните ресурси
Ползи	Защита на данни, контрол на достъпа, проследимост
Рискове при липса	Кражба на данни, злоупотреби, пробиви в сигурността

Съществено значение има и мащабируемостта на механизмите за удостоверяване. В големи системи с милиони потребители процесът трябва да бъде бърз и ефективен. Това налага използването на оптимизирани протоколи и разпределени архитектури. Освен това удостоверяването играе роля и в одита и проследимостта на действията в системата. Чрез него се създават логове, които позволяват анализ на инциденти и откриване на злоупотреби. Това е важно за корпоративната и регулаторната сигурност. Удостоверяването се допълва от защита на комуникационния канал. Приложението на TLS и SSL, изграждането на VPN и закъснението при криптиране на глас през VPN са разгледани в [2, 3, 5]. Нелинейните функции за защита на информацията и генераторите на псевдослучайни последователности са предмет на [1, 12].

3 Удостоверяване чрез пароли

Най-разпространеният механизъм за удостоверяване е използването на потребителско име и парола. Този метод се базира на информация, която потребителят знае и предоставя при влизане в системата. Въпреки широкото му приложение, удостоверяването чрез пароли има редица недостатъци. Слабите или лесно отгатваеми пароли могат да бъдат компрометирани чрез атаки като груба сила, фишинг или изтичане на данни. Поради тази причина организациите все по-често прилагат политики за създаване на сложни пароли и тяхната редовна подмяна. Паролите остават най-широко използваният метод поради своята простота и ниска цена на внедряване. Те не изискват допълнителен хардуер и са лесни за интеграция в различни системи. Това ги прави предпочитани за масови услуги и приложения. Съществуват различни техники за съхранение на пароли, като хеширане и използване на сол. Те целят да предотвратят директното разкриване на оригиналните стойности при изтичане на база данни. Въпреки това, слаби алгоритми или неправилна имплементация могат да компрометират сигурността. Основен проблем при паролите е човешкият фактор. Потребителите често избират лесни за запомняне комбинации, които са уязвими на атаки. Това създава необходимост от обучение и налагане на политики за сигурност. С развитието на автоматизирани атаки се увеличава значението на допълнителни защитни механизми. Те включват ограничаване на опитите за вход, CAPTCHA системи и мониторинг на подозрително поведение. Така паролите се използват като част от по-широка защитна стратегия. На фиг. 2 е показано удостоверяването чрез пароли.



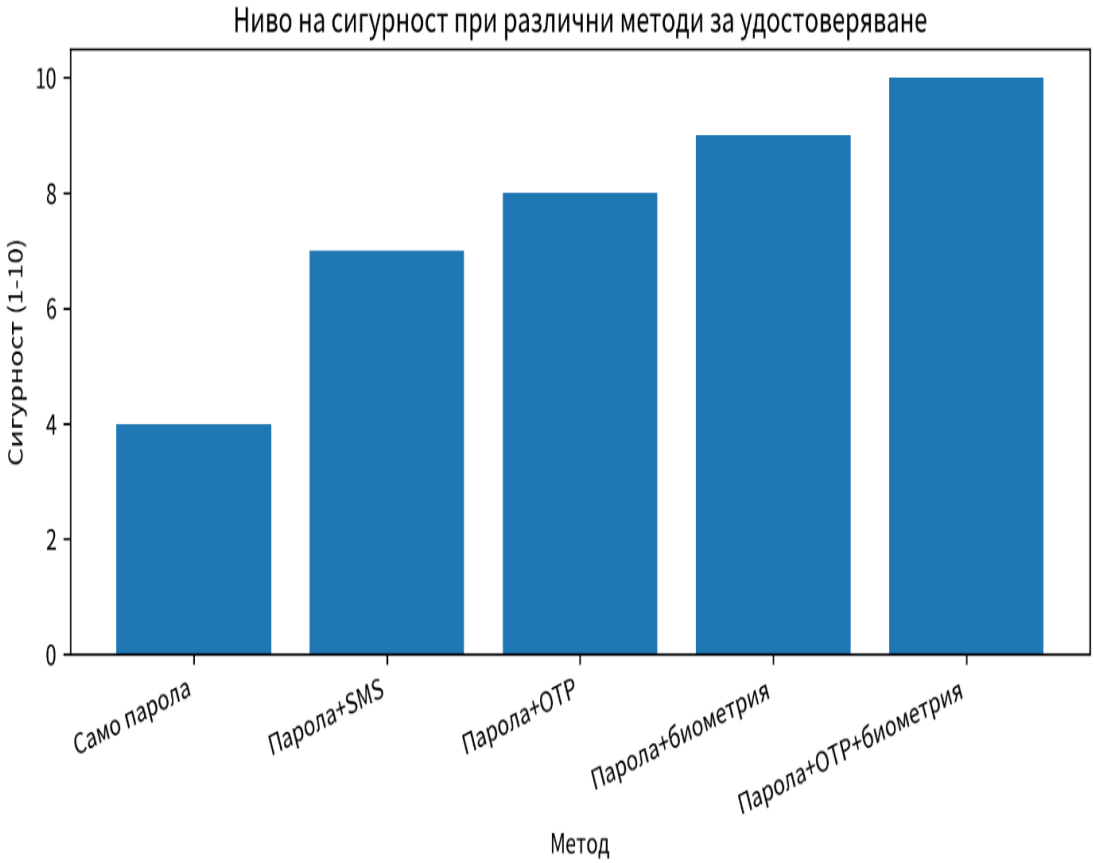
Фиг. 2. Удостоверяване чрез пароли

4 Многофакторно удостоверяване

Многофакторното удостоверяване представлява комбинация от два или повече независими фактора за потвърждаване на самоличността. Обикновено тези фактори включват нещо, което потребителят знае (парола), нещо, което притежава (смартфон, токен или смарт карта) и нещо, което е (биометрична характеристика). Използването на няколко фактора значително повишава нивото на сигурност, тъй като компрометирането на един фактор не е достатъчно за получаване на достъп. Поради това многофакторното удостоверяване се превръща в стандарт за защита на критични системи и онлайн услуги. Многофакторното удостоверяване значително повишава сигурността чрез комбиниране на различни категории фактори. Това намалява риска от компрометиране на акаунти дори при изтичане на парола. Системата изисква независими доказателства за идентичност. Един от важните аспекти е балансът между сигурност и удобство. Колкото повече фактори се добавят, толкова по-сигурна става системата, но и по-сложна за използване. Това може да повлияе на потребителското изживяване. Съвременните решения използват мобилни приложения за генериране на еднократни кодове. Това елиминира нуждата от физически токени и улеснява внедряването. В същото време се запазва високо ниво на защита. Многофакторното удостоверяване често се комбинира с адаптивни системи. Те анализират риска в реално време и прилагат допълнителни проверки само при съмнителни действия. Това оптимизира процеса и намалява излишното натоварване на потребителя. В таблица 2 и фиг. 3 е извършено сравнение на методи за удостоверяване.

Таблица 2. Сравнение на методи за удостоверяване

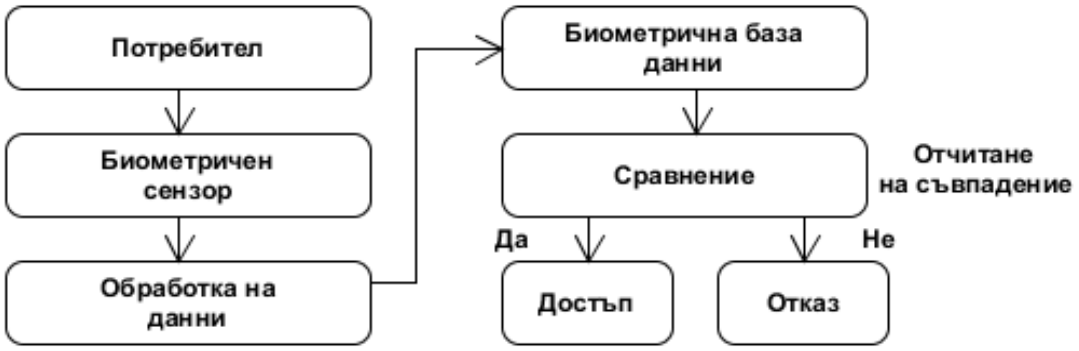
Метод	Брой фактори	Ниво на сигурност (1–10)	Време за вход (сек.)
Само парола	1	4	5
Парола + SMS код	2	7	12
Парола + OTP приложение	2	8	10
Парола + биометрия	2	9	8
Парола + OTP + биометрия	3	10	15



Фиг. 3. Ниво на сигурност при различни методи за удостоверяване

5 Биометрични механизми за удостоверяване

Биометричното удостоверяване използва уникални физически или поведенчески характеристики на човека. Най-често се прилагат пръстови отпечатъци, лицево разпознаване, сканиране на ириса и разпознаване на гласа. Основното предимство на този подход е удобството за потребителите, тъй като не е необходимо да запомнят сложни пароли. Въпреки това биометричните данни изискват специална защита, защото при компрометиране те не могат лесно да бъдат променени, както е възможно при паролите. Биометричните системи се базират на уникалността на човешките характеристики, което ги прави трудно подменяеми. Те осигуряват висока степен на сигурност при правилна имплементация. Това ги прави подходящи за критични приложения. Развитието на сензорни технологии значително подобрява точността на биометричните системи. Камери с висока резолюция и усъвършенствани алгоритми за разпознаване намаляват процента на грешки. Това увеличава тяхната надеждност. Въпреки това съществуват рискове, свързани със защита на биометричните данни. При компрометиране те не могат да бъдат променени, за разлика от паролите. Това изисква специални методи за криптиране и съхранение. Допълнително предизвикателство е възможността за фалшификация чрез сложни атаки като deepfake технологии. Това налага постоянно усъвършенстване на алгоритмите за разпознаване. Биометрията се развива в посока на многослойна проверка. На фиг. 4 е показано биометрично удостоверяване.



Фиг. 4. Биометрично удостоверяване

6 Съвременни тенденции и предизвикателства

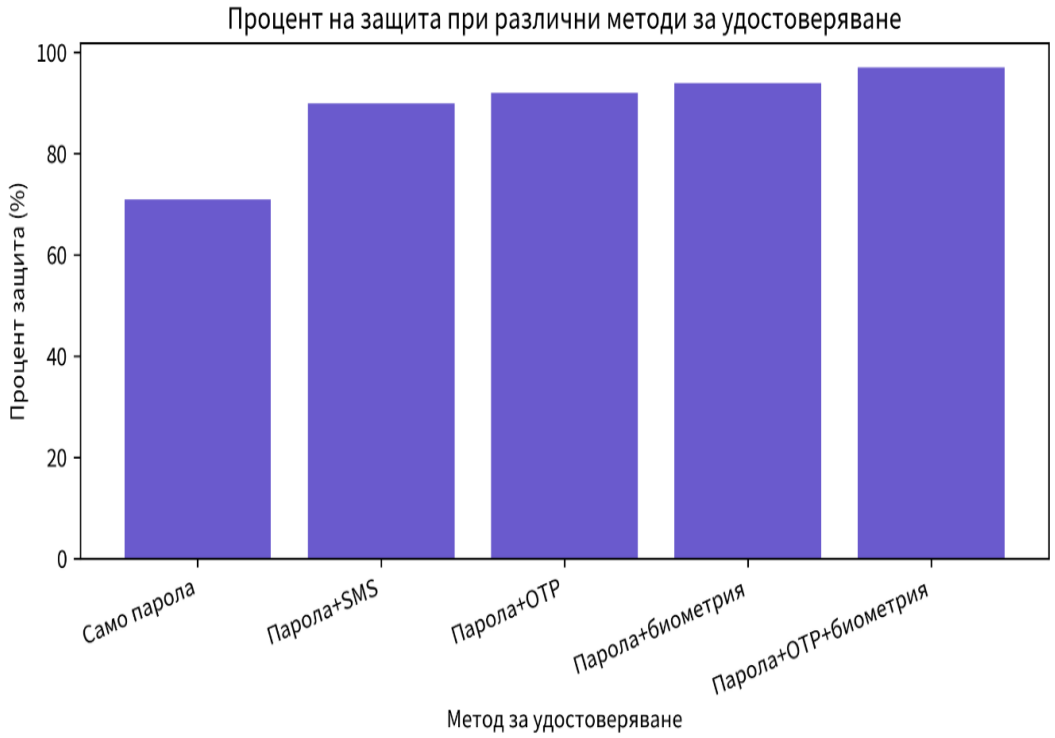
Развитието на комуникационните технологии води до появата на нови подходи за удостоверяване. Сред тях са удостоверяването без парола, използването на криптографски ключове, адаптивното удостоверяване и системите, базирани на изкуствен интелект. Тези технологии анализират поведението на потребителите и контекста на достъпа, за да определят нивото на риск и необходимите мерки за сигурност. В същото време организациите се сблъскват с предизвикателства като защита на личните данни, сложност на внедряването и необходимост от баланс между сигурност и удобство за потребителите. Една от основните тенденции е преминаването към удостоверяване без пароли. То използва криптографски ключове и хардуерни устройства за идентификация. Това значително намалява риска от фишинг атаки. Изкуственият интелект играе все по-голяма роля в анализа на потребителското поведение. Системите могат да откриват отклонения от нормалните модели на достъп. Това позволява проактивна защита. Друга тенденция е използването на децентрализирани идентичности. Те дават на потребителя контрол върху личните му данни и намаляват зависимостта от централизирани бази. Това повишава прозрачността и сигурността. Основните предизвикателства остават свързани със сложността на интеграцията и защитата на личните данни. Организациите трябва да балансират между регулаторни изисквания и технически възможности. Това прави областта динамична и бързо развиваща се. Удостоверяването не изчерпва защитата на комуникационната система. Успешно идентифициран потребител също може да предава съдържание, което изисква допълнителен анализ. Отделно направление е откриването на скрита информация чрез визуална стеганализа [4]. То разглежда съдържанието на обменяните данни и допълва проверката на идентичността, без да представлява самостоятелен механизъм за удостоверяване.

КАЗУС: Прилагане на многофакторно удостоверяване в корпоративна среда

С нарастването на киберзаплахите много организации внедряват многофакторно удостоверяване (MFA), за да повишат сигурността на своите информационни системи. За целите на настоящото изследване е разгледан примерен сценарий във фирма с около 500 служители, която използва различни методи за удостоверяване при достъп до вътрешните си ресурси. В рамките на един месец са наблюдавани опити за неоторизиран достъп до системата. Анализът има за цел да покаже как различните механизми за удостоверяване влияят върху нивото на защита и способността на системата да предотвратява успешни атаки.

Таблица 3. Ефективност на различни методи за удостоверяване

Метод за удостоверяване	Брой потребители	Опити за атака	Успешно блокирани атаки	Процент защита (%)
Само парола	120	45	32	71
Парола + SMS код	110	40	36	90
Парола + OTP приложение	100	38	35	92
Парола + биометрия	90	35	33	94
Парола + OTP + биометрия	80	30	29	97



Фиг. 5. Процент на защита при различни методи за удостоверяване в корпоративна среда

От представените данни в таблица 3 и фиг. 5 се наблюдава ясна тенденция за повишаване на сигурността при използване на повече от един фактор за удостоверяване. Докато системите, разчитащи единствено на пароли, постигат ниво на защита от 71%, комбинирането на парола с допълнителни фактори като еднократни кодове и биометрични данни значително намалява риска от неоторизиран достъп. Най-висока ефективност показва комбинацията от парола, OTP приложение и биометрична идентификация, при която процентът на защита достига 97%. Резултатите потвърждават, че многофакторното удостоверяване е едно от най-ефективните средства за защита на съвременните комуникационни системи и е препоръчително за организации, които обработват чувствителна информация.

7 Заключение

Механизмите за удостоверяване играят ключова роля в защитата на съвременните комуникационни системи. Те осигуряват контрол върху достъпа до информация и намаляват риска от неоторизирани действия. Въпреки че традиционното удостоверяване чрез пароли все още е широко използвано, съвременните тенденции са насочени към многофакторни, биометрични и криптографски решения. Нарастващите изисквания за сигурност налагат непрекъснато усъвършенстване на тези механизми, за да се гарантира надеждна защита на данните и цифровите комуникации в бъдеще. Удостоверяването е фундаментален елемент от сигурността на съвременните комуникационни системи. То осигурява надежден контрол на достъпа и защита на чувствителна информация. Без него цифровата инфраструктура би била изключително уязвима. Различните методи за удостоверяване имат своите силни и слаби страни. Паролите са лесни за използване, но уязвими, докато биометричните и многофакторните системи предлагат по-висока сигурност. Комбинацията от подходи е най-ефективното решение. Бъдещето на удостоверяването е свързано с автоматизация, адаптивност и използване на изкуствен интелект. Системите ще стават все по-интелигентни и контекстуални. Това ще позволи по-добра защита срещу сложни киберзаплахи. В заключение може да се каже, че развитието на механизмите за удостоверяване е ключово за устойчивостта на дигиталното общество. Постоянните иновации в тази област ще определят нивото на сигурност в бъдещите комуникационни системи.

ЛИТЕРАТУРА:

[1] Цанков Ц. С. Приложения на нелинейните функции за защита на информацията в комуникационните системи. Университетско издателство „Епископ К. Преславски“, Шумен, 2018, 204 с., ISBN 978-619-201-212-0.

[2] Denev D., Tsankov Ts., Use in Internet of Protocols Transport Layer Security and its Now-Deprecated Predecessor Secure Sockets Layer, 2018, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 94-101.

[3] Denev D., Tsankov Ts., Development of a Virtual Private Network in Computer Networks and Communication Environments, 2020, International scientific refereed online journal SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71, ISSN 2367-5721, pp. 11-19.

[4] Terziev H., Denev D., Analysis of the Possibilities for Discovery of Information in the Communication Information Systems Through the use of Visual Steganalysis, 2020, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 229-233.

[5] Denev D., Analytical Study of the Delay Introduced as a Result of Encryption/Decryption of Voice Transmitted over a VPN Networks, 2021, Journal scientific and applied research, vol. 20, International Journal, ISSN 1314-6289, pp. 73-77.

[6] Denev D., Research of Wi-Fi and its Protocols, 2022, Conference with international participation MATTEH 2022, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 95-101.

[7] 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.

[8] 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.

[9] Denev D., Dimitrova E., Security and Vulnerabilities in Zigbee Technology, 2024, Annual of Konstantin Preslavski University of Shumen, Vol. XIV E, Faculty of technical sciences, ISSN 1314-8818, pp. 92-97.

[10] Denev D., Tsankov Ts., A Novel Approach in Implementation and Amelioration of Data Processing in Packet Switching Technology, 2025, 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies ICEST, Ohrid, North Macedonia, 26-28 June, ISBN 979-8-3315-2655-9, ISSN: 2603-3267, DOI: 10.1109/ICEST66328.2025.11098340, pp. 1-6.

[11] Denev D., Petrov I., Cybersecurity in Multimedia Networks of Automated Systems, 2025, Annual of Konstantin Preslavski University of Shumen, Vol. XV E, Faculty of technical sciences, ISSN 1314-8818, pp. 61-73

[12] Iliev M. P., Nikolov N. R., Tsankov T. Sv. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Electrotechnica & Electronica, Vol. 46, No. 7–8, 2011, pp. 29–33. ISSN 0861-4717.

[13] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144. ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[14] Stoyanova, V. Problems with Information Security on Mobile Devices. Industry 4.0, 2019, p. 200. https://stumejournals.com/journals/i4/2019/4/200

MODEL OF A WEB-BASED INFORMATION SYSTEM "DOKTORANT"*

YOVKO M. HRISTOV, VALENTIN T. ATANASOV

ABSTRACT: *The paper presents a model of a web-based information system for centralized management and monitoring of the administrative process for the PhD students. The model comprises a three-tier application architecture, a normalized relational data model and role-based access control. The main functional components cover users, roles and permissions, doctoral student profiles, document management, reports, system settings, help content and audit logging. A prototype, implemented using PHP and MariaDB, is used to validate the proposed model. Particular attention is paid to authentication, session management, CSRF protection, prepared database queries, password hashing, file integrity verification and traceability of user actions. The experimental implementation confirms the applicability of the model as a basis for a secure, maintainable and extensible information system in a university environment.*

KEYWORDS: *web-based information system, doctoral education, RBAC, information security, relational database, audit log*

DOI: https://doi.org/10.46687/MT26YMH

МОДЕЛ НА УЕБ-БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА „ДОКТОРАНТ“

ЙОВКО М. ХРИСТОВ, ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *В статията е представен модел на уеб-базирана информационна система за централизирано управление и мониторинг на административните процеси, свързани с докторантите. Моделът включва трислойна архитектура на приложението, нормализиран релационен модел на данните и ролево базиран контрол на достъпа. Основните функционални компоненти обхващат управление на потребители, роли и права за достъп, профили на докторанти, управление на документи, справки и отчети, системни настройки, помощно съдържание и регистриране на потребителските действия (audit logging). За валидиране на предложения модел е разработен прототип, реализиран с използване на PHP и MariaDB. Особено внимание е отделено на механизмите за автентикация, управление на потребителските сесии, защита срещу CSRF атаки, използване на подготвени заявки към базата данни, хеширане на пароли, проверка на целостта на файловете и проследимост на действията на потребителите. Резултатите от експерименталната реализация потвърждават приложимостта на предложения модел като основа за изграждане на сигурна, лесна за поддръжка и разширяема информационна система в университетска среда.*

1 Въведение

Цифровизацията на административните и академичните процеси във висшите училища поставя необходимост от централизирано, надеждно и контролируемо управление на информацията. Докторантското обучение е процес, в който участват докторанти, научни ръководители и административни звена и се създава значителен обем структурирани данни и електронни документи. Използването на несвързани електронни таблици, локални файлови архиви и хартиени документи затруднява актуализирането на информацията,

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

проследяването на промените и прилагането на единна политика за достъп, както и създава предпоставки за допускане на грешки. Дигитализацията и предизвикателствата пред сигурността в електронната администрация са разгледани в [7].

Целта на настоящата публикация е да представи модел на WEB базирана информационна система „Докторант“, предназначена за централизирано управление и следене на данните и документите, свързани с докторантското обучение. Моделът е разработен и практически апробиран чрез прототип на системата. При проектирането са поставени изисквания за модулност, разделяне на отговорностите, референтна цялост на данните, контрол на достъпа и проследимост на действията. За оторизация е приложен Role-Based Access Control (RBAC), при който разрешенията се асоциират с роли, а ролите – с потребители, в съответствие с утвърдения модел за ролево управление на достъпа [3].

2 Концептуален и функционален модел

Концептуалният модел обхваща основните обекти „Потребител“, „Роля“, „Разрешение“, „Докторант“, „Документ“, „Системна настройка“, „Помощна статия“ и „Одитен запис“. Централен обект е профилът на докторанта, към който се асоциират предефинира тип данни за обучението, научното направление, докторската програма, научния ръководител, статуса и електронните документи. Потребителският профил може да бъде свързан с профил на докторант, а действията на удостоверените и упълномощени потребители се регистрират в одитния журнал.

В концептуалния модел са дефинирани четири основни роли – администратор, оператор, преподавател и докторант. администраторът управлява потребители, роли, разрешения, настройки и одитна информация; операторът изпълнява административни операции с данните за докторантите; преподавателят работи с информацията за свързаните с него докторанти; докторантът разполага с ограничен достъп до собствения си профил и разрешените документи.

Функционалният модел се изгражда чрез модули за управление на потребители, роли и разрешения, докторанти, електронни документи, справки, помощен център, системни настройки и одитен журнал. В продължение на добрата практика за функционално моделиране на приложения и системи се използват нотациите на езика UML. На фиг. 1 е представена диаграма на случаите на употреба, която описва взаимодействието на основните потребителски роли и техните функционални характеристики чрез които се изгражда информационната система „Докторант“.

Диаграмата описва подхода за разпределението на достъпа и основните операции, достъпни за основните актьори в системата - администратор, оператор, преподавател и докторант.

2.1. Архитектура и модел на данните

Архитектурният модел е трислоен и разделя приложението на слой за представяне, слой на бизнес логиката и слой за достъп до данните. В прототипа това разделение е развито чрез Controller и Service компоненти, като заявките се приемат от контролера, бизнес правилата се изпълняват в сервизния слой, а достъпът до MariaDB се осъществява чрез PDO. Така потребителският интерфейс не взаимодейства директно с базата данни, което

намалява свързаността между компонентите и улеснява поддръжката и бъдещото разширяване. Възможностите на отдалечени клиенти в архитектурата клиент-сървър са разгледани в [2]. На фиг. 2 е представена логическата архитектура на системата, изградена чрез разделяне на слоя за представяне, бизнес логиката и достъпа до данни.

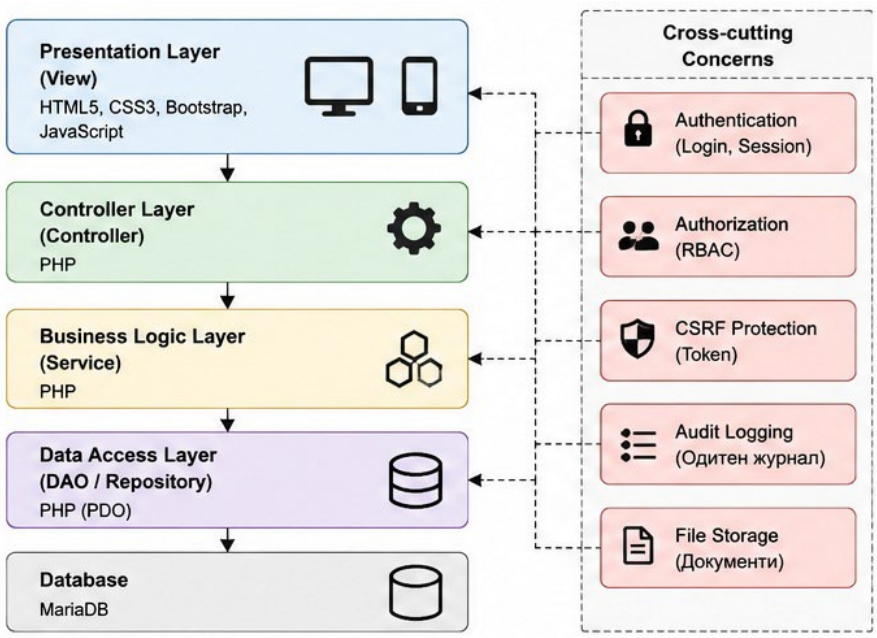


Фигура 1. Случаи на употреба на WEB-/базирана информационна система „Докторант“

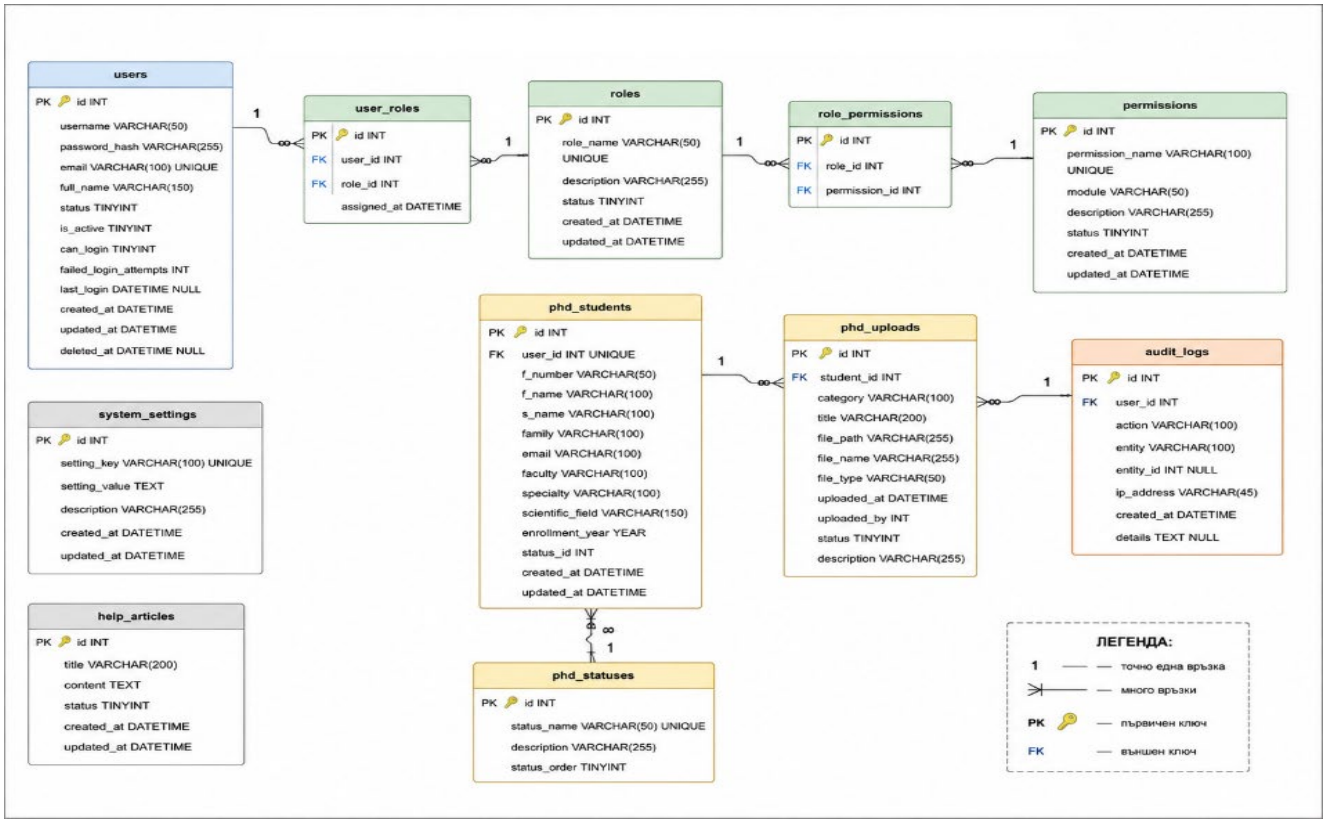
Напречните механизми за сигурност изграждат механизъм контрол на достъпа, защита на заявките и проследимост на действията във всички основни компоненти на системата.

Релационният модел е нормализиран до трета нормална форма (3NF). Основните таблици са users, roles, permissions, user_roles, role_permissions, phd_students, phd_uploads, help_articles, settings и audit_logs. Междинните таблици user_roles и role_permissions реализират отношенията Many-to-Many, необходими за RBAC. Връзката между phd_students и phd_uploads е One-to-Many и позволява към един докторант да се асоциират множество документи. Първичните и външните ключове поддържат референтната цялост, а индексирането на използваните при търсене и свързване полета подпомага

производителността. На фиг. 3 е представена ER диаграмата на модела на данните, която визуализира основните таблици и връзките между тях.



Фигура 2. Логическа архитектура на системата и напречни механизми за сигурност



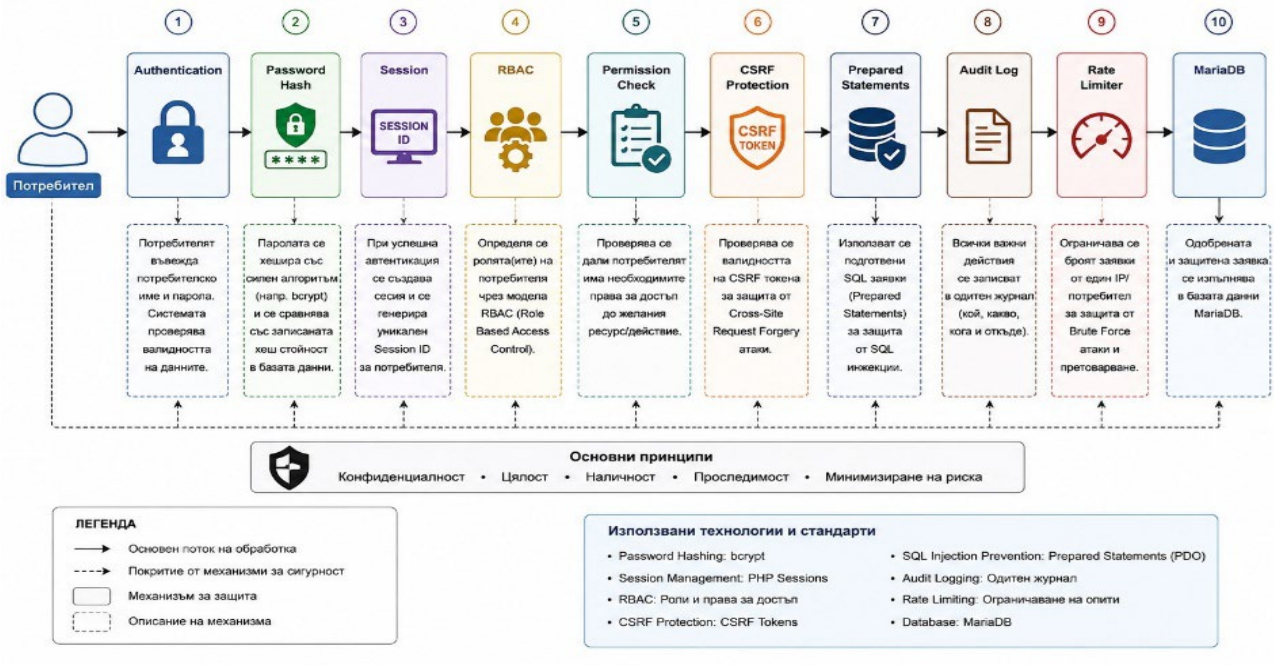
Фигура 3. ER диаграма на модела на данните (основни таблици и връзки)

Структурата обхваща данните за потребителите, ролите и правата за достъп, докторантите и свързаната с тях информация. Моделът осигурява логическа организация и свързаност на данните, необходими за функционирането на системата.

2.2. Модел за информационна сигурност

В предлагания модел защитата на данните е реализирана като последователност от взаимнодопълващи се механизми. Достъпът започва с удостоверяване на потребителя и защитено управление на сесията. Паролите не се съхраняват в открит вид, а чрез специализирания механизъм за еднопосочно хеширане на PHP [4]. След удостоверяване RBAC определя допустимите операции според присвоените роли и разрешения [3]. Проверката се извършва преди изпълнението на защитена функционалност, което прилага принципа на минимално необходимия достъп.

Заявките, променящи състоянието на системата, се защитават чрез CSRF токени, генерирани за потребителската сесия и проверявани на сървъра – подход, препоръчван за приложения без вградена framework защита [5]. За достъп до базата данни се използват PDO и параметризирани подготвени заявки; този механизъм отделя параметрите от SQL конструкцията и е основен елемент от защитата срещу SQL Injection [6]. Към модела са добавени ограничаване на неуспешните опити за вход, валидиране на качваните файлове, контрол на достъпа до документите, SHA-256 контролни суми за проверка на целостта и одитен журнал. Журналът съхранява потребител, действие, обект, дата и час и IP адрес и осигурява последваща проследимост на значимите операции. Представеният на фиг. 4 модел обобщава последователното прилагане на основните механизми за защита в системата – от удостоверяването на потребителя и управлението на сесията до контрола на достъпа, защитата на заявките и регистрирането на действията.



Фигура 4. Обобщен модел на механизмите за защита

Комбинирането на тези механизми осигурява многостепенна защита на достъпа до данните и операциите в информационната система.

2.3. Реализация и експериментална проверка

За практическа проверка(апробация) на модела е разработен работещ прототип с PHP, MariaDB, HTML5, CSS3, JavaScript и Bootstrap. Приложението е разгърнато в контролирана тестова среда с Windows 11, XAMPP, Apache, PHP и MariaDB. Използването на WEB интерфейс позволява достъп чрез стандартен браузър и централизирано обновяване на приложната логика.

3 Заключение

Експерименталната проверка обхваща инсталационния процес и основните функционални сценарии: управление на потребители и роли, създаване и редактиране на профили на докторанти, търсене и филтриране, управление на документи, генериране на справки, работа с помощния център и регистриране на действията. Проверени са също и удостоверяването, защитата на паролите, контролът на достъпа, CSRF защитата, използването на подготвени заявки и одитната проследимост. Извършена е проверка на сценарии за зареждане на списъци, търсене, филтриране, работа с документи и едновременна работа на няколко потребители. Апробацията не установи значими отклонения от зададените функционалности. Установи се поддържането на коректно взаимодействие между основните модули на прототипа.

Приложението на технологиите в образователна среда се разглежда и като направление на педагогическите изследвания [8]. Предложеният модел на WEB базирана информационна система „Докторант“ обединява централизирано управление на академична информация, модулна трислойна архитектура, нормализиран релационен модел и многослоен подход към сигурността. Разделянето на представянето, бизнес логиката и достъпа до данните създава предпоставки за поддържаемост и разширяемост, а RBAC позволява гъвкаво управление на правата. Комбинирането на контрол на сесиите, CSRF защита, подготвени заявки, защитено съхранение на паролите, контрол върху файловете и одитна проследимост формира цялостен модел за защита на основните информационни потоци. Реализираният прототип и проведената експериментална проверка показват, че моделът може да служи като основа за развитие на реална университетска информационна система. Бъдещото развитие може да включва интеграция с други университетски системи, автоматизирани известия, разширени аналитични справки и електронен документооборот. По-широкият университетски контекст включва и решенията, проблемите и перспективите на електронното обучение [1].

ЛИТЕРАТУРА:

[1] Вардева, И., Станева, Л. Електронно обучение – решения, проблеми и перспективи. Годишник на Университет „Проф. д-р Асен Златаров“, Бургас, т. 36, № 2, 2007, с. 117–120.

[2] Цанков Ц., Ненков Н. Възможностите на отдалечени клиенти в архитектурата клиент-сървър. Сборник статии от XII международна научна конференция „Инновации в технологиях и образовании“, филиал на КузГТУ в г. Белово, 2019, ISBN 978-5-00137-063-5, с. 342–346.

[3] Sandhu R., Ferraiolo D., Kuhn R. The NIST Model for Role-Based Access Control: Towards a Unified Standard. Proceedings of the 5th ACM Workshop on Role-Based Access Control, 2000.

[4] PHP Documentation. Password Hashing Functions: password_hash() and password_verify(). The PHP Group.

[5] OWASP Foundation. Cross-Site Request Forgery Prevention Cheat Sheet. OWASP Cheat Sheet Series.

[6] MariaDB Documentation. Prepared Statements. MariaDB Server Documentation.

[7] Кемил И., Симеонова И. Дигитализация и предизвикателствата пред сигурността в електронната администрация. Научна конференция на НВУ „Васил Левски“, Велико Търново, 12–14 ноември 2025.

[8] Бурова И. Същност на технологиите и приложението им в обучението. Е-списание „Образование и развитие“, бр. 17, 2026, с. 78–83. ISSN 2603-3577.

PLC AND HMI IMPLEMENTATION OF AN AUTOMATED CONTROL SYSTEM FOR AN INDUSTRIAL PACKAGING LINE*

ZDRAVKO A. ZDRAVKOV

ABSTRACT: *The paper presents a PLC and HMI software implementation of an automated control system for an industrial packaging line. The developed model is intended for a technological process related to placing sealing liners in aluminum caps and directing the finished products to transport boxes. The control system is implemented in Siemens TIA Portal V16 and uses a Siemens S7-1200 CPU 1214C controller, a KTP700 Basic PN operator panel and PROFINET communication. The PLC program is organized in separate functional blocks for system control, process logic, counting and dosing, alarm diagnostics and data exchange with the HMI. The performed tests confirm the correct operation of the main functions in automatic and manual mode, counting of finished products, dosing into boxes and visualization of alarm states.*

KEYWORDS: *PLC, HMI, TIA Portal, Siemens S7-1200, PROFINET, automated control, packaging line, alarm diagnostics*

DOI: https://doi.org/10.46687/MT26ZAZ

PLC И HMI РЕАЛИЗАЦИЯ НА АВТОМАТИЗИРАНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНДУСТРИАЛНА ПАКЕТИРАЩА ЛИНИЯ

ЗДРАВКО А. ЗДРАВКОВ

АБСТРАКТ: *В доклада е представена PLC и HMI софтуерна реализация на автоматизирана система за управление на индустриална пакетираща линия. Разработеният модел е предназначен за технологичен процес, свързан с поставяне на уплътнители в алуминиеви капачки и насочване на готовата продукция към транспортни кашони. Системата е реализирана в среда Siemens TIA Portal V16 чрез контролер Siemens S7-1200 CPU 1214C, операторски панел KTP700 Basic PN и комуникация чрез PROFINET. PLC програмата е организирана в отделни функционални блокове за управление на режимите, технологична логика, броене и дозиране, алармена диагностика и обмен на данни с HMI интерфейса. Проведеното тестване потвърждава коректната работа на основните функции в автоматичен и ръчен режим, отчитането на готовите изделия, дозирането по кашони и визуализацията на алармени състояния.*

1 Въведение

Съвременното индустриално производство поставя високи изисквания към точността, повторяемостта и надеждността на технологичните операции. При пакетиращите линии тези изисквания са особено важни, тъй като крайният етап от производството обединява няколко взаимно свързани операции: подаване на изделия, ориентиране, поставяне на компонент, контрол, броене и насочване към транспортна опаковка. Автоматизираното управление създава условия за намаляване на ръчната намеса, ограничаване на грешките и по-добро наблюдение на производствения процес [7]. Основно място при решаването на подобни задачи заемат програмируемите логически контролери и операторските HMI интерфейси. Чрез PLC контролера се реализира обработката на входните сигнали,

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

изпълнението на управляващата логика и формирането на изходни команди към изпълнителните механизми. HMI панелът осигурява визуализация на текущото състояние, настройка на параметри и показване на алармени съобщения към оператора [1], [3], [4]. Целта на доклада е да представи разработена PLC и HMI система за управление на индустриална линия за поставяне на уплътнители в алуминиеви капачки и пакетиране на готовата продукция. Акцентът е поставен върху функционалната структура на системата, програмната организация в TIA Portal, броенето и дозирането по кашони, алармената диагностика, HMI визуализацията и резултатите от проведените функционални тестове.

2 Технологичен процес и функционална структура на системата

Разглежданата производствена линия включва последователно подаване и ориентиране на алуминиеви капачки, подаване на уплътнители, пресов механизъм за поставяне на уплътнителя, преброяване на готовите изделия и разпределяне на продукцията към кашони. За правилното протичане на процеса е необходимо отделните операции да бъдат синхронизирани и да се изпълняват само при наличие на зададените входни условия. Функционалната структура на системата обединява входна част, управляващо устройство, изходна част и HMI визуализация. Входните сигнали включват команди от бутони, избор на режим и данни от датчици за наличие на капачки, уплътнители и кашони. Изходната част управлява основния конвейер, ориентиращия механизъм, вибраторите, пресовия механизъм, разпределителния клапан и сигнализацията. Така системата осигурява връзка между технологичния процес, PLC управлението и операторския интерфейс. Визуалният PLC мониторинг и моделирането на конвейери в индустриални комуникационни мрежи са разгледани в [10, 11].



Фиг. 1. Функционална структура на разработената PLC и HMI система

За повишаване на надеждността и безопасността на производствения процес в системата са предвидени механизми за контрол на последователността на операциите, откриване на липса на детайли и обработка на аварийни състояния. При възникване на неизправност или несъответствие в технологичния процес PLC прекъсва изпълнението на съответната операция, подава сигнал към оператора чрез HMI интерфейса и не допуска продължаване на производството до отстраняване на причината. По този начин се намалява вероятността от производство на дефектни изделия и се повишава ефективността на автоматизираната линия. Систематичният анализ на отказите може да бъде развит чрез метода FMEA [8]. Пример за PLC управление с вградени сензори за безопасност е представен в [15].

Таблица 1. Основни елементи и функции в разработената система

Елемент	Функция в системата	Роля в управлението
PLC Siemens S7-1200	Обработка на входни сигнали и изпълнение на логиката	Основно управляващо устройство
HMI KTP700 Basic PN	Визуализация, настройки и аларми	Операторски интерфейс
Входни сигнали DI	Бутони, датчици и избор на режим	Контрол на условията за работа
Изходни сигнали DQ	Конвейер, вибратори, преса, клапан	Управление на изпълнителните механизми
DB_Production	Параметри, времена, броячи и статуси	Обмен на данни между PLC и HMI

3 PLC програмна реализация в TIA Portal

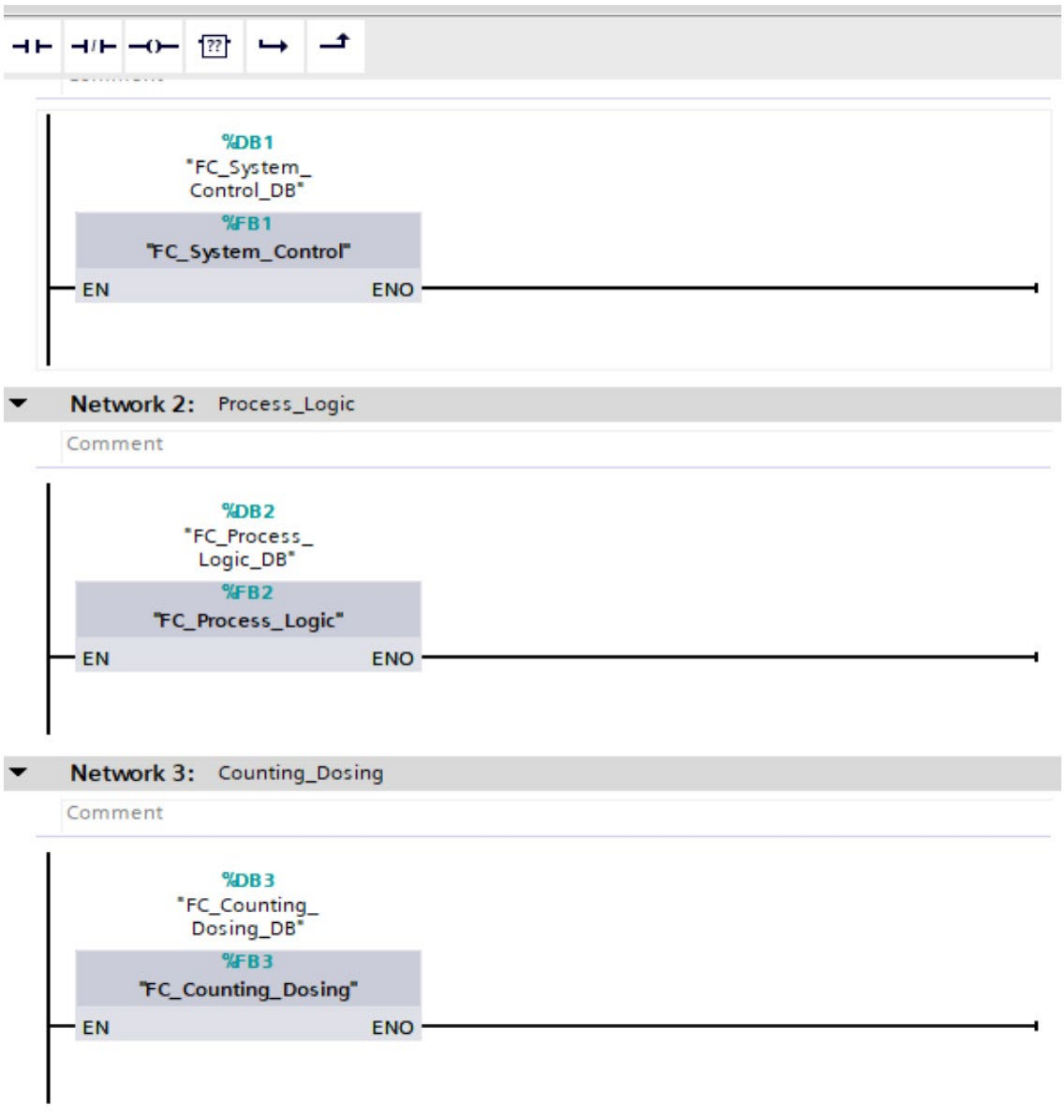
Софтуерната реализация е извършена в инженерната среда Siemens TIA Portal V16. Използването на обща среда за конфигуриране на PLC и HMI улеснява създаването на комуникация между контролера и операторския панел, както и обмена на технологични и диагностични данни [2], [5]. Програмата е организирана модулно, което позволява по-ясно разделяне на отделните функции, по-лесна проверка на логиката и възможност за бъдещо разширяване.

Основният организационен блок Main [OB1] извиква последователно програмните блокове, реализиращи управлението на режимите, технологичната логика, броенето, дозирането и алармените състояния. Блокът FC_System_Control формира общото разрешение за работа на системата и обработва условията за старт, стоп, авариен стоп и избор между автоматичен и ръчен режим. Блокът FC_Process_Logic управлява основните изпълнителни механизми на линията според активния режим и състоянието на входните сигнали.

Блокът FC_Counting_Dosing е реализиран на език SCL и съдържа логика за преобразуване на времеви стойности, генериране на симулационен импулс, броене на изделия, дозиране по кашони, превключване на разпределителния клапан и формиране на алармени състояния. Използването на LAD и SCL съответства на практиката при PLC програмиране съгласно IEC 61131-3. LAD е подходящ за визуализиране на логически зависимости и междублокировки, а SCL е удобен при реализиране на последователна логика, броене и обработка на данни [6].

При разработването на програмата са използвани символно адресиране на входовете, изходите и вътрешните променливи, което повишава четимостта на кода и улеснява неговата поддръжка. Разделянето на логиката във функционални блокове позволява всяка част от управлението да бъде тествана и модифицирана независимо, без да се нарушава работата на останалите програмни модули. Този подход подобрява надеждността на приложението и създава предпоставки за лесно добавяне на нови функционалности.

За проверка на програмната реализация е използвана симулационната среда PLCSIM, чрез която е проследена последователността на изпълнение на технологичния процес и са проверени реакциите на системата при различни входни събития и аварийни ситуации. Проведените тестове потвърждават коректната работа на логическите зависимости, управлението на изпълнителните механизми и обмена на данни между PLC контролера и HMI панела, което гарантира готовността на системата за внедряване в реална производствена среда. Моделирането и управлението на производствени системи чрез Factory I/O и PLC е разгледано в [16].



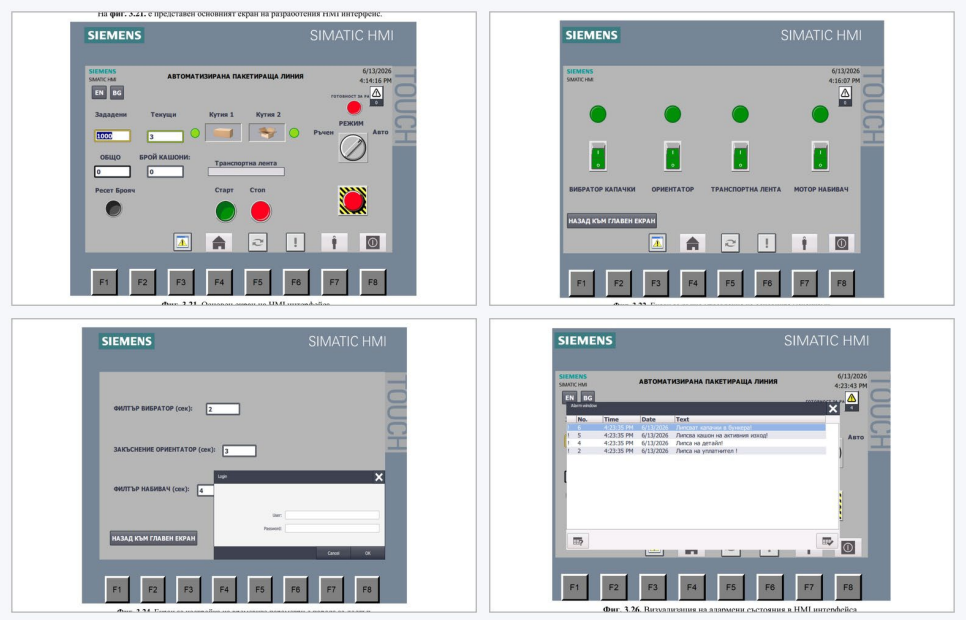
Фиг. 2. Организация на основните програмни блокове в TIA Portal

4 HMI интерфейс, броене и алармена диагностика

Операторското управление е реализирано чрез HMI панел Siemens KTP700 Basic PN. Интерфейсът предоставя основен екран за наблюдение на процеса и броячите, екран за ръчно управление, екран за настройка на технологични времена, алармен екран и избор на език. Чрез тези екрани операторът може да следи състоянието на линията, да управлява отделни механизми при настройка и да получава информация при възникване на неправилни работни състояния [3, 4]. Взаимодействието между хора и машини при управление на физически обекти е разгледано в [20].

Броенето и дозирането по кашони са ключови функции на разработката. При отчитане на готово изделие се увеличава текущият брой. След достигане на зададена стойност за един кашон системата отчита готов кашон, нулира текущия брояч и превключва разпределителния клапан към друг изход. По този начин се реализира последователно разпределяне на продукцията без прекъсване на технологичния процес.

Алармената диагностика обхваща основни аварийни и технологични състояния: авариен стоп, липса на уплътнител, липса на капачка преди пресовия механизъм, липса на кашон на активния изход, липса на капачки в бункера и запълнен транспортен канал. Визуализацията на тези състояния чрез HMI панела улеснява оператора и съкращава времето за откриване на причината за спиране.



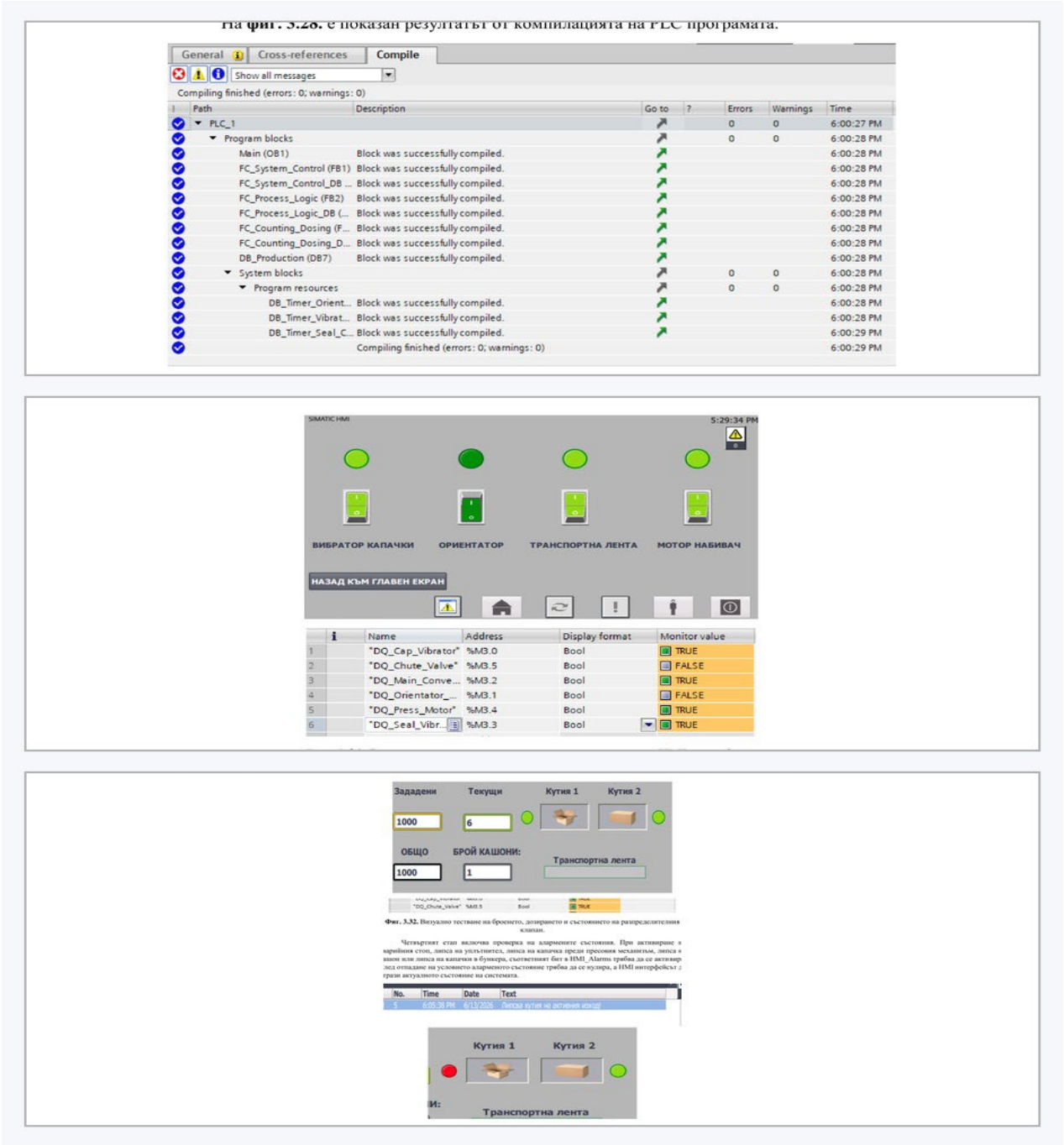
Фиг. 3. Основни HMI екрани за управление, настройки и аларми

5 Тестване и анализ на резултатите

След завършване на програмната реализация е извършено тестване на разработената система в TIA Portal. Проверени са компилацията на PLC програмата, компилацията на HMI проекта, работата на автоматичния и ръчния режим, броенето на готовите изделия, дозирането по кашони, превключването на разпределителния клапан и визуализацията на алармените състояния.

Проведените проверки показват, че програмните блокове се компилират успешно и че взаимодействието между PLC логиката и HMI интерфейса е коректно. При симулационно

тестване системата изпълнява зададената последователност, отчита произведените изделия, формира готови кашони и визуализира активните аларми. Това потвърждава, че разработеният модел може да служи като основа за бъдещо реално внедряване.



Фиг. 4. Резултати от компилация, симулация и визуална проверка

Към техническата реализация е направена и ориентировъчна икономическа оценка на PLC и HMI частта. Тя включва управляващо оборудване, операторски панел, входно-изходни елементи, електрическа периферия, окабеляване, софтуерна разработка, настройка и тестване. Оценката не включва цялостна механична конструкция на производствената

линия. Практическият ефект от внедряване на подобна система се свързва с по-точно отчитане, по-бърза диагностика, намаляване на ръчната намеса и по-добра проследимост на производствения процес. Методологията за проектиране на логистични системи, експертният анализ на управлението и качеството и измерването на производствени фактори са разгледани в [12, 13, 19].

Резултатите от проведеното тестване показват, че разработената система изпълнява коректно зададения алгоритъм на управление при различни работни сценарии. Не са установени логически конфликти между отделните програмни блокове, а преходите между режимите на работа се осъществяват без нарушаване на последователността на технологичния процес. Това потвърждава правилното структуриране на програмната логика и надеждната работа на алгоритмите за управление.

Извършената разработка демонстрира възможностите на средата TIA Portal за създаване на интегрирани системи за автоматизация, съчетаващи PLC управление и HMI визуализация. Получените резултати могат да бъдат използвани като основа за последващо надграждане на системата чрез добавяне на индустриални комуникационни мрежи, архивиране на производствени данни, дистанционен мониторинг и функции за превантивна диагностика, което ще повиши ефективността и гъвкавостта на производствената линия. Развитието на комуникационната инфраструктура може да се съпостави с изследванията за индустриални мрежи, качество на данните и интелигентни комутатори [9, 14, 18]. За последващ анализ на производствените данни може да се разгледа и използването на динамични масиви в MS Excel [17].

6 Заключение

В доклада е представена PLC и HMI реализация на автоматизирана система за управление на индустриална пакетираща линия за поставяне на уплътнители в алуминиеви капачки. Разработката обединява технологично управление, операторска визуализация, производствено броене, дозиране по кашони и алармена диагностика.

Получените резултати показват, че модулната организация на PLC програмата осигурява по-добра прегледност, възможност за тестване на отделните функции и условия за бъдещо разширяване. HMI интерфейсът подобрява взаимодействието между оператора и системата, като осигурява наблюдение, настройки и визуализация на алармени състояния.

Разработеният модел може да бъде използван като основа за реално внедряване в индустриална среда. В бъдеще системата може да бъде надградена чрез добавяне на допълнителни датчици, архивиране на производствени данни, отдалечен мониторинг и интеграция със системи от по-високо ниво.

ЛИТЕРАТУРА:

[1] Siemens AG. SIMATIC S7-1200 Programmable Controller. System Manual.

[2] Siemens AG. SIMATIC STEP 7 Basic/Professional V16. Engineering System Manual.

[3] Siemens AG. SIMATIC WinCC Basic V16. System Manual.

[4] Siemens AG. SIMATIC HMI Basic Panels 2nd Generation. Operating Instructions.

[5] Siemens AG. TIA Portal V16 Online Help Documentation.

[6] IEC 61131-3. Programmable controllers - Part 3: Programming languages.

[7] Petruzella F. Programmable Logic Controllers. McGraw-Hill Education.

[8] Arabadzhieva-Kalcheva N., Tsankov Ts. Failure Modes and Effects Analysis – FMEA. Scientific Conference with International Participation MATTEH 2022, Conference Proceedings, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 58–62.

[9] Denev D., Tsankov Ts., Design and Implementation of a Field Level of an Industrial Communication Network for the Needs of the Industry, 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), Ohrid, North Macedonia, 2022, ISBN 978-1-6654-8500-5, DOI: 10.1108/ICEST55168.2022.9828607.

[10] Denev D., Tsankov Ts., Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring, Annual University Scientific Conference, National Military University "Vasil Levski", Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1259–1266.

[11] Denev D., Nikolova S., Tsankov Ts., Elaborating a 3D Blueprint of a Conveyor and Its Application in Industrial Communication Networks, XIX International Conference on Communication Electromagnetics and Medical Application (CEMA), Athens, Greece, 2025, ISSN 1314-2100, pp. 52–58.

[12] Kodzheykova, V. Methodology of design of logistics systems in medium-serial production. Proceedings of the Annual University Scientific Conference 2021, National Military University “Vasil Levski”, Veliko Tarnovo, 2021, pp. 2481–2488, ISSN 2367-7481.

[13] Yankova-Yordanova, Y., Kodzheykova, V. Expert approach for analysing a logistics control system and quality management in the conditions of small and medium serial production. Journal Scientific and Applied Research, Vol. 15, 2019, pp. 37–47, ISSN 1314-6289.

[14] 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, Proceedings of the 15th International Scientific and Practical Conference "Environment. Technology. Resources.", Vol. II, Rezekne, Latvia, 2024, ISSN 1691-5402, DOI: 10.17770/etr2024vol2.8036, pp. 120–126.

[15] Danev A., Denev D., Intelligent Garage Door Control System via PLC with Built-in Safety Sensors, Proceedings of International Scientific Conference Defense Technology Forum, National Military University "Vasil Levski", Shumen, 2025, ISSN 2815-4282, pp. 648–655.

[16] Docheva A., Denev D., Modeling and Control of an Automated Manufacturing System using the Factory I/O Simulation Platform and Programmable Logic Controller, Proceedings of Student Scientific Session, Technical University of Gabrovo, 2025, ISSN 1313-3055, pp. 291–296.

[17] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.

[18] Tsankov Ts., Docheva A. Implementing smart switches and technologies in communication networks. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, pp. 103–110. https://doi.org/10.46687/YT24CAL

[19] Kodzheykova, V. Measurement of factors to provide medium serial technological production. Proceedings of the Scientific Conference with International Participation MATTEH 2022, Vol. 2, Shumen, 2022, pp. 302–308, ISSN 1314-3921.

[20] Tsvetanova, P. T., Stoyanova, V. T. Research of Systems for Interaction between People and Machines in the Management of Physical Objects. Proceedings of the International Scientific Conference “Defense Technology”, 2019. ISSN 2367-7902.

INTEGRATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES INTO MODERN COMMUNICATION AND INFORMATION SYSTEMS*

GABRIELA S. MARKOVA, DANIEL R. DENEV

ABSTRACT: *Artificial intelligence is becoming a key technology for the development of modern communication and information systems. Through machine learning, automated data analysis and natural language processing, AI allows for the optimization of communication networks, the automation of information processes and the improvement of human-system interaction. The integration of artificial intelligence creates opportunities for faster processing of large volumes of information, load forecasting, anomaly detection and increased information security. Along with the benefits, there are challenges related to data protection, the reliability and transparency of algorithms and the need for human control. Artificial intelligence is essential for the construction of more intelligent, adaptive and efficient communication and information systems.*

KEYWORDS: *data processing, artificial intelligence, cybersecurity*

DOI: https://doi.org/10.46687/MT26GSM

ИНТЕГРАЦИЯ НА ТЕХНОЛОГИИ С ИЗКУСТВЕН ИНТЕЛЕКТ В СЪВРЕМЕННИТЕ КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ

ГАБРИЕЛА С. МАРКОВА, ДАНИЕЛ Р. ДЕНЕВ

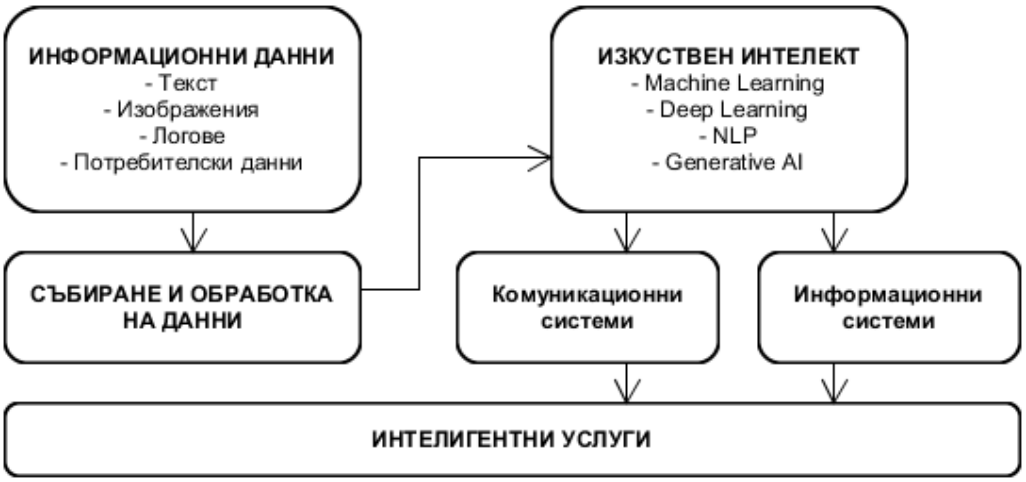
АБСТРАКТ: *Изкуственият интелект се превръща в ключова технология за развитието на съвременните комуникационни и информационни системи. Чрез машинно обучение, автоматизиран анализ на данни и обработка на естествен език ИИ позволява оптимизиране на комуникационните мрежи, автоматизиране на информационни процеси и подобряване на взаимодействието между човек и система. Интеграцията на изкуствен интелект създава възможности за по-бързо обработване на големи обеми от информация, прогнозиране на натоварването, откриване на аномалии и повишаване на информационната сигурност. Наред с ползите съществуват предизвикателства, свързани със защитата на данните, надеждността и прозрачността на алгоритмите и необходимостта от човешки контрол. Изкуственият интелект има съществено значение за изграждането на по-интелигентни, адаптивни и ефективни комуникационни и информационни системи.*

1 Въведение

Съвременното общество се характеризира с непрекъснато нарастване на обема, скоростта и разнообразието на информационните потоци. Организациите, институциите и бизнес структурите ежедневно обработват огромни количества структурирани и неструктурирани данни, които постъпват от комуникационни мрежи, информационни платформи, мобилни устройства, сензори, облачни услуги и различни цифрови приложения. В резултат на това традиционните подходи за обработка и управление на информацията все по-трудно отговарят на изискванията за бързина, точност, мащабируемост и адаптивност. Изкуственият интелект предоставя технологични механизми, чрез които информационните системи могат не само да обработват

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

предварително зададени инструкции, но и да анализират модели, да откриват зависимости, да правят прогнози и да подпомагат вземането на решения. За разлика от традиционните информационни системи, при които голяма част от логиката е предварително дефинирана, интелигентните системи могат да използват исторически и текущи данни, за да адаптират своето поведение. Това превръща ИИ в ключов компонент на процеса на цифрова трансформация. Програмните модели за автоматизиране на когнитивни процеси и подпомагането на разработката на web приложения чрез когнитивна машина са разгледани в [2, 3]. Интеграцията на изкуствен интелект има особено значение за комуникационните системи. Съвременните мрежи трябва да обслужват милиарди устройства и огромен брой едновременни комуникационни сесии, като същевременно осигуряват висока надеждност, ниска латентност и ефективно използване на наличните ресурси. Интелигентните алгоритми могат да подпомагат управлението на мрежовия трафик, откриването на аномалии, разпределението на ресурсите и прогнозното управление на инфраструктурата. Поради това изследването на интеграцията между ИИ и комуникационните и информационните системи представлява актуална научна и практическа задача. Въпросът вече не се състои единствено в това дали изкуственият интелект може да бъде внедрен в дадена система, а по какъв начин това да бъде направено така, че да се постигне баланс между ефективност, сигурност, надеждност, икономическа целесъобразност и човешки контрол. На фиг. 1 е показан общия модел на интеграция на ИИ.



Фиг. 1. Общ модел на интеграция на ИИ

2 Изкуственият интелект като основа за интелигентни информационни системи

Една от основните области, в които изкуственият интелект променя информационните системи, е автоматизираният анализ на данни. Съвременните организации разполагат с големи информационни масиви, но самото наличие на данни не гарантира възможност за ефективното им използване. Необходимо е данните да бъдат структурирани, обработени и интерпретирани по начин, който позволява извличане на практически значима информация. Систематизирането на информационни потоци в логистиката и обработката на данни чрез динамични масиви в MS Excel са разгледани в [4, 21]. Алгоритмите за машинно обучение могат да идентифицират зависимости и

закономерности, които трудно биха били открити чрез традиционни методи. Особено важна е способността на интелигентните системи да извършват прогнозен анализ. На базата на исторически данни алгоритмите могат да подпомагат прогнозиране на потребителско поведение, натоварване на информационни ресурси, възникване на технически проблеми и промени в определени процеси. По този начин информационната система се превръща от пасивен инструмент за съхранение и представяне на информация в активен механизъм за подпомагане на управленските решения. Друга съществена област е автоматичното класифициране и обработване на информация. Чрез методи на машинното обучение и дълбокото обучение могат да бъдат анализирани текстове, изображения, аудио и видео съдържание. Това намира приложение при автоматично категоризиране на документи, извличане на информация от текстови масиви, анализ на клиентски заявки, обработка на мултимедийно съдържание и управление на цифрови архиви. Специализирани изследвания разглеждат разпознаването на обекти чрез невронни мрежи и трансфер на знания [5, 8]. В резултат на това се намалява необходимостта от ръчна обработка и се повишава скоростта на информационните процеси. Генеративният изкуствен интелект допълнително разширява възможностите на информационните системи. Съвременните генеративни модели могат да създават текст, обобщения, структурирана информация и други цифрови резултати въз основа на естественоезикови инструкции. Това позволява разработването на ново поколение интерфейси, при които потребителят взаимодейства със системата чрез естествен език, вместо да използва сложни менюта и предварително зададени команди. По този начин ИИ се превръща не само в аналитичен компонент, но и в интелигентен посредник между човека и информационната инфраструктура. На фиг. 2 е показана архитектура на интелигентна комуникационна система.



Фиг. 2. Архитектура на интелигентна комуникационна система

3 Интеграция на ИИ в съвременните комуникационни системи и мрежи

Комуникационните мрежи представляват сложни динамични среди, в които постоянно се променят натоварването, разпределението на ресурсите и поведението на

потребителите. Традиционното управление на мрежите до голяма степен се основава на предварително зададени правила и конфигурации. При увеличаване на мащаба и сложността на инфраструктурата този подход може да стане недостатъчно ефективен. Интегрирането на ИИ предоставя възможност управлението на мрежовите ресурси да бъде автоматизирано и адаптирано към текущото състояние на системата [9, 18]. Софтуерно дефинираните мрежи са разгледани в [25], а пример за паралелна изчислителна инфраструктура е клъстерната система в среда MPI [7]. Алгоритмите за машинно обучение могат да се използват за прогнозиране на мрежовото натоварване и оптимизиране на разпределението на комуникационните ресурси. Например системата може да анализира исторически и текущи показатели, за да установи вероятността от претоварване на определен мрежов сегмент и предварително да предприеме действия за преразпределяне на ресурсите. Подобен подход може да намали латентността, да повиши качеството на услугата и да подобри използването на наличния капацитет. Особено перспективно направление представляват самооптимизиращите се мрежи. При тях изкуственият интелект се използва за наблюдение на мрежовото състояние, откриване на отклонения и автоматично адаптиране на определени параметри. Вместо операторът да реагира след възникването на проблем, интелигентната система може да идентифицира потенциален риск и да предприеме превантивни действия. Това е особено важно при мащабни инфраструктури, при които ръчният контрол на всички компоненти е практически невъзможен. ИИ има значение и за развитието на комуникационните системи от ново поколение. При внедряването на 5G и развитието на бъдещи комуникационни архитектури се увеличават изискванията към автоматизацията, ниската латентност и динамичното управление на ресурсите. Интелигентните алгоритми могат да подпомагат управлението на мрежовите функции, оптимизацията на трафика и адаптирането на услугите към конкретните потребности [12–15]. В този контекст интеграцията на ИИ постепенно се превръща от допълнителна функционалност в стратегически елемент от архитектурата на комуникационните системи. Друг пример за алгоритмична оптимизация е синтезът на сигнали с оптимални автокорелационни свойства чрез изкуствени имунни системи [11, 23]. Таблица 1 показва цифрови показатели при интеграция на ИИ в комуникационни системи.

Таблица 1. Цифрови показатели при интеграция на ИИ в комуникационни системи

Показател	Без ИИ	С ИИ	Промяна (%)
Латентност (ms)	42	25	−40,5
Използване на мрежовия капацитет (%)	68	84	+23,5
Загуба на пакети (%)	3,2	1,1	−65,6
Енергийна ефективност (%)	71	89	+25,4
Точност при прогнозиране (%)	64	93	+45,3
Време за откриване на аномалия (s)	18	4	−77,8
Време за реакция (s)	12	3	−75,0
Ниво на автоматизация (%)	35	82	+134,3

4 Интелигентно взаимодействие между човека и информационната система

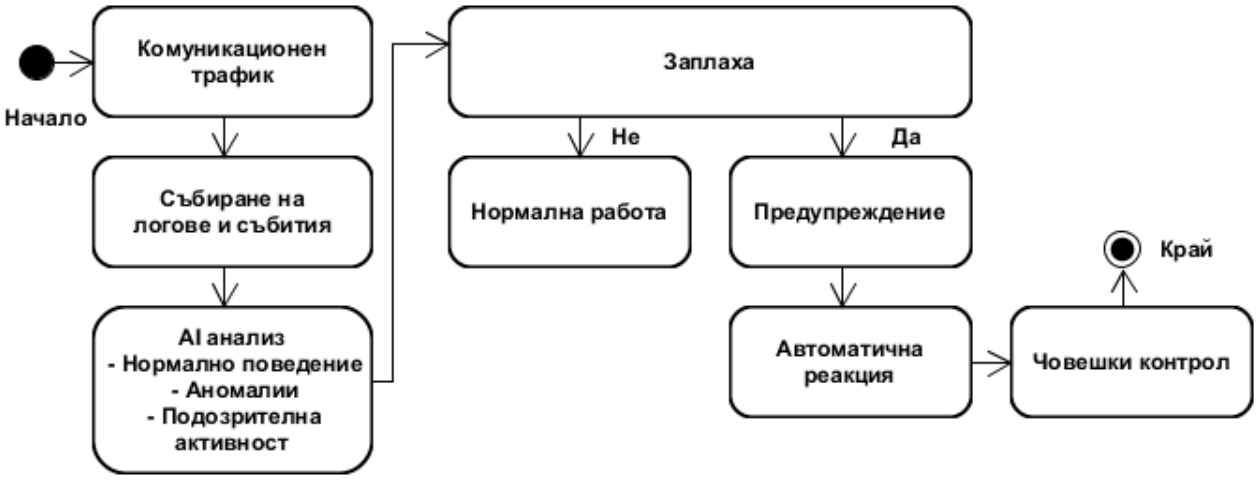
Една от най-видимите промени, предизвикани от изкуствения интелект, е трансформацията на начина, по който потребителите взаимодействат с информационните системи. Традиционните интерфейси обикновено изискват от потребителя да познава определена структура от менюта, команди и процедури. Интелигентните интерфейси позволяват взаимодействие чрез естествен език, гласови команди и контекстно ориентирани механизми. Управлението чрез виртуален гласов асистент и личностовата персонификация на големи езикови модели са разгледани в [1, 10]. Това създава предпоставки за по-достъпни и по-интуитивни информационни системи. Чатботовете и виртуалните асистенти са сред най-разпространените приложения на тази концепция. Те могат да предоставят информация, да обработват стандартни потребителски заявки, да подпомагат обслужването на клиенти и да насочват потребителите към подходящи информационни ресурси. При правилно интегриране тези системи могат да намалят натоварването върху служителите и едновременно с това да осигурят по-бърз достъп до информация. Обработката на естествен език има съществено значение за развитието на подобни приложения. Чрез нея информационната система може да анализира не само отделни ключови думи, но и контекста на потребителската заявка. Това позволява създаването на по-гъвкави системи за търсене, автоматично обобщаване на документи, анализ на текстови комуникации и извличане на конкретна информация от големи информационни масиви. По този начин се намалява времето, необходимо за намиране и обработване на релевантна информация. Въпреки тези предимства човешкият фактор остава ключов. Интелигентната система може да предостави препоръка или автоматично генериран резултат, но в редица области окончателната преценка трябва да остане в ръцете на компетентен специалист. Това е особено важно при системи, които могат да влияят върху финансови, административни, технически или други значими решения. Следователно ефективната интеграция на ИИ трябва да се основава на модел на взаимодействие човек–машина, при който автоматизацията подпомага човешката експертиза, а не я замества безконтролно. Фиг. 3 показва диаграмата на взаимодействие.



Фиг. 3. Диаграма на взаимодействие

5 Изкуствен интелект и информационна сигурност

С нарастването на цифровата свързаност се увеличава и необходимостта от защита на комуникационните и информационните системи. Съвременните киберзаплахи и заплахите при интелигентни домове са разгледани в [17, 22]. Хардуерни реализации на генератори на псевдослучайни последователности за криптографски приложения са представени в [6, 19]. Класическите механизми за сигурност често разчитат на предварително дефинирани правила и известни модели на атаки. Този подход има ограничения при откриването на нови или динамично променящи се заплахи. Изкуственият интелект предоставя възможност за анализ на големи обеми от системни събития и идентифициране на аномалии, които могат да бъдат индикатор за потенциална атака. Машинното обучение може да бъде използвано за изграждане на модели, които анализират нормалното поведение на мрежовия трафик и откриват отклонения от него. Ако определено устройство или потребител започне да генерира необичайна комуникационна активност, интелигентната система може да сигнализира за потенциален инцидент. Предимството на този подход се състои във възможността за откриване на поведенчески модели, които не са предварително описани като конкретни сигнатури. ИИ може да подпомага и автоматизираната реакция при инциденти. При определени условия системата може да изолира подозрителен компонент, да блокира необичайна комуникация или да насочи инцидента към специалист за допълнителен анализ. Това съкращава времето между откриването и реакцията и може да ограничи потенциалните последствия от кибератака. В същото време автоматизираните действия трябва да бъдат внимателно контролирани, тъй като неправилно класифицирана активност може да доведе до блокиране на легитимни потребители или услуги. Съществува и обратната страна на интеграцията на ИИ в областта на сигурността. Същите технологии могат да бъдат използвани от злонамерени лица за автоматизиране на атаки, генериране на убедително съдържание, откриване на уязвимости и мащабиране на определени злонамерени дейности. Поради това бъдещето на информационната сигурност вероятно ще бъде свързано с непрекъсната технологична надпревара между интелигентни защитни и атакуващи системи. Това налага развитието на устойчиви архитектури, човешки надзор и политики за отговорно използване на изкуствения интелект. Фиг. 4 изобразява диаграмата на информационен процес на откриване и реакция при заплаха.



Фиг. 4. Диаграма на процес на откриване и реакция при заплаха

6 Предизвикателства и перспективи пред интеграцията на ИИ

Въпреки значителния потенциал на изкуствения интелект, неговото интегриране в съществуващи комуникационни и информационни системи е свързано с редица технически и организационни предизвикателства. Едно от тях е необходимостта от висококачествени данни. Алгоритмите за машинно обучение зависят от информацията, върху която се обучават и с която работят. Неточни, непълни или предубедени данни могат да доведат до неправилни резултати, което поставя въпроса за качеството на данните и механизмите за тяхното управление. Друг важен проблем е прозрачността на алгоритмичните решения. При сложни модели, особено при дълбоко обучение, невинаги е лесно да се обясни защо системата е достигнала до определен резултат. Това създава затруднения в области, в които е необходимо решение да бъде обосновано и проверимо. Поради тази причина развитието на обясним изкуствен интелект представлява важно направление, чрез което се търси баланс между висока производителност на моделите и възможност за разбиране на техните решения. Съществено предизвикателство е и защитата на личните и чувствителните данни. Интелигентните системи често работят с информация за потребители, комуникационни модели и поведенчески характеристики. Това изисква внимателно управление на достъпа до данни, подходящи механизми за защита и ясни правила за тяхното използване. Наред с техническите мерки е необходимо организациите да изграждат култура на отговорно използване на ИИ и да определят конкретни правила относно ролята на човека при автоматизираното вземане на решения. В дългосрочна перспектива може да се очаква все по-тясно сливане между изкуствения интелект, облачните технологии, периферните изчисления, Интернет на нещата и комуникационните мрежи. Това ще създаде разпределени интелигентни среди, в които обработката и анализът на информация се извършват близо до източника на данните. Подобен модел може да намали латентността и комуникационните разходи и да позволи изграждането на системи, които реагират в реално време. Следователно бъдещото развитие на информационните и комуникационните технологии вероятно ще бъде свързано не просто с добавяне на ИИ към съществуващите системи, а с изграждането на архитектури, проектирани от самото начало около принципите на интелигентността и адаптивността. Различни приложни направления включват ИИ в обучението по геодезия [16], интелигентна паркинг инфраструктура с видеонаблюдение [20] и моделиране на управлението на звукозаписно студио чрез обобщени мрежи [24]. На фиг. 5 е показана устойчивостта на интелигентните системи със изкуствен интелект.

В рамките на разглеждания казус се анализира комуникационна мрежа с променливо натоварване, обслужваща голям брой потребители и свързани устройства. При увеличаване на броя на едновременните комуникационни сесии се наблюдава неравномерно разпределение на мрежовия трафик и недостатъчно ефективно използване на наличния комуникационен капацитет. При традиционния подход управлението се извършва чрез предварително зададени правила, което затруднява адаптирането на системата към бързо променящите се условия. За решаване на проблема се предлага интегриране на модул с изкуствен интелект, който непрекъснато анализира състоянието на комуникационната инфраструктура. Системата обработва информация за обема на трафика, натоварването на мрежовите устройства, използването на комуникационния капацитет, загубата на пакети и възникването на необичайна мрежова активност. Чрез алгоритми за машинно обучение се идентифицират характерни модели на поведение и се прогнозира възможността за претоварване или възникване на технически проблем. При установяване на неблагоприятна тенденция интелигентният модул автоматично предприема действия за оптимизиране на мрежовите ресурси. Трафикът може да бъде пренасочен към по-слабо натоварени участъци,

да бъдат променени приоритетите на определени комуникационни потоци и да бъде извършено по-ефективно разпределение на наличния капацитет. По този начин управлението на мрежата се превръща от реактивен в адаптивен процес, при който системата може да реагира автоматично според текущото състояние и прогнозираното натоварване. В таблица 2 е извършен сравнителен анализ на основни показатели преди и след внедряването на интелигентния модул.



Фиг. 5. Устойчивост на интелигентна система

КАЗУС: Интелигентна оптимизация на комуникационна мрежа чрез изкуствен интелект

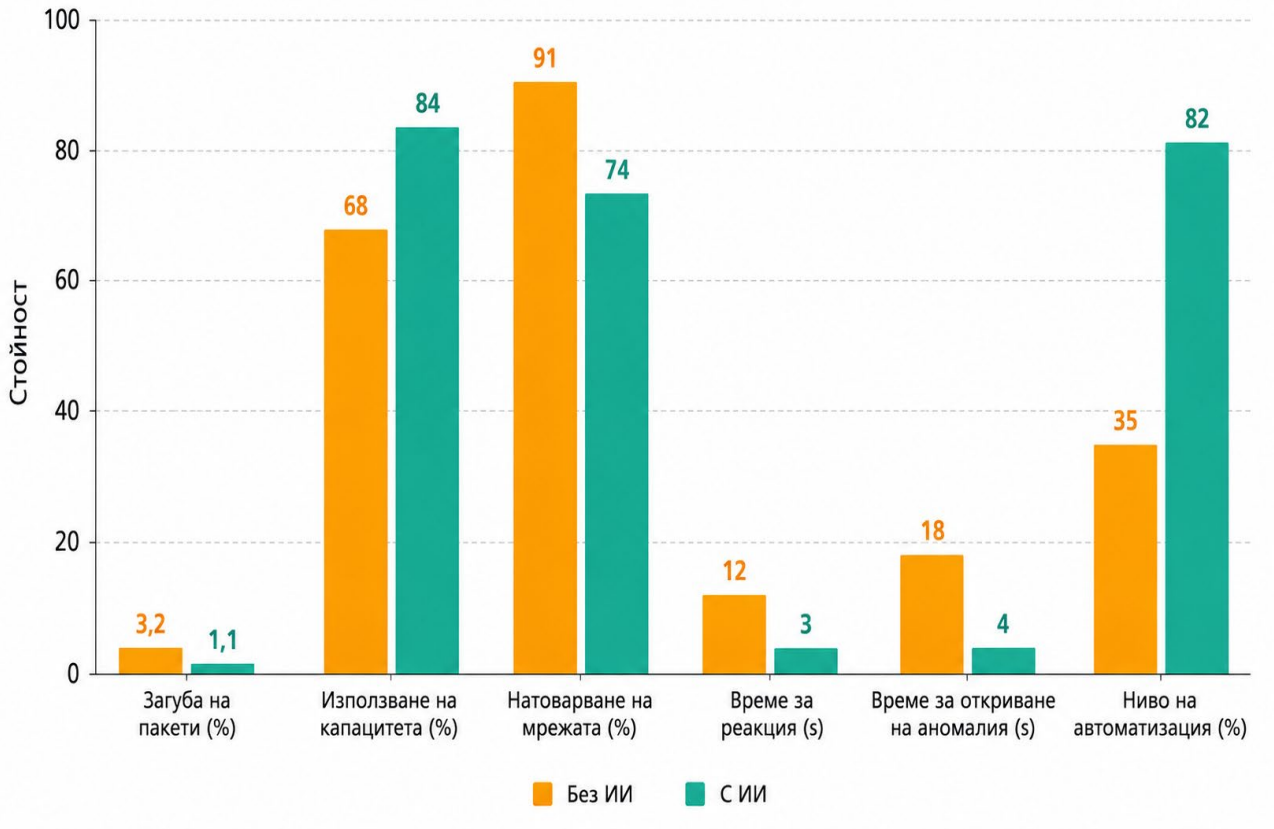
Таблица 2. Сравнителен анализ на основни показатели преди и след внедряването на интелигентния модул

Показател	Без ИИ	С ИИ
Загуба на пакети (%)	3,2	1,1
Използване на капацитета (%)	68	84
Натоварване на мрежата (%)	91	74
Време за реакция (s)	12	3
Време за откриване на аномалия (s)	18	4
Ниво на автоматизация (%)	35	82

За оценка на ефекта от интеграцията на изкуствения интелект се извършва сравнителен анализ на основни показатели преди и след внедряването на интелигентния модул. В примерния сценарий загубата на пакети намалява от 3,2% на 1,1%, използването

на комуникационния капацитет се увеличава от 68% на 84%, а времето за реакция при възникване на проблем се съкращава от 12 на 3 секунди. Допълнително времето за откриване на аномална активност се намалява от 18 на 4 секунди, което показва по-бързо идентифициране на потенциални проблеми в мрежовата инфраструктура.

Резултатите от казуса показват, че интегрирането на изкуствен интелект може да подобри ефективността и адаптивността на съвременните комуникационни системи. Основните ползи се изразяват в по-ефективното използване на мрежовия капацитет, намаляване на загубата на информационни пакети, по-бързо откриване на аномалии и автоматизиране на процесите по управление на мрежовите ресурси. Представеният казус демонстрира възможността традиционната комуникационна инфраструктура да бъде трансформирана в по-интелигентна и самооптимизираща се система. На фиг. 6 са показани резултати.



Фиг. 6. Сравнителни резултати на мрежови показатели

7 Заключение

Интеграцията на технологии с изкуствен интелект в съвременните комуникационни и информационни системи представлява един от най-значимите процеси в развитието на цифровата среда. ИИ променя начина, по който системите обработват информация, управляват ресурси, взаимодействат с потребителите и реагират на динамично променящи се условия. Машинното обучение, дълбокото обучение, обработката на естествен език и генеративните модели разширяват функционалността на традиционните системи и създават предпоставки за по-висока степен на автоматизация. В комуникационните мрежи изкуственият интелект позволява оптимизиране на трафика, прогнозиране на

натоварването, автоматично управление на ресурсите и откриване на аномалии. В информационните системи той подпомага анализа на големи масиви от данни, автоматизирането на рутинни операции и предоставянето на интелигентни услуги. Особено важно е развитието на естественоезиковите интерфейси, които постепенно променят традиционния модел на взаимодействие между човека и цифровите системи. Наред с възможностите трябва да бъдат отчетени и съществуващите рискове. Качеството на данните, прозрачността на алгоритмите, защитата на личната информация, киберсигурността и човешкият контрол са фактори, които определят дали интеграцията на ИИ ще бъде устойчива и обществено приемлива. Технологичният напредък сам по себе си не е достатъчен, ако не е съпроводен от подходящи организационни и етични механизми. В обобщение може да се приеме, че бъдещето на комуникационните и информационните системи ще бъде все по-тясно свързано с изкуствения интелект. Основната тенденция няма да бъде просто автоматизиране на отделни функции, а създаване на интелигентни, адаптивни и взаимосвързани екосистеми. Успешното им развитие ще зависи от способността на технологичните организации и научната общност да съчетават иновациите с принципите на сигурност, надеждност, прозрачност и отговорно използване на изкуствения интелект.

ЛИТЕРАТУРА:

[1] Алексиева А. Е., Кулев Н. З., Манов Л. Е. Личностова персонификация на големи езикови модели на базата на IPIP-50. Сборник доклади от научна конференция „Актуални проблеми на сигурността“, НВУ „Васил Левски“, Велико Търново, 2026, с. 807–814. ISSN 2367-7473 (PDF).

[2] Атанасов В. Един подход за подпомагане разработването на web приложения чрез когнитивна машина. Годишник на Шуменския университет „Епископ Константин Преславски“, Том XIV Е, 2024, ISSN 1314-8818 (Print), публикуван през 2025 г. https://doi.org/10.46687/AN24FTN

[3] Атанасов В., Иванова А. Анализ на програмните модели за автоматизиране на когнитивни процеси. Стратегии на образователната и научната политика, Vol. 32, № 5s, 2024, ISSN 1310-0270. https://doi.org/10.53656/str2024-5s-24-ana

[4] Казаков Ст. Систематизиране на информационни потоци в логистиката. Годишна университетска научна конференция, НВУ „Васил Левски“, Велико Търново, 2020, с. 1721–1729. ISSN 2367-7481.

[5] Манов Л. Е. Съвременни технологии с изкуствен интелект за разпознаване на обекти с военно предназначение в оптични изображения: Компютърен експеримент с невронни мрежи в MATLAB. DefTech 2025, 2025, с. 714–722. ISSN 2815-4282.

[6] Николов Н. Р., Цанков Ц. С. Хардуерна реализация на генератор на псевдослучайни последователности, описван с полином от 1024 степен, и програмно управление на обратните връзки. Научна сесия 2010, сборник научни трудове, част I, НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, Шумен, 2011, с. 159–163. ISSN 1313-7433.

[7] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, сборник доклади, т. 1, Шумен, 2011, с. 229–232. ISSN 1314-3921.

[8] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[9] 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.

[10] Стоянова, В. Анализ на възможностите за управление по зададен показател с помощта на виртуален гласов асистент. Конференция „Нови предизвикателства пред цифровата икономика (Индустрия 4.0) и ролята на жените в инженерните и технологични области“, София: Звезди, 2020, с. 32–39. ISBN 978-954-8697-83-5.

[11] Николов Н. Р., Беджев Б. Й., Цанков Ц. С. Приложение на изкуствените имунни системи при синтеза на сигнали с оптимални автокорелационни свойства. MATTEX 2016, т. 2, Шумен, 2016, с. 23–29. ISSN 1314-3921.

[12] Wang C.-X., Di Renzo M., Stańczak S., Wang S., Larsson E. G. Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges. IEEE Wireless Communications, Vol. 27, No. 1, 2020, ISSN 1536-1284, DOI: 10.1109/MWC.001.1900292, pp. 16–23.

[13] Yao M., Sohul M., Marojevic V., Reed J. H. Artificial Intelligence-Defined 5G Radio Access Networks. IEEE Communications Magazine, Vol. 57, No. 3, 2019, ISSN 0163-6804, DOI: 10.1109/MCOM.2019.1800629, pp. 14–20.

[14] Ouyang Y., Wang L., Yang A., Shah M., Belanger D., Gao T., Wei L., Zhang Y. The Next Decade of Telecommunications Artificial Intelligence. CAAI Artificial Intelligence Research, Vol. 1, No. 1, 2022, DOI: 10.26599/AIR.2022.9150003, pp. 28–53.

[15] Fu Y., Wang S., Wang C.-X., Hong X., McLaughlin S. Artificial Intelligence to Manage Network Traffic of 5G Wireless Networks. IEEE Network, Vol. 32, No. 6, 2018, DOI: 10.1109/MNET.2018.1800115, pp. 58–64.

[16] Стефанова А. Приложение на изкуствения интелект в обучението по геодезия. Трета национална научно-практическа конференция „Дигитална трансформация на образованието – проблеми и решения“, Русе, 24–25 април 2025, с. 415–419, ISSN 3033-0610, ISSN 3033-0629.

[17] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144. ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[18] Nikolova S., Tsankov Ts. Intelligent resource management systems in computer networks. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, DOI: 10.46687/YT24SIS, pp. 210–220.

[19] Iliev M. P., Nikolov N. R., Tsankov T. Sv. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Electrotechnica & Electronica, Vol. 46, No. 7–8, 2011, pp. 29–33. ISSN 0861-4717.

[20] Nikolova S., Tsankov Ts. Intelligent automated parking infrastructure with integrated AI surveillance and security systems. Annual of Konstantin Preslavsky University of Shumen, Vol. XV E, Faculty of Technical Sciences, 2025, ISSN 1314-8818, DOI: 10.46687/YT25SNC, pp. 256–265.

[21] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.

[22] Tsankov Ts., Konstantinova E. Analyzing security threats in smart homes technology. In: International Scientific Conference “Defense Technologies” DefTech 2020, Shumen, 2020, ISSN 2367-7902, pp. 373–378.

[23] Bedzhev B., Nikolov N., Tsankov Ts. Training artificial immune system using “good” paths for synthesis of signals with optimal autocorrelation properties. In: Scientific Conference with International Participation MATTEH 2018, Conference Proceedings, Vol. 2, Shumen, 2018, ISSN 1314-3921, pp. 3–11.

[24] Staneva, L., Petrov, Y. Generalized Nets and Their Application in the Management of a Recording Studio. Black Sea Journal of Engineering and Transport, Vol. I, 2025, pp. 5–7. ISSN 3033-2885.

[25] Uzun, M. B., Atanasov, V. T. Common conception of software-defined networks. Annual of Konstantin Preslavsky University of Shumen, Vol. XIII E, 2023, pp. 112–119, ISSN 2815-4703 (Online).

STREAMING INFORMATION DATA AND THEIR APPLICATION IN SMART GRID SYSTEMS*

MILEN S. DAVIDKOV, LILIYA A. STANEVA

ABSTRACT: *The paper examines the nature and main characteristics of streaming information data as an important element of modern information and control systems. The processes of generation, transmission, and processing of continuous data streams are analyzed, with particular attention paid to their time dependence, communication latency, transmission reliability, and the need for time synchronization. The specific features of real-time and near-real-time stream processing and the use of time windows for incoming data analysis are presented. The application of streaming information data in Smart Grid systems is considered. Their importance for monitoring the current state of the power system, detecting deviations and events, and supporting control decisions is analyzed.*

KEYWORDS: *data streams, stream processing, Smart Grid, time synchronization, communication latency, information and control systems*

DOI: https://doi.org/10.46687/MT26MSD

ПОТОЧНИ ИНФОРМАЦИОННИ ДАННИ И ПРИЛОЖЕНИЕТО ИМ В SMART GRID СИСТЕМИ

МИЛЕН С. ДАВИДКОВ, ЛИЛИЯ А. СТАНЕВА

АБСТРАКТ: *В доклада са разгледани същността и основните характеристики на поточните информационни данни като важен елемент на съвременните информационно-управляващи системи. Анализирани са процесите на формиране, предаване и обработване на непрекъснати информационни потоци, като е обърнато внимание на времевата им зависимост, комуникационното закъснение, надеждността на предаването и необходимостта от времева синхронизация. Представени са особеностите на поточната обработка в реално и близко до реалното време и използването на времеви прозорци за анализ на постъпващите данни. Разгледано е приложението на поточните информационни данни в интелигентни електроенергийни мрежи Smart Grid. Анализирано е значението им за наблюдението на текущото състояние на електроенергийната система, откриването на отклонения и събития и подпомагането на управляващите решения.*

1 Въведение

Развитието на съвременните информационни и комуникационни технологии води до непрекъснато увеличаване на обема и скоростта на генериране на данни. Все по-голямо значение придобива информацията, постъпваща непрекъснато от множество разпределени източници и изискваща обработване в реално или близко до реалното време. Тези особености определят поточните информационни данни като съществен елемент на съвременните информационно-управляващи системи.

Особено характерно е тяхното приложение в интелигентните електроенергийни мрежи Smart Grid, където множество измервателни устройства, сензори, контролери и комуникационни средства непрекъснато генерират информация за състоянието и динамиката на електроенергийната система. Ефективното използване на тези данни е

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

свързано с изисквания към тяхното своевременно предаване, времева синхронизация, надеждност и обработване.

Целта на настоящия доклад е да бъдат разгледани същността и основните характеристики на поточните информационни данни, процесите на тяхното формиране, предаване и обработване, както и особеностите на приложението им в Smart Grid системи.

Като характерен пример за среда с множество разпределени източници на поточни информационни данни могат да се посочат интелигентните инфраструктурни системи, при които сензори, интелигентни устройства и крайни потребители са свързани чрез обща комуникационна инфраструктура (фиг. 1) [9].



Фиг. 1. Комуникационна инфраструктура и източници на поточни информационни данни в интелигентна енергийна мрежа

Представената на фиг. 1 структура показва разпределения характер на съвременните информационни системи. Данните се генерират едновременно от множество пространствено разпределени източници и посредством комуникационната инфраструктура се предават за последваща обработка и анализ. Това обуславя непрекъснатия характер на информационните потоци и необходимостта от тяхното своевременно приемане, обработване и предаване.

2 Същност и основни характеристики на поточните информационни данни

Поточните информационни данни се формират като непрекъсната последователност от стойности, събития или съобщения, постъпващи от един или множество информационни източници. За разлика от традиционните масиви от данни, при които обработката

обикновено се извършва върху предварително формиран и ограничен набор, поточните данни се характеризират с динамичност и непрекъснатост на постъпването [1], [2].

Потокът от данни може да бъде представен като последователност от информационни елементи

$$D = \{d_1, d_2, ..., d_i, ...\},$$

където всеки елемент d_i съдържа определена стойност или събитие и съответстваща времева характеристика. В общия случай крайната дължина на потока не е предварително известна, тъй като нови данни могат да се генерират непрекъснато в процеса на функциониране на наблюдавания обект или система [1]. Поради това обработването на поточни данни се извършва последователно, непосредствено след тяхното постъпване или в рамките на определени времеви интервали.

Една от основните характеристики на поточните информационни данни е тяхната непрекъснатост. Данните възникват в резултат от протичането на реални процеси и постъпват към информационната система с определена честота. В зависимост от характера на наблюдавания процес потокът може да бъде равномерен, периодичен или събитиен. Следователно интензивността на постъпване не е задължително постоянна и може значително да се изменя във времето.

Съществена характеристика е и неограниченият или предварително неопределеният обем на информационния поток. При продължително функциониране на дадена система количеството генерирани данни постоянно нараства. Това обстоятелство ограничава възможността всички постъпващи данни да бъдат предварително съхранени и едва след това обработени. Необходимо е значителна част от операциите по филтриране, проверка, агрегиране и анализ да се изпълняват непосредствено върху информационния поток.

Поточните данни се характеризират и с висока времева чувствителност. Стойността на даден информационен елемент зависи не само от съдържащата се в него величина, но и от момента, в който тя е възникнала и е станала достъпна за обработване. В тази връзка е необходимо да бъдат разграничени поне два времеви момента – времето на възникване на данните и времето на тяхното приемане от обработващата система. Разликата между тях определя закъснението при предаването и може да бъде съществен показател за пригодността на информацията за използване в реално време.

Наличието на комуникационни закъснения, различна скорост на предаване и временна недостъпност на отделни информационни източници може да доведе до нарушаване на последователността на постъпващите данни. Информационен елемент, генериран по-рано, може да бъде получен след елемент, възникнал в по-късен момент. Следователно редът на приемане невинаги съответства на действителната времева последователност на наблюдавания процес [4]. Това налага използването на времеви маркери и механизми за синхронизация, позволяващи възстановяване на коректната последователност на информационните събития.

Друга съществена особеност е разнородността на поточните данни. В една информационна система могат едновременно да постъпват измерени физически величини, дискретни състояния, диагностични съобщения, алармени събития, управляващи сигнали и други типове информация. Те могат да се различават по формат, структура, единици за измерване, честота на генериране и начин на представяне. Поради това интерпретацията на отделната стойност изисква наличие на съответстващи метаданни, чрез които да бъдат определени нейният източник, тип, времева принадлежност и физически смисъл.

Поточните данни притежават и изразена контекстна зависимост. Една и съща числова стойност може да има различно информационно значение в зависимост от източника, момента на възникване, режима на работа на наблюдавания обект и състоянието на свързаните с него процеси. Поради това отделният информационен елемент не следва да се разглежда изолирано, а като част от времево и логически свързана последователност.

Посочените характеристики определят съществена разлика между поточния и традиционния пакетен подход при обработването на информация. При пакетната обработка анализът се извършва върху вече формиран набор от данни, докато при поточната обработка информационните елементи се приемат и обработват в процеса на тяхното възникване [2], [3]. Това поставя повишени изисквания към скоростта на обработване, времевата синхронизация, устойчивостта при загуба или закъснение на данни и способността на системата да реагира на измененията в наблюдавания процес.

Следователно поточните информационни данни могат да бъдат разглеждани не просто като последователност от отделни стойности, а като динамична информационна структура, развиваща се във времето. Нейната информативност се определя едновременно от съдържанието на отделните елементи, техните времеви характеристики, последователността на възникване, източника и контекста, в който са генерирани. Именно тези особености определят необходимостта от специализирани подходи за тяхното приемане, обработване, оценяване и използване в съвременните информационно-управляващи системи.

3 Формиране, предаване и обработване на поточни информационни данни

Формирането на поточни информационни данни е непосредствено свързано с непрекъснатото наблюдение на състоянието и изменението на процеси, обекти и технически системи. Източници на такива данни могат да бъдат измервателни устройства, сензори, контролери, комуникационни модули, информационни системи и други средства, способни периодично или при настъпване на определено събитие да генерират информационни съобщения. В резултат се създава последователност от данни, която отразява развитието на наблюдавания процес във времето.

В общия случай процесът на формиране и използване на поточните данни може да бъде представен чрез последователността **източник – комуникационна среда – обработваща система – потребител на информацията**. Всеки от тези елементи оказва влияние върху характеристиките и качеството на получаваната информация. Поради това потокът не следва да се разглежда единствено като съвкупност от предавани стойности, а като резултат от взаимодействието между процесите на измерване, преобразуване, предаване и обработване. Обобщената структура на този процес е представена на фиг. 2.

Първичните данни се формират чрез регистриране на определени параметри на наблюдавания обект или процес. В зависимост от предназначението на системата това могат да бъдат физически величини, логически състояния, времеви характеристики, диагностична информация или събития, възникващи в процеса на нейното функциониране. След първоначалното им получаване данните могат да преминат през преобразуване, кодиране, филтриране или предварително агрегиране, преди да бъдат предадени към следващите нива на информационната система.

Съществено значение при поточните данни има **честотата на тяхното генериране**. Тя определя количеството информация, което постъпва в системата за единица време, и съответно необходимите комуникационни и изчислителни ресурси. При повишаване на

честотата на измерване се увеличава възможността за по-точно проследяване на динамиката на наблюдавания процес, но едновременно с това нарастват обемът на предаваните данни и натоварването върху комуникационната инфраструктура.



Фиг. 2. Обобщен модел на формиране, предаване и обработване на поточни информационни данни

За даден интервал от време количеството генерирани информационни елементи може да бъде представено в опростен вид чрез зависимостта

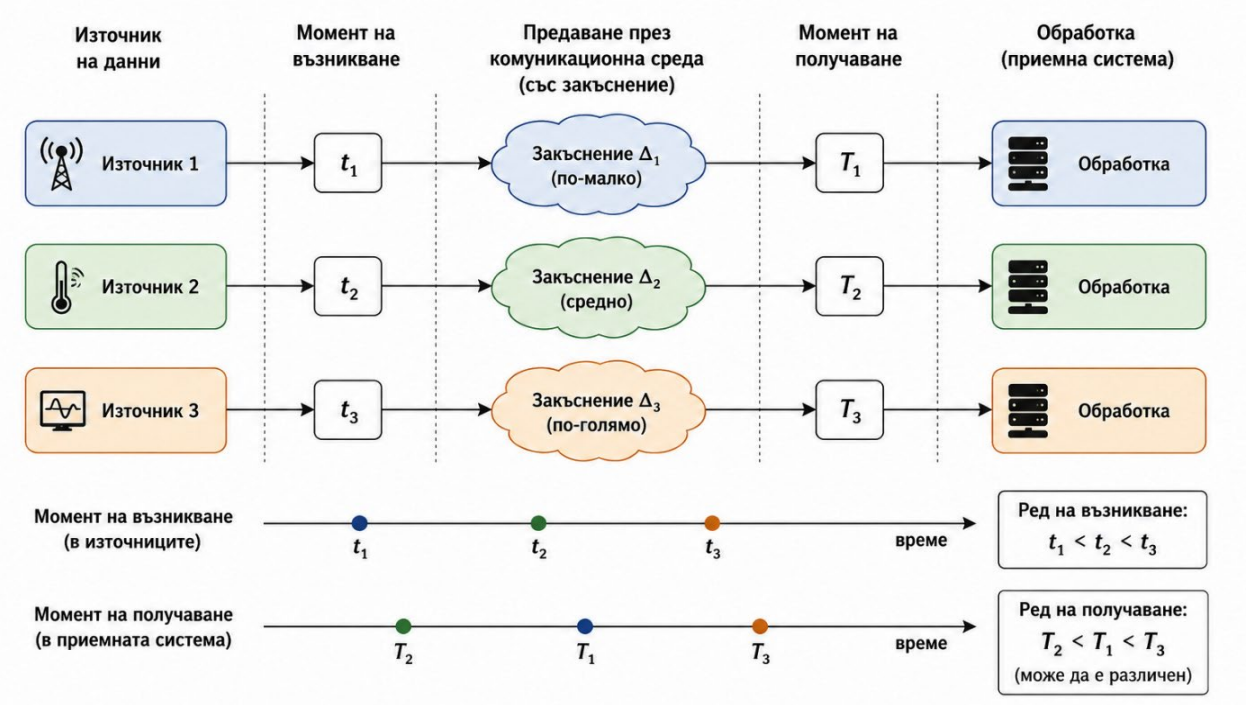
$$N = f_s \cdot T$$

където N е броят на генерираните информационни елементи, f_s – честотата на тяхното формиране, а T – разглежданият времеви интервал. Ако всеки информационен елемент има определен размер, увеличаването на честотата на генериране води непосредствено до нарастване на необходимата пропускателна способност на комуникационния канал.

Предаването на поточните данни представлява критичен етап от тяхното използване. Комуникационната среда трябва да осигури пренасянето на информационните елементи от източника до обработващата система при допустими стойности на закъснението, загубите и нарушенията в последователността. В реални условия тези параметри могат да се изменят

във времето в зависимост от натоварването на мрежата, използваната комуникационна технология и състоянието на отделните нейни компоненти.

Особено значение има **закъснението на информационния поток**, тъй като то определя времето между възникването на дадено събитие и момента, в който информацията за него става достъпна за обработване. Общото закъснение може да се разглежда като резултат от няколко последователни компонента – време за формиране и предварителна обработка на данните, време за предаване, комуникационно закъснение и време за обработване в приемащата система. При системи, функциониращи в реално време, увеличаването на това закъснение може да доведе до намаляване на актуалността и практическата стойност на получената информация. Влиянието на комуникационното закъснение върху момента и последователността на получаване на поточните данни е представено на фиг. 3.



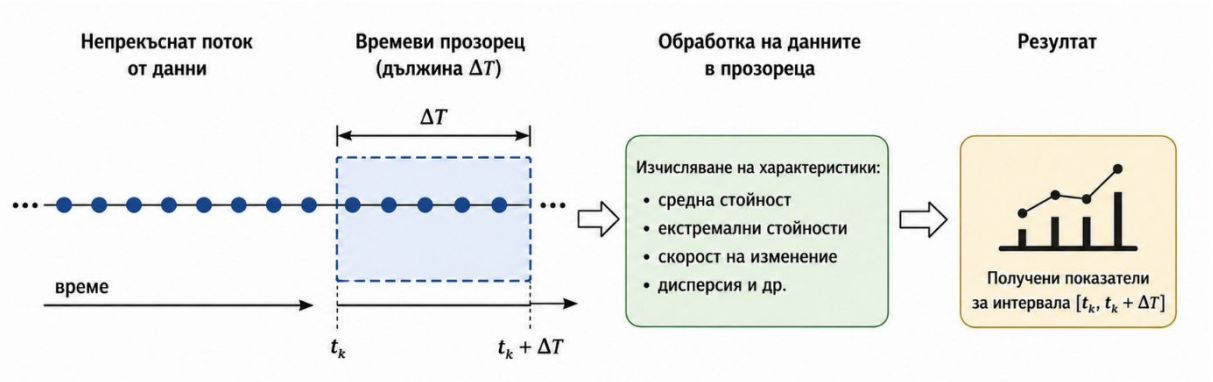
Фиг. 3. Влияние на комуникационното закъснение върху времевата последователност на поточните данни

Наред със закъснението, съществен показател е **надеждността на предаването**. Част от информационните елементи могат да бъдат загубени, повредени или получени извън очакваната последователност. При наличие на множество разпределени източници възниква и необходимост от времева синхронизация, тъй като данните могат да бъдат генерирани и предавани независимо едни от други. Без коректна времева привързаност съпоставянето на стойности от различни източници може да доведе до неправилно представяне на действителното състояние на наблюдавания процес.

След приемането им поточните данни подлежат на **обработване в реално или близко до реалното време** [3]. Основната особеност на този подход е, че обработката се извършва върху постъпващата информация, без да е необходимо предварително да бъде формиран пълният набор от данни. Това позволява своевременно откриване на изменения, отклонения и събития, изискващи реакция от страна на информационната или управляващата система.

Обработването може да включва проверка за коректност, филтриране на шумове и недостоверни стойности, преобразуване на формати, синхронизиране на данни от различни източници, агрегиране и извличане на характеристики. В зависимост от предназначението на системата върху получения информационен поток могат да бъдат прилагани и алгоритми за откриване на събития, оценяване на текущото състояние и прогнозиране на последващото развитие на наблюдавания процес.

Практическо значение има използването на **времеви прозорци**, чрез които непрекъснатият поток се разделя на ограничени множества от информационни елементи [4]. По този начин могат да бъдат определяни средни стойности, екстремуми, скорост на изменение и други характеристики за конкретен времеви интервал. Този подход позволява непрекъснатата последователност от постъпващи данни да бъде обработвана чрез ограничен обем оперативна информация, без да е необходимо цялата история на потока да се съхранява в оперативната памет. Принципът на обработване на непрекъснат информационен поток чрез времеви прозорци е представен на фиг. 4.



Фиг. 4. Обработване на поточни информационни данни чрез времеви прозорци

Важна особеност на поточната обработка е необходимостта от **съгласуване между скоростта на постъпване и скоростта на обработване на данните**. Ако информационните елементи се генерират по-бързо, отколкото системата може да ги обработи, се натрупват необработени данни, увеличава се закъснението и може да се стигне до загуба на информация. Следователно производителността на обработващата система и пропускателната способност на комуникационната инфраструктура трябва да бъдат съобразени с максималната очаквана интензивност на информационния поток.

От тази гледна точка ефективното използване на поточни информационни данни изисква координирано функциониране на всички етапи – от тяхното генериране и времево маркиране до предаването, приемането и последващото обработване. Нарушенията в който и да е от тези етапи могат да повлияят върху пълнотата, актуалността и достоверността на получената информация. Поради това оценяването на информационния поток следва да отчита не само неговия обем, но и времевите, комуникационните и качествените характеристики на данните. Качеството и обработката на информация в интелигентни устройства са разгледани в [7].

Така процесите на формиране, предаване и обработване определят практическата пригодност на поточните данни за използване в информационно-управляващи системи. Особено значение тези процеси придобиват при разпределени технически системи, в които множество информационни източници трябва да бъдат наблюдавани и анализирани практически в реално време. Това създава предпоставки за разглеждане на приложението

на поточните данни в съвременните интелигентни енергийни и комуникационни инфраструктури.

4 Приложение на поточните информационни данни в Smart Grid системи

Развитието на интелигентните електроенергийни мрежи Smart Grid е непосредствено свързано с интегрирането на съвременни комуникационни, измервателни и информационни технологии в процесите по производство, пренос, разпределение и потребление на електрическа енергия [5], [6], [10]. За разлика от традиционните електроенергийни системи, при които информационният обмен има сравнително ограничен характер, Smart Grid предполага непрекъснато взаимодействие между голям брой разпределени технически средства, което поставя съществени изисквания към тяхната оперативна съвместимост [12]. Сред приложните комуникационни стандарти е IEEE 2030.5 за Smart Energy Profile [13]. В резултат се формират значителни по обем и интензивност потоци от данни, които отразяват текущото състояние и динамиката на електроенергийната система.

Основни източници на поточни информационни данни в Smart Grid са интелигентните измервателни устройства, сензорните системи, устройствата за измерване на фазори, защитните устройства, локалните контролери и различните средства за автоматизация и дистанционно наблюдение [8]–[10]. Чрез тях се регистрират стойности на напрежение, ток, активна и реактивна мощност, честота, фазови характеристики, показатели за качеството на електрическата енергия, състояния на комутационни устройства и редица други параметри.

Получаваната информация има различна времева характеристика. Част от данните се генерират периодично през предварително определени интервали, докато други възникват при настъпване на конкретно събитие или изменение на състоянието. Следователно в рамките на една Smart Grid инфраструктура едновременно съществуват информационни потоци с различна честота, обем, приоритет и изисквания към времето за доставка [9]. Това обстоятелство определя необходимостта от диференциран подход при тяхното предаване и обработване.

Особено значение има **оперативната информация**, използвана за наблюдение на текущото състояние на електроенергийната система. При нея стойността на данните е пряко зависима от момента на тяхното получаване. Информация, която точно описва определено състояние, може да загуби част от практическата си стойност, ако бъде получена със значително закъснение. Поради това времевите характеристики на информационните потоци представляват съществен фактор за ефективността на управлението.

В Smart Grid системите поточните данни могат условно да бъдат разделени според тяхното предназначение на **измервателни, оперативни, диагностични и събитийни**. Основните видове поточни информационни данни и тяхното предназначение са систематизирани в табл. 1.

Измервателните потоци съдържат последователности от стойности на наблюдаваните електрически величини. Оперативните данни отразяват текущото състояние на мрежовите елементи и се използват при вземането на управляващи решения. Диагностичната информация позволява оценяване на техническото състояние на оборудването, а събитийните потоци регистрират изменения, аварии, превключвания и други процеси, изискващи своевременна реакция.

Съществена особеност е **разпределеният характер на информационните източници**. Данните могат да се генерират едновременно в различни географски точки на електроенергийната мрежа и да бъдат предавани посредством различни комуникационни

технологии [9]. Вследствие на това моментът на получаване на даден информационен елемент не винаги съответства непосредствено на момента на неговото възникване. Различията в комуникационното закъснение могат да нарушат времевата последователност на информацията и да затруднят формирането на достоверна картина за състоянието на системата.

Таблица 1. Основни видове поточни информационни данни в Smart Grid системи

Вид на данните	Съдържание	Основно предназначение	Времеви изисквания
Измервателни	Напрежение, ток, активна и реактивна мощност, честота, фазови характеристики	Наблюдение и оценка на текущите електрически параметри	Периодично или непрекъснато постъпване
Оперативни	Състояние на мрежови елементи и комутационни устройства	Оперативно управление и подпомагане на управляващи решения	Високи изисквания към актуалността и малко закъснение
Диагностични	Данни за техническото състояние на съоръженията и оборудването	Откриване на отклонения и оценяване на техническото състояние	Според характера на наблюдавания процес
Събитийни	Аварии, превключвания, изменения на състоянието и други събития	Регистриране на събития и осигуряване на своевременна реакция	Критично значение на времето за регистриране и предаване

Поради тази причина **времевата синхронизация** има съществено значение при обработването на поточни данни в Smart Grid. При анализа на информация от множество измервателни точки е необходимо стойностите да бъдат съпоставени спрямо момента, в който са възникнали. Това е особено важно при бързо протичащи преходни процеси, когато дори относително малки времеви отклонения могат да доведат до неправилна интерпретация на последователността и взаимната зависимост между регистрираните събития.

Друг важен фактор е **надеждността на информационния обмен**. Загубата на отделни измервания, временната недостъпност на комуникационния канал или повреждането на информационни съобщения могат да доведат до непълно представяне на наблюдавания процес. При поточната обработка този проблем е особено съществен, тъй като решенията могат да бъдат формирани непосредствено върху текущо постъпващите данни. Следователно системата трябва да разполага с механизми за установяване на липсващи, некоректни или противоречиви информационни елементи.

Поточната обработка създава възможност за **своевременно откриване на отклонения и аномални състояния**. Чрез непрекъснат анализ на постъпващите измервания могат да бъдат установявани резки изменения на електрически величини, отклонения от допустими граници, необичайни зависимости между параметри или последователности от събития, свидетелстващи за възникване на нарушение. По този начин информационният поток се превръща от средство за регистриране на състоянието в основа за оперативна оценка и подпомагане на управленските решения.

Важна област на приложение е и **управлението на разпределени енергийни ресурси**. Интегрирането на възобновяеми енергийни източници, системи за съхранение на енергия, зарядна инфраструктура за електрически превозни средства и активни потребители води до значително увеличаване на броя на информационните източници [10–12]. Същевременно производството и потреблението придобиват по-динамичен характер, което налага по-често актуализиране на информацията за състоянието на системата.

Поточните данни имат съществено значение и при **прогнозирането на натоварването и производството на електрическа енергия**. Натрупването и текущото обработване на времеви последователности позволяват да бъдат идентифицирани тенденции, периодични зависимости и изменения в поведението на отделни потребители или групи потребители. Съчетаването на текущата информация с исторически данни създава възможност за актуализиране на прогнозите в зависимост от настъпващите изменения в реално време.

Особено предизвикателство представлява едновременното обработване на голям брой информационни потоци. При увеличаване на броя на измервателните точки нарастват както общият обем на информацията, така и необходимостта от нейното своевременно анализиране. Това поставя изисквания към мащабируемостта на комуникационната и изчислителната инфраструктура и налага използването на разпределени подходи за обработване на данните.

В този контекст обработката може да бъде извършвана както в централизирани информационни системи, така и в непосредствена близост до източниците на данни. Локалното обработване позволява част от операциите по филтриране, агрегиране и откриване на събития да бъдат извършени преди предаването към по-високо йерархично ниво. По този начин може да бъде намален обемът на комуникационния трафик и времето за реакция при критични изменения в състоянието на системата.

Следователно ефективността на Smart Grid зависи не само от наличието на голям брой измервателни и комуникационни устройства, а в значителна степен от **способността информационните потоци да бъдат своевременно приемани, синхронизирани, оценявани и обработвани**. Качеството на поточните данни и времето, необходимо за тяхното преобразуване в използваема информация, оказват непосредствено влияние върху достоверността на оценката на текущото състояние и възможността за своевременно вземане на управляващи решения.

По този начин поточните информационни данни могат да бъдат разглеждани като един от основните информационни ресурси на интелигентните електроенергийни мрежи. Тяхното ефективно използване създава предпоставки за повишаване на наблюдаемостта, адаптивността и надеждността на електроенергийната система и за преминаване от традиционно наблюдение към динамично управление, основано на актуална информация за протичащите процеси.

5 Заключение

Поточните информационни данни представляват динамична информационна структура, чиито основни характеристики са свързани с непрекъснатото постъпване, времевата зависимост, разнородността и необходимостта от своевременно обработване. Тяхното ефективно използване изисква съгласуване на процесите по генериране, предаване, синхронизиране и обработване, тъй като закъсненията, загубите и нарушенията във времевата последователност могат непосредствено да повлияят върху качеството и достоверността на получаваната информация.

При Smart Grid системите значението на поточните данни се увеличава поради големия брой разпределени информационни източници и необходимостта от непрекъснато наблюдение на състоянието на електроенергийната мрежа. Тяхното своевременно приемане и обработване създава възможност за откриване на отклонения и събития, оценяване на текущото състояние и подпомагане на управляващите решения.

В този смисъл поточните информационни данни могат да се разглеждат като основен информационен ресурс на интелигентните електроенергийни мрежи, чието ефективно използване допринася за повишаване на наблюдаемостта, адаптивността и надеждността на електроенергийната система и създава условия за преминаване към динамично управление, основано на актуална информация за протичащите процеси.

ЛИТЕРАТУРА:

[1] Babcock B., Babu S., Datar M., Motwani R., Widom J. Models and Issues in Data Stream Systems. Proceedings of the Twenty-First ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS '02), ACM, 2002, pp. 1–16.

[2] Golab L., Özsu M. T. Issues in Data Stream Management. ACM SIGMOD Record, Vol. 32, No. 2, 2003, pp. 5–14.

[3] Stonebraker M., Çetintemel U., Zdonik S. The 8 Requirements of Real-Time Stream Processing. ACM SIGMOD Record, Vol. 34, No. 4, 2005, pp. 42–47.

[4] Akidau T., Bradshaw R., Chambers C., Chernyak S., Fernández-Moctezuma R. J., Lax R., McVeety S., Mills D., Perry F., Schmidt E., Whittle S. The Dataflow Model: A Practical Approach to Balancing Correctness, Latency, and Cost in Massive-Scale, Unbounded, Out-of-Order Data Processing. Proceedings of the VLDB Endowment, Vol. 8, No. 12, 2015, pp. 1792–1803.

[5] Amin S. M., Wollenberg B. F. Toward a Smart Grid: Power Delivery for the 21st Century. IEEE Power and Energy Magazine, Vol. 3, No. 5, 2005, pp. 34–41.

[6] Farhangi H. The Path of the Smart Grid. IEEE Power and Energy Magazine, Vol. 8, No. 1, 2010, pp. 18–28.

[7] Denev D., Tsankov Ts. A Survey of Data Quality and Processing of Information in Innovative Smart Devices. 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2022, ISBN 978-1-6654-7625-6, pp. 311–315. https://doi.org/10.1109/ICAI55857.2022.9960040

[8] Moslehi K., Kumar R. A Reliability Perspective of the Smart Grid. IEEE Transactions on Smart Grid, Vol. 1, No. 1, 2010, pp. 57–64. DOI: 10.1109/TSG.2010.2046346.

[9] Gungor V. C., Lu B., Hancke G. P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. IEEE Transactions on Industrial Electronics, Vol. 57, No. 10, 2010, pp. 3557–3564.

[10] Gungor V. C., Sahin D., Kocak T., Ergut S., Buccella C., Cecati C., Hancke G. P. Smart Grid Technologies: Communication Technologies and Standards. IEEE Transactions on Industrial Informatics, Vol. 7, No. 4, 2011, pp. 529–539.

[11] Fang X., Misra S., Xue G., Yang D. Smart Grid – The New and Improved Power Grid: A Survey. IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, 2012, pp. 944–980. DOI: 10.1109/SURV.2011.101911.00087.

[12] Gopstein A., Nguyen C., O'Fallon C., Hastings N., Wollman D. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. NIST Special Publication 1108r4, National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.1108r4.

[13] IEEE. IEEE Std 2030.5-2023 – IEEE Standard for Smart Energy Profile Application Protocol. Institute of Electrical and Electronics Engineers, 2023.

COMPARATIVE ANALYSIS OF MACHINE LEARNING METHODS*

STEFAN M. KAZAKOV

ABSTRACT: *This paper presents a comparative analysis of the major methods and paradigms in machine learning, including supervised, unsupervised, semi-supervised learning, and reinforcement learning. The theoretical foundations, key characteristics, advantages, and limitations of representative algorithms and models are examined, including decision trees, support vector machines, neural networks and deep learning models, ensemble methods, clustering algorithms, and dimensionality reduction techniques. The analysis considers their effectiveness in relation to data characteristics, including dimensionality, volume, structure, and noise, as well as the requirements of specific application domains. Particular attention is given to the trade-offs between predictive accuracy, interpretability, computational efficiency, scalability, and robustness. The ethical aspects of deploying machine learning systems are also addressed, with a focus on transparency, fairness, and algorithmic bias. The comparative analysis confirms that there is no universally optimal machine learning method and that algorithm selection should be guided by the characteristics of the data and the specific requirements of the task. Finally, promising directions for future development are outlined, including AutoML, meta-learning, transfer learning, hybrid and multimodal approaches, and the advancement of explainable and fair artificial intelligence.*

KEYWORDS: *AI, learning methods, clustering algorithms, machine learning*

DOI: https://doi.org/10.46687/MT26SMK

СРАВНИТЕЛЕН АНАЛИЗ НА МЕТОДИТЕ ЗА МАШИННО ОБУЧЕНИЕ

СТЕФАН М. КАЗАКОВ

АБСТРАКТ: *Настоящият доклад представя сравнителен анализ на основните методи и парадигми в машинното обучение, включително контролирано, неконтролирано, полуконтролирано обучение и обучение с подсилване. Разгледани са теоретичните основи, характерните особености, предимствата и ограниченията на представителни алгоритми и модели, сред които дървета на решенията, машини с опорни вектори, невронни мрежи и методи за дълбоко обучение, ансамблови подходи, алгоритми за клъстеризация и техники за намаляване на размерността. Анализът разглежда тяхната ефективност в зависимост от характеристиките на данните, включително размерност, обем, структура и наличие на шум, както и от изискванията на конкретната приложна област. Особено внимание е отделено на компромисите между прогнозна точност, интерпретируемост, изчислителна ефективност, мащабируемост и устойчивост. Разгледани са също етичните аспекти при внедряването на системи за машинно обучение, свързани с прозрачността, справедливостта и алгоритмичните пристрастия. Резултатите от сравнителния анализ потвърждават, че не съществува универсално оптимален метод, а изборът на алгоритъм следва да бъде съобразен с характеристиките на данните и спецификата на поставената задача. В заключение са очертани перспективни направления, включващи AutoML, метаобучение, трансферно обучение, хибридни и мултимодални подходи, както и развитието на обясним и справедлив изкуствен интелект.*

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

1 Въведение

Машинното обучение (МО) се очертава като трансформираща дисциплина, която оформя дълбоко ландшафта на изкуствения интелект (ИИ) и вземането на решения, основани на данни. Разпространението на разнообразни методи за МО – от класически парадигми като контролирано и неконтролирано обучение до съвременни постижения като дълбокото обучение – катализира иновациите в различни области, включително здравеопазване, финанси, обработка на естествен език и компютърно зрение. Тази изследователска работа предоставя цялостен сравнителен анализ на методите за машинно обучение, изяснявайки техните теоретични основи, силни страни, ограничения и емпирична производителност в различни контексти на приложение.

Сравнителната оценка на методите за МО не е просто академично упражнение, а необходимост на практика, тъй като изборът на подходящи алгоритми влияе критично върху точността на модела, интерпретируемостта, мащабируемостта и етичните съображения. Множеството алгоритми за МО, всеки с уникални индуктивни отклонения и изчислителни характеристики, налага строги рамки за оценка. Тази статия систематично разглежда основните семейства методи за машинно обучение – контролирано, неконтролирано, полуконтролирано и обучение с подсилване – заедно с техните представителни алгоритми, като дървета на решенията, машини с опорни вектори, невронни мрежи, техники за клъстериране и ансамбълни подходи.

Базиран на най-новите теоретични и емпирични изследвания, този анализ изследва условията, при които специфични методи се отличават или се провалят, като акцентира върху взаимодействието между характеристиките на данните, алгоритмичната сложност и ограниченията в реалния свят. Дискусията допълнително интегрира перспективите за интерпретируемостта на модела, обобщаемостта, изчислителната ефективност и етичните последици, предлагайки цялостен поглед, релевантен както за академичните изследователи, така и за практици в областта. Подготовката и анализът на таблични данни могат да бъдат подпомогнати чрез динамични масиви в MS Excel (Todorova-Lazarova, 2025).

Приложението на модерни технологични решения и специфични материали в инженерната практика има ключова роля за оптимизацията на ресурсите [11]

2 Теоретични основи на методите за машинно обучение

Дефиниция и таксономия на машинното обучение

Машинното обучение е широко дефинирано като област на изследване, която дава на компютрите способността да учат от данни, без да бъдат изрично програмирани (Mitchell, 1997). Методите за машинно обучение обикновено се категоризират въз основа на наличието на етикетирани данни и естеството на учебната задача. Основните категории включват контролирано обучение, неконтролирано обучение, полуконтролирано обучение и обучение с подсилване (Murphy, 2012).

Методите за контролирано обучение използват етикетирани набори от данни, за да направят извод за съпоставяне от входни характеристики към изходни етикети, обикновено като се занимават с проблеми с класификацията или регресията. Методите за неконтролирано обучение, за разлика от тях, се стремят да открият присъщи структури или модели в немаркирани данни, често чрез техники за клъстериране или намаляване на размерността. Полуконтролираното обучение работи в междинен режим, като използва както етикетирани, така и немаркирани данни. Обучението с подсилване (RL) моделира

последователния процес на вземане на решения, при който агентите се учат да максимизират кумулативните награди чрез взаимодействие с динамична среда (Sutton & Barto, 2018).

Индуктивно отклонение и теоремата за липсата на безплатен обяд

Фундаментално теоретично съображение при сравняването на методите за машинно обучение е концепцията за индуктивно отклонение – наборът от предположения, които обучаващият се алгоритъм прави, за да обобщи отвъд наблюдаваните данни (Mitchell, 1980). Никой обучаващ се алгоритъм не е универсално превъзходен; по-скоро производителността зависи от съответствието между индуктивното отклонение на алгоритъма и основното разпределение на данните. Този принцип е формализиран в теоремата за липсата на безплатен обяд, която твърди, че нито един алгоритъм не се представя най-добре при всички възможни проблеми (Wolpert & Macready, 1997).

Изводът е ясен: сравнителният анализ трябва да вземе предвид съответствието между специфичните за метода предположения (напр. линейност, гладкост, независимост) и характеристиките на целевата област. Той също така подчертава значението на емпиричната валидация и избора на алгоритъм, съобразен с конкретни задачи.

3 Методи за контролирано обучение

Дървета на решенията

Теоретична основа

Дърветата на решенията са йерархични, базирани на правила модели, които рекурсивно разделят пространството от характеристики, за да правят прогнози. Алгоритми като CART (Класификационни и регресионни дървета) изграждат двоични дървета, като избират характеристики и прагове, които максимизират информационния добив или минимизират мерките за примеси, като индекс на Джини или ентропия (Breiman et al., 1984).

Силни страни и ограничения

Дърветата на решенията предлагат интерпретируемост и обработват както числови, така и категорични данни по своята същност. Те са устойчиви на отклонения и липсващи стойности. Дърветата обаче са склонни към свръхнапасване, особено при наличие на дълбоко разклоняване или шумни данни. Техниките за подрязване и ансамбъл разширенията (напр. случайни гори) смекчават тези проблеми, но за сметка на интерпретируемостта (Quinlan, 1993).

Емпирична производителност

Емпиричните изследвания показват, че дърветата на решенията се представят конкурентно върху таблични набори от данни с ясни йерархии на характеристиките, но може да се представят по-слабо върху многомерни или неструктурирани данни (Loh, 2011). Дървета на решенията са прилагани и при анализ на студентски анкетни данни (Kalchev & Tsankov, 2020).

Машини с опорни вектори (SVM)

Теоретична основа

Машините с опорни вектори изграждат хиперплоскости във многомерни пространства, за да разделят класовете с максимален марж. Трикът с ядрото позволява на SVM да моделират нелинейни граници на решения чрез имплицитно картографиране на данни в по-високомерни пространства на характеристики (Cortes & Vapnik, 1995).

Силни страни и ограничения

SVM са ефективни в многомерни пространства и са устойчиви на пренапасване поради свойствата си на регуляризация. Те обработват ефективно малки до средни набори от данни, но се мащабират слабо с големи набори от данни поради изчислителната сложност. Изборът на ядро и хиперпараметри значително влияе върху производителността, което налага внимателен подбор на модела (Cristianini & Shawe-Taylor, 2000).

Емпирична производителност

SVM са демонстрирали най-съвременна производителност в класификацията на текст, биоинформатиката и разпознаването на изображения, особено когато броят на характеристиките надвишава броя на пробите. Мащабируемостта обаче остава практическо предизвикателство (Joachims, 1998).

Невронни мрежи и дълбоко обучение

Теоретична основа

Невронните мрежи са универсални функционални апроксиматори, съставени от взаимосвързани слоеве от изкуствени неврони. Архитектурите за дълбоко обучение, като конволюционни невронни мрежи (CNN) и рекурентни невронни мрежи (RNN), позволяват йерархично извличане на характеристики и моделиране на сложни, нелинейни взаимовръзки (LeCun, Bengio, & Hinton, 2015).

Силни страни и ограничения

Дълбоките невронни мрежи се отличават с превъзходство в обучението на представяния от неструктурирани данни, като изображения, аудио и текст. Способността им да моделират сложни зависимости доведе до пробиви в компютърното зрение, обработката на естествен език и разпознаването на реч. Те обаче изискват големи етикетирани набори от данни, изискват големи изчислителни усилия и страдат от проблеми с интерпретируемостта, често функционирайки като „черни кутии“ (Goodfellow, Bengio, & Courville, 2016).

Емпирична производителност

Моделите за дълбоко обучение са постигнали производителност на човешко или свръхчовешко ниво в бенчмаркове като ImageNet, но тяхната обобщаемост за условия с ниски ресурси или състезателни условия е активна област на изследване (Krizhevsky, Sutskever, & Hinton, 2012).

Ансамблови методи

Теоретична основа

Ансамбловите методи, като bagging, boosting и stacking, комбинират множество базови обучаващи се, за да подобрят прогнозната производителност и устойчивост. Случайните гори обединяват прогнозите на множество дървета на решения, докато алгоритмите за усилване (напр. AdaBoost, Gradient Boosting Machines) последователно обучават моделите, за да коригират грешките на предшествениците (Breiman, 2001; Friedman, 2001).

Силни страни и ограничения

Ансамблите често превъзхождат единичните модели по отношение на точност и обобщаемост поради намаляване на дисперсията и корекция на отклоненията. Те обаче увеличават сложността на модела и изчислителните разходи, а получените модели са по-трудно интерпретируеми.

Емпирична производителност

Случайните гори и машините за усилване на градиента постоянно се нареждат сред най-добрите в състезанията по машинно обучение, особено за структурирани/таблични данни (Caruana & Niculescu-Mizil, 2006).

Методи за неконтролирано обучение

Алгоритми за клъстериране

K-means

K-means е алгоритъм за клъстериране, базиран на центроиди, който разделя данните на k клъстера, като минимизира дисперсията в рамките на клъстера. Неговата простота, ефективност и мащабируемост го правят популярен избор за изследователски анализ на данни (MacQueen, 1967).

K-means обаче приема сферични клъстери с подобен размер и е чувствителен към инициализация и отклонения.

Йерархично клъстериране

Йерархичното клъстериране изгражда дървовидна дендрограма, представляваща вложени групировки от точки от данни въз основа на показатели за сходство. Не изисква спецификация на броя на клъстерите, но има по-висока изчислителна сложност (Jain, Murty, & Flynn, 1999).

Гаусови смесени модели (GMM)

GMM моделират данните като смес от Гаусови разпределения, което позволява меко клъстериране, където точките имат вероятностни клъстерни принадлежности. За оценка на параметрите се използва метод на максимизиране на очакванията (EM). GMM са гъвкави, но могат да бъдат чувствителни към инициализация и склонни към пренареждане с високоразмерни данни (Bishop, 2006).

Намаляване на размерността

Техниките за намаляване на размерността, като анализ на главните компоненти (PCA) и t-разпределено стохастично вграждане на съседи (t-SNE), проектират данни в по-нискоразмерни пространства, като същевременно запазват дисперсията или локалната структура (Jolliffe, 2002; van der Maaten & Hinton, 2008).

PCA е линеен и интерпретируем, но може да пропуска нелинейни зависимости. t-SNE се отличава с визуализацията на високомерни данни, но е изчислително интензивен и неподходящ за последващо прогнозно моделиране.

Емпирични сравнения

Емпиричните изследвания показват, че няма универсален доминиращ метод за клъстеризация; производителността зависи от формата, мащаба и характеристиките на шума на данните (Xu & Wunsch, 2005). По подобен начин, полезността на методите за намаляване на размерността зависи от линейността и присъщата размерност на данните.

Полу-контролирано обучение

Полу-контролираното обучение (SSL) използва както етикетирани, така и немаркирани данни, като се справя със сценарии, при които етикетираните примери са оскъдни или скъпи за получаване. Методите включват самообучение, съвместно обучение и трансдуктивно обучение (Zhu & Goldberg, 2009).

SSL се основава на предположения като хипотези за гладкост, клъстерност и многообразие, които, ако бъдат нарушени, могат да влошат производителността. На практика обаче SSL е показало обещаващи резултати в области като обработката на естествен език и компютърното зрение, където немаркираните данни са в изобилие (Chapelle, Scholkopf, & Zien, 2006).

Обучение с подсилване

Обучението с подсилване (RL) моделира ученето като процес на вземане на решения на Марков (MDP), при който агентите взаимодействат със средата, за да максимизират очакваните кумулативни награди (Sutton & Barto, 2018).

Моделно-базирано срещу моделно-свободно RL

Моделно-базираните RL алгоритми изучават експлицитен модел на средата и планират действия съответно, докато моделите без модел изучават политики или функции на стойност директно от опита. Последните, включително Q-обучение и методи на градиент на политики, са постигнали впечатляващи резултати в области като игри и роботика (Mnih et al., 2015).

Предизвикателства и сравнения

RL е изправен пред предизвикателства, включително неефективност на извадките, компромиси между изследване и експлоатация и спецификация на наградите. В сравнение с контролираните и неконтролираните методи, RL алгоритмите изискват активно

взаимодействие със средата, което може да бъде скъпо или рисковано в реални приложения (Kober, Bagnell, & Peters, 2013).

4 Сравнителен анализ на различните методи

Прогностична производителност

Сравнителните изследвания показват, че алгоритмичната производителност зависи от характеристиките на данните, включително размерност, шум и размер на извадката. Например, моделите за дълбоко обучение се отличават с високомащабни, високоразмерни, неструктурирани данни (напр. изображения, текст), докато SVM и ансамбъл методите често се представят по-добре със средно големи, структурирани набори от данни (Caruana & Niculescu-Mizil, 2006).

Нито един метод не е еднакво превъзходен; емпиричният бенчмаркинг и кръстосаната валидация остават от съществено значение за избора на модел (Fernández-Delgado et al., 2014). Отделно направление е създаването на контролирани синтетични изображения за сравнение между човешкото и компютърното зрение (Manov, 2026).

Интерпретируемост

Интерпретируемостта е критично съображение, особено в области с висок залог, като здравеопазването и правото. Дърветата на решенията и линейните модели предлагат прозрачност и лекота на обяснение, докато дълбоките невронни мрежи и ансамблите са известни с непрозрачността си (Doshi-Velez & Kim, 2017).

Компромисът между точност и интерпретируемост е текущ фокус на изследванията, като подходи като дестилация на модели, механизми за внимание и методи за пост-хок обяснение се стремят да преодолеят разликата.

Мащабируемост и изчислителна ефективност

Мащабируемостта разграничава методите за машинно обучение по отношение на способността им да обработват големи набори от данни и многомерни пространства. Методите за дълбоко обучение и ансамбъл изискват значителни изчислителни ресурси, включително графични процесори и разпределени системи, докато по-простите модели (напр. линейна регресия, K-средни стойности) са по-ефективни, но може да им липсва предсказваща сила при сложни задачи (Dean et al., 2012). Пример за паралелна изчислителна инфраструктура е клъстерната система в среда MPI (Станев, Николов и Цанков, 2011).

Устойчивост и обобщение

Устойчивостта към шум, отклонения и състезателни примери все повече се признава за жизненоважна за внедряването на модели за машинно обучение в реални условия. Ансамбълните методи и регуларизираните модели (напр. SVM с подходящи ядра) предлагат подобрено обобщение, докато дълбоките невронни мрежи са податливи на състезателни атаки и преобучение, ако не са правилно регуларизирани (Goodfellow, Shlens, & Szegedy, 2015).

Пригодност на приложната област

Пригодността на методите за машинно обучение варира в зависимост от областта. Например, дърветата на решенията и ансамблите се използват широко във финансите за кредитно оценяване, докато дълбокото обучение доминира в разпознаването на изображения и реч. RL е постигнало забележителен успех в автономния контрол и играта, но е по-слабо разпространено в области, в които липсва интерактивна среда.

Етични и обществени съображения

Сравнителната оценка на методите за машинно обучение се простира отвъд техническите показатели, за да обхване етичните и обществените въздействия. Моделите „черна кутия“ оспорват отчетността и прозрачността, пораждайки опасения относно справедливостта, пристрастията и дискриминацията (Barocas & Selbst, 2016). Изборът на метод влияе не само върху точността на прогнозиране, но и върху капацитета за човешки надзор и смекчаване на вредите.

Последните изследвания се застъпват за алгоритмични одити, интерпретируемост по проект и обучение, съобразено с справедливостта, за да се гарантира отговорно внедряване на системи за машинно обучение (Mehrabi et al., 2021).

Бъдещи насоки в сравнителните изследвания на машинното обучение

Автоматизирано машинно обучение (AutoML)

Рамките на AutoML целят да автоматизират избора, състава и оптимизирането на ML тръбопроводи, демократизирайки достъпа до най-съвременни модели. Сравнителните изследвания все повече използват AutoML за сравняване на алгоритми при стандартизирани условия (Feurer et al., 2015).

Метаобучение и трансферно обучение

Метаобучението, или „учене за учене“, се стреми да подобри избора и адаптирането на алгоритми въз основа на предишен опит. Трансферното обучение позволява повторното използване на предварително обучени модели в различни задачи, особено полезно в области с ограничени данни (Pan & Yang, 2010). Трансферът на знания е разгледан и при разпознаване на частично видими обекти (Манов, 2025). Друг пример за адаптивно търсене е обучаемата имунна система за синтез на сигнали (Беджев, Николов и Цанков, 2018).

Хибридни и мултимодални подходи

Хибридните методи, комбиниращи символно и субсимволично обучение, и мултимодалните модели, които интегрират различни типове данни, представляват обещаващи пътища за преодоляване на ограниченията на отделните методи (Kiela et al., 2018).

Обяснимо и справедливо машинно обучение

Изследванията върху обяснимостта и справедливостта движат разработването на нови методи, които балансират прогнозната производителност с обществените ценности.

Разработват се сравнителни рамки за оценка не само на технически показатели, но и на етични критерии (Doshi-Velez & Kim, 2017).

5 Заключение

Пейзажът на методите за машинно обучение е богат и многостранен, обхващащ спектър от алгоритми с различни теоретични основи, силни страни и ограничения. Сравнителният анализ подчертава, че нито един метод не е универсално оптимален; по-скоро ефикасността зависи от съответствието между алгоритмичните допускания, характеристиките на данните и изискванията на приложението.

Дърветата на решенията и ансамблите предлагат интерпретируемост и висока производителност върху структурирани данни, докато машините с опорни вектори се отличават в многомерни настройки. Моделите за дълбоко обучение революционизираха анализа на неструктурирани данни, но изискват големи набори от данни и изчислителни ресурси. Неконтролираните и полуконтролираните методи са незаменими, когато етикетите са оскъдни, а обучението с подсилване е уникално подходящо за последователни задачи за вземане на решения.

Освен предсказуемата точност, съображенията за интерпретируемост, мащабируемост, устойчивост и етични последици са от първостепенно значение при избора и внедряването на методи. Напредъкът в AutoML, мета-обучението и обяснимия изкуствен интелект обещава допълнително усъвършенстване на сравнителните рамки, улеснявайки отговорното и ефективно приложение на машинното обучение в различни области.

Текущите изследвания трябва да продължат да оценяват и внедряват иновации в методите за машинно обучение, като гарантират, че тяхното приемане се ръководи не само от техническите умения, но и от обществената полза и етичната почтеност.

ЛИТЕРАТУРА:

[1] Беджев Б. Й., Николов Н. Р., Цанков Ц. С. Обучаема изкуствена имунна система използваща „добри“ пътища за синтез на сигнали с оптимални автокорелационни свойства. MATTEX 2018, т. 2, част 2, Шумен, 2018, с. 3–11. ISSN 1314-3921.

[2] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[3] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, сборник доклади, т. 1, Шумен, 2011, с. 229–232. ISSN 1314-3921.

[4] Barocas, S., & Selbst, A. D. (2016). Big data’s disparate impact. California Law Review, 104(3), 671–732.

[5] Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.

[6] Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.

[7] Breiman, L., Friedman, J. H., Olshen, R. A., & Stone, C. J. (1984). Classification and regression trees. Wadsworth.

[8] Caruana, R., & Niculescu-Mizil, A. (2006). An empirical comparison of supervised learning algorithms. In Proceedings of the 23rd International Conference on Machine Learning (pp. 161–168). ACM.

[9] Chapelle, O., Scholkopf, B., & Zien, A. (2006). Semi-supervised learning. MIT Press.

[10] Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20(3), 273–297.

[11] Cristianini, N., & Shawe-Taylor, J. (2000). An introduction to support vector machines and other kernel-based learning methods. Cambridge University Press.

[12] Dean, J., Corrado, G., Monga, R., Chen, K., Devin, M., Le, Q. V., … & Ng, A. Y. (2012). Large scale distributed deep networks. In Advances in Neural Information Processing Systems (pp. 1223–1231).

[13] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.

[14] Enimanev, I. (2023). Design of Passive Buildings with Environmentally Friendly Materials. KNOWLEDGE - International Journal, Vol. 58.3, pp. 505–511

[15] Fernández-Delgado, M., Cernadas, E., Barro, S., & Amorim, D. (2014). Do we need hundreds of classifiers to solve real world classification problems? Journal of Machine Learning Research, 15, 3133–3181.

[16] Feurer, M., Klein, A., Eggensperger, K., Springenberg, J. T., Blum, M., & Hutter, F. (2015). Efficient and robust automated machine learning. In Advances in Neural Information Processing Systems (pp. 2962–2970).

[17] Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189–1232.

[18] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[19] Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. In International Conference on Learning Representations.

[20] Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: A review. ACM Computing Surveys, 31(3), 264–323.

[21] Joachims, T. (1998). Text categorization with support vector machines: Learning with many relevant features. In European Conference on Machine Learning (pp. 137–142). Springer.

[22] Jolliffe, I. T. (2002). Principal component analysis (2nd ed.). Springer.

[23] Kiela, D., Bulat, L., Clark, S., & Clark, S. (2018). Learning multi-modal representations. In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Tutorials (pp. 1–6).

[24] Kober, J., Bagnell, J. A., & Peters, J. (2013). Reinforcement learning in robotics: A survey. International Journal of Robotics Research, 32(11), 1238–1274.

[25] Kalchev K., Tsankov Ts. Use of the Decision Tree Method in Analysis of Student Data from Surveys. Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of Technical Sciences, 2020, ISSN 1311-834X, pp. 72–75.

[26] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. In Advances in Neural Information Processing Systems (pp. 1097–1105).

[27] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.

[28] Loh, W. Y. (2011). Classification and regression trees. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 1(1), 14–23.

[29] Manov L. E. Creation of a parametrically controlled synthetic image dataset of Ishihara-like plates for comparing human and computer vision. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2026, National Military University, 2026. ISSN 2815-4282.

[30] MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability (pp. 281–297). University of California Press.

[31] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM Computing Surveys, 54(6), 1–35.

[32] Mitchell, T. M. (1980). The need for biases in learning generalizations. Technical Report CBM-TR-117, Rutgers University.

[33] Mitchell, T. M. (1997). Machine learning. McGraw-Hill.

[34] Murphy, K. P. (2012). Machine learning: A probabilistic perspective. MIT Press.

[35] Pan, S. J., & Yang, Q. (2010). A survey on transfer learning. IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345–1359.

[36] Todorova-Lazarova, V. P. Dynamic Arrays in MS Excel for Data Processing and Analysis in Information Systems. International Scientific Conference UNITECH 2025, Gabrovo, 2025, pp. 1–6, ISSN 1313-230X.

[37] Quinlan, J. R. (1993). C4.5: Programs for machine learning. Morgan Kaufmann.

[38] Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). MIT Press.

[39] van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. Journal of Machine Learning Research, 9, 2579–2605.

[40] Wolpert, D. H., & Macready, W. G. (1997). No free lunch theorems for optimization. IEEE Transactions on Evolutionary Computation, 1(1), 67–82.

[41] Xu, R., & Wunsch, D. (2005). Survey of clustering algorithms. IEEE Transactions on Neural Networks, 16(3), 645–678.

[42] Zhu, X., & Goldberg, A. B. (2009). Introduction to semi-supervised learning. Morgan & Claypool Publishers.

CYBERSECURITY OF INTELLIGENT VIDEO SURVEILLANCE SYSTEMS WITH ARTIFICIAL INTELLIGENCE*

SILVIA H. NIKOLOVA

ABSTRACT: *AI-enabled video surveillance requires protection of both digital infrastructure and the semantic validity of automated decisions. This paper proposes a layered architecture that combines device identity, authenticated communication, model provenance, cross-sensor verification and controlled incident response. A conditional risk model distinguishes successful compromise from undetected operational impact. A reproducible analytical example examines sensor dependence and shows why redundant channels cannot be assumed independent. A validation protocol links cybersecurity outcomes to detection quality, latency and service continuity. The contribution is an integrated engineering framework and evaluation method; the numerical results are illustrative calculations, not measurements from a deployed system.*

KEYWORDS: *video surveillance, artificial intelligence, cybersecurity, adversarial machine learning, zero trust, cyber resilience*

DOI: https://doi.org/10.46687/MT26SHI

КИБЕРСИГУРНОСТ НА ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА ВИДЕОНАБЛЮДЕНИЕ С ИЗКУСТВЕН ИНТЕЛЕКТ

СИЛВИЯ Х. НИКОЛОВА

АБСТРАКТ: *Интелигентното видеонаблюдение изисква защита както на цифровата инфраструктура, така и на достоверността на автоматизираните решения. Предлага се многослойна архитектура, която обединява идентичност на устройствата, защитена комуникация, проследимост на моделите, междусензорна проверка и управляема реакция при инциденти. Условен модел на риска разграничава успешното компрометиране от неоткритото оперативно въздействие. Възпроизводим аналитичен пример изследва зависимостта между резервирани канали. Разработена е методика за оценяване чрез показатели за сигурност, разпознаване, закъснение и непрекъсваемост. Приносът е инженерна рамка и метод за проверка; числените резултати са илюстративни изчисления, а не измервания от внедрена система.*

1 Въведение

Видеонаблюдението с изкуствен интелект (ИИ) преобразува видеопотоците в оперативни решения: откриване на проникване, проследяване на обекти и приоритизиране на тревоги. Компрометирането на такава система може да засегне едновременно информационната сигурност и физическата защита на наблюдавания обект. Валиден цифров подпис на потока не доказва, че алгоритъмът правилно интерпретира заснетата сцена.

Целта на доклада е да разработи цялостен подход за защита на веригата „сензор–модел–решение–оператор“. Изследователският въпрос е как техническите контроли и проверката на AI решенията да ограничават неоткритият пропуск, без да нарушават

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

навременността на охранителната реакция. Обхватът включва IP камери, гранични изчислителни устройства, система за управление на видео (VMS) и център за наблюдение.

2 Научна основа и постановка на проблема

Класическата защита на мрежови устройства и устойчивостта на машинното обучение разглеждат различни механизми на отказ. NIST AI 100-2 E2025 систематизира атаките според етапа от жизнения цикъл, целите, знанията и възможностите на противника [18]. За видеонаблюдението особено значение имат манипулирането на входа при експлоатация, отравянето на обучаващи данни, внедряването на скрито поведение и извличането на чувствителна информация.

Thys, Van Ranst и Goedemé демонстрират физически противникови изображения, които могат да затруднят разпознаването на хора [5]. Това показва, че наблюдаваната сцена също е вход за атака: не е задължително противникът да придобива административен достъп. Резултатите са специфични за изследваните детектори и условия; пренасянето им към друга камера, компресия, дистанция или осветеност изисква отделна проверка.

BadNets показва възможността модел да работи нормално върху обичайни данни и да проявява нежелано поведение при специален входен признак [6]. Следователно високото качество върху стандартен тестов набор не е достатъчно доказателство за отсъствие на скрити зависимости. Защитата трябва да обхваща произхода на теглата, данните, средата за обучение и процедурата за одобряване на версията.

Робастното обучение формулира защитата като оптимизация спрямо допустими противникови смущения [7]. Практическата му стойност зависи от съответствието между използвания модел на атака и реалните условия. Athalye, Carlini и Wagner показват, че затрудненото изчисляване на градиента може да създаде привидна устойчивост [8]. Поради това оценяването трябва да включва адаптивни проверки и ясно описан достъп на тестовия противник.

DetectorGuard предлага формални гаранции срещу локализирани атаки за скриване на обекти в рамките на определен модел на заплаха [9]. Гаранцията е условна спрямо допусканията на метода и не обхваща автоматично откраднати идентификационни данни, подменен фърмуер или прекъсване на захранването. Това различие мотивира съчетаването на AI защита с мрежови, организационни и експлоатационни контроли.

На инфраструктурно равнище NIST SP 800-207 поставя акцент върху проверката на субекта и устройството преди достъп до ресурс, без автоматично доверие поради мрежово местоположение [10]. NISTIR 8259A дава базови способности за сигурност на IoT устройства [11]. Анализът на Mirai илюстрира последствията от масово компрометиране на свързани устройства [12]. Тези източници подкрепят необходимостта камерата да бъде управляван цифров актив, а не пасивен периферен елемент. Сигурността на интелигентни IoT структури и уязвимостите на безжични мрежи са разгледани в [3, 21]. Използването на инструменти за прихващане и анализ на мрежови пакети е предмет на [4].

Принос и граници на разработката

Предложеният принос е интеграционен: общ модел на заплахите; архитектура с контролирани граници на доверие; условна оценка на остатъчния риск; протокол за съвместно изпитване на киберсигурност и охранителна ефективност. Не се предлага нов алгоритъм за разпознаване и не се претендира за експериментално доказано превъзходство. Работната хипотеза е, че разнообразни и проверими защитни механизми ограничават неоткритото въздействие по-ефективно от формално резервиране на сходни компоненти.

Разработката използва критичен литературен обзор, архитектурен синтез и детерминистичен анализ на чувствителността. Числените допускания са зададени изрично. Това позволява повторение на изчисленията и замяна на примерните стойности с данни от конкретен обект при последващо валидиране.

3 Модел на системата и заплахите

Системата се представя като ориентиран граф G = (V, E), където V включва сензори, обработващи възли, регистри на модели, операторски станции и архиви, а E описва потоците от видео, метаданни и команди. Всеки възел има собственик, идентичност, версия, разрешени взаимодействия и допустимо време за възстановяване. Границата на доверие се пресича при всяка промяна на административната отговорност или начина на обработка.

Защитаваните активи са оригиналният видеозапис, метаданните за събития, ключовете и сертификатите, конфигурациите, теглата на моделите и журналите. Освен конфиденциалност, цялостност и наличност се изискват свежест на данните, проследимост на произхода и семантична достоверност. Последната означава, че изводът съответства на реалното събитие в рамките на предварително определена област на приложение.

Разграничават се външен мрежов противник, лице с физически достъп до сцената, компрометиран доставчик и вътрешен потребител с прекомерни права. За всеки сценарий се задава дали са достъпни само входове и изходи, частична информация за модела или пълни параметри. Не се допуска по подразбиране едновременно компрометиране на всички възли; общите зависимости се анализират отделно.

Таблица 1 свързва представителни заплахи с проверими проявления. Тя служи като основа за тестове, а не като изчерпателен каталог на уязвимости. Едно проявление може да има както злонамерена, така и техническа причина, поради което сигналът за аномалия не е самостоятелно доказателство за атака.

Таблица 1. Заплахи, последствия и доказателства за контрол

Повърхност	Сценарий / последствие	Проверимо доказателство
Устройство	Чужд фърмуер; загуба на контрол	Проверена версия и защитено обновяване
Комуникация	Повторен поток; скрита промяна в сцената	Идентичност, ред и свежест на съобщенията
Визуален вход	Противников мотив; пропуск на човек	Проверка с независим сензор и оператор
Модел / данни	Отравяне или скрит тригер	Произход, тестов набор, одобрена версия
VMS / API	Злоупотреба с права; изтичане на записи	Одит на достъпа и разрешенията
Инфраструктура	Претоварване; закъсняла тревога	Измерена опашка и време до уведомяване

Критичен сценарий за физическа охрана

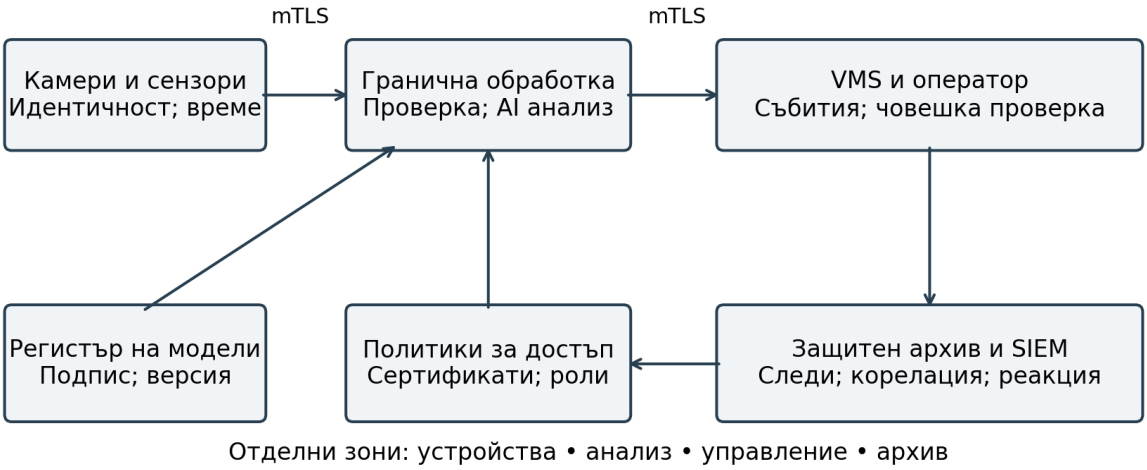
При охрана на периметър нарушител навлиза в зона, но операторът получава стар кадър или AI моделът пропуска човека. Мрежовата връзка може да изглежда активна и сървърът да е технически наличен. Затова оперативният отказ се определя като липса на

достоверна тревога в допустимото време, а не само като спиране на камерата. Този критерий свързва киберсигурността с реалната задача на охраната.

Общи причини за отказ са споделен комутатор, един доставчик на модели, общ часовник, захранване или административен акаунт. Две камери с еднакъв модел и сходна гледна точка не осигуряват независимост. Карта на зависимостите трябва да предшества оценката на резервирането и избора на допълнителни сензори.

4 Предложена защитна архитектура

Архитектурата на фиг. 1 разделя събирането, анализа, управлението и съхраняването на данни. Потокът от камерата преминава през проверка на идентичността, свежестта и допустимия формат преди AI обработка. Политиките се прилагат на границите между зоните. Моделите се разпространяват чрез отделен регистър, а събитията за сигурност се изпращат към защитен журнал и система за корелация (SIEM). Пример за паралелна изчислителна инфраструктура е клъстерната система в среда MPI [2].



Фиг. 1. Архитектура с отделени потоци за данни, модели и управление

На устройствено равнище се задават уникални идентификатори, премахват се неизползваните услуги и се ограничават интерфейсите за администрация. Обновяването изисква удостоверен пакет, проверка за съвместимост и възможност за възстановяване до одобрена версия. Защитеното зареждане и апаратното съхраняване на ключове се включват при поддръжка от конкретното устройство. Липсваща способност се документира като ограничение, а не се приема за налична.

Между съвместими компоненти се използва взаимно удостоверяване чрез TLS (mTLS), с управление на сертификатите и ограничени права на услугите. ONVIF Profile T включва възможности за HTTPS стрийминг, но съвместимостта с профила не доказва, че всяка инсталация реално използва защитен режим [13]. Проверява се договореният транспорт. Наследени устройства могат да бъдат изолирани зад защитен шлюз, като незащитеният участък остава изрично посочен остатъчен риск.

Граничният възел валидира последователността на кадрите и маркира прекъсвания, застиване на изображението и разминаване между сензори. Времевите марки се комбинират с номера на съобщенията и състояние на сесията; само синхронизиран часовник не е

достатъчен срещу повторение. Статична сцена не се обявява автоматично за подмяна, защото охранявани зони могат дълго да остават неподвижни.

Операторският интерфейс показва източника, времето, версията на модела и причината за тревогата. При невалидна идентичност потокът се поставя под карантина и незабавно се обозначава загубеното покритие. При визуална несигурност се запазва наблюдението и се активира проверка. Автоматичната изолация се съобразява с резервния канал, за да не създаде сама незащитен периметър.

Архивът отделя оригиналните доказателствени материали от копията за анализ. Контролът на достъпа, криптирането и записът на действията защитават съдържанието след приемане. Хардуерни реализации на генератори на псевдослучайни последователности за криптографски приложения са представени в [1, 20]. Хешът удостоверява непромененост спрямо конкретно състояние, но не доказва истинността на сцената или липсата на компрометиране преди изчисляването му.

5 Математически модел на риска и реакцията

Нека A_i означава опит за атака от сценарий i в фиксиран времеви прозорец. Нека $a_i = P(A_i)$, $b_i = P(B_i \mid A_i)$ е вероятността за пробив при опит, а $m_i = P(M_i \mid A_i, B_i)$ е вероятността въздействието да остане неоткрито до крайния срок. Тогава вероятността за неоткрито успешно въздействие е:

$$p_i = a_i \cdot b_i \cdot m_i \,. \tag{1}$$

Равенство (1) следва от правилото за условни вероятности и не изисква независимост между трите събития. При L_i – средна условна загуба за съответния изход, очакваната загуба се оценява чрез:

$$R = \sum_i p_i L_i \,. \tag{2}$$

Сумата е приложима за неприпокриващи се категории загуби или след премахване на двойното отчитане. При последователна атака върху общ актив се моделират съвместните събития. Вероятностите се оценяват за еднакъв хоризонт, а L_i се измерва в съгласувани единици. Експертна степен „висок риск“ не може директно да се замести като статистическа вероятност.

5.1. Зависимост между каналите за проверка

Нека q_1 и q_2 са условните вероятности два канала да пропуснат едно и също опасно събитие след пробив. При правило „тревога от поне един канал“ крайният пропуск е съвместен пропуск. За бернулиеви индикатори с допустим коефициент на корелация ρ:

$$m = q_1 q_2 + \rho \sqrt{[q_1(1 - q_1)q_2(1 - q_2)]} \,. \tag{3}$$

Стойността трябва да удовлетворява границите $\max(0, q_1 + q_2 - 1) \le m \le \min(q_1, q_2)$. При $q_1 = q_2 = q$ формулата се свежда до $m = \rho q + (1 - \rho)q^2$. Изводът е, че резервирането намалява риска само доколкото вторият канал предоставя допълнителна информация. Корелацията се оценява условно за съответния сценарий, а не върху смес от всички нормални и аварийни записи.

5.2. Оперативен индикатор и времеви ограничения

За текущ прозорец се дефинира индикатор $s_t = \sum_j w_j z_{j,t}$, където $z_{j,t} \in [0,1]$ са нормализирани признаци за мрежова аномалия, несъгласуваност на сензорите, нарушена свежест и необичайно поведение на модела; $w_j \ge 0$ и $\sum_j w_j = 1$. Това е оценка за приоритизиране, не калибрирана вероятност. Невалиден подпис или отнет сертификат

задейства отделно твърдо правило и не се компенсира от ниски стойности на останалите признаци.

$$T_{общо} = T_{прием} + T_{проверка} + T_{AI} + T_{сливане} + T_{известяване} \leq T_{доп} . \quad (4)$$

Прагът за предупреждение τ_1 и прагът за ескалация τ_2 се избират върху отделна валидационна извадка при $\tau_1 < \tau_2$. За връщане в нормален режим се използва по-нисък праг и минимално време на стабилност. Така се избягва често превключване. Ограничението (4) се проверява за висок персентил на закъснението, защото приемливата средна стойност може да скрива опасни редки забавяния.

6 Защита на моделите и оперативен жизнен цикъл

AI моделът се управлява като версиониран компонент с проверим произход. За всяка версия се съхраняват идентификатор, хеш, източник на теглата, конфигурация на предварителната обработка, зависимости и резултати от одобрени тестове. Подписването защитава целостта на пакета и идентифицира подписващия; то не гарантира отсъствие на отравяне или скрито поведение. Решението за внедряване трябва да включва и независима проверка на качеството.

SSDF описва практики за сигурна разработка през жизнения цикъл [14]. За разглежданата система се предлага те да се конкретизират чрез отделяне на среди за обучение и експлоатация, контрол на промените, минимални права на автоматизираните процеси и одобряване на зависимостите. Автоматичното самообучение от непроверени експлоатационни записи не се допуска: обратната връзка се поставя в карантинен набор и се оценява преди включване в обучение.

За данните се води произход на записите, основание за употреба, версия на анотациите и история на корекциите. Разделянето на обучение, валидация и тест трябва да е по обекти или времеви периоди. Съседни кадри от един клип в различни извадки създават изтичане на информация и завишават оценката. Проверяват се дублирани сцени, необичайни анотации и концентрирани промени в редки класове.

Робастното обучение и входните преобразувания се използват само след измерване на ефекта върху реалните класове и условия. Защитата се тества срещу противник, който познава приложеното преобразуване. Премахването на високочестотен шум например може едновременно да намали някои смущения и да заличи малък далечен обект. Следователно промяната се оценява спрямо пропуснати събития, а не само спрямо визуалния вид на кадъра.

Обяснимостта подпомага техническото разследване. Grad-CAM предоставя визуални обяснения чрез локализация на области, свързани с изхода на невронната мрежа [15]. Подобна карта може да насочи оператора към необичайна зависимост, но не доказва вярност или устойчивост. В предложения процес тя е допълнение към оригиналния запис, сензорните данни и журналите, а не критерий за автоматично оправдаване на решение.

Алгоритъм за обработка на събития

Алгоритъмът изпълнява последователно удостоверяване, оценка на качеството, AI анализ, сливане и избор на реакция. При недостъпен сензор се записва липсваща стойност, а не нулева опасност. Операторът получава отделни известия за охранително събитие и за намалено доверие в наблюдението. Така техническата повреда не се прикрива като нормална сцена.

Вход: кадър x_t, метаданни u_t, сензори v_t, одобрен модел M.

Ако идентичността или целостта са невалидни: карантина; тревога за покритие.

Иначе: проверка на свежестта; извличане на признаци z_t; анализ чрез M.
Изчисли s_t; съпостави детекциите със сензорите и разрешената зона.
При $s_t \geq \tau_2$: ескалирай; активирай резервна проверка и запази доказателства.
При $\tau_1 \leq s_t < \tau_2$: предупреди оператора и увеличи наблюдението.
При валидна охранителна тревога: изпрати я независимо от нисък s_t.
Запиши решение, причина, версия и време; възстанови след проверка.

При обновяване се използва ограничено пробно внедряване, последвано от разширяване само при изпълнени критерии. Връщането към предишна версия е разрешено единствено към одобрен пакет, който не е оттеглен поради уязвимост. След инцидент се преглеждат както техническата причина, така и пропуските в процеса на одобряване [16].

7 Методика за експериментално валидиране

Предлага се изолиран стенд с IP камери, граничен сървър, VMS, регистър на модели, независим сензор и централизирани журнали. Точният хардуер, резолюция, кадрова честота, кодек, версия на детектора и ускорител се фиксират преди изпитването. Методиката е предназначена за бъдещо валидиране; в настоящия доклад не се твърди, че стендът е реализиран или че са проведени измервания.

Сравняват се три конфигурации: C0 – базова система с обичайни мрежови контроли; C1 – C0 плюс идентичност, сегментация и проверка на свежестта; C2 – C1 плюс управление на модела, междусензорна проверка и адаптивна реакция. За коректно сравнение входните сцени, моделът и хардуерният ресурс се запазват еднакви, освен когато конкретният компонент е предмет на контролирано изменение.

Тестовите сцени обхващат нормално движение, реално проникване, ниска осветеност, закриване на обект и техническо прекъсване. Към тях се добавят контролирани киберсценарии: невалидна идентичност, повторен поток, неодобрена версия на модел и визуално противниково въздействие. Изпитванията се извършват само в разрешената среда. За физическите проверки се описват дистанция, ъгъл и видим размер на обекта. Разпознаването на частично видими обекти, включително чрез трансфер на знания, е разгледано в [23–25].

Таблица 2. Показатели и правила за измерване

Показател	Определение	Практически смисъл
Recall на събития	TP / (TP + FN)	Открити реални проникванията
Лъжливи тревоги	Брой за камера·час	Натоварване на оператора
Успех на атака	Успешни / допустими опити	Отделно за всеки сценарий
p95 закъснение	95-и персентил до тревога	Навременност на реакцията
Полезна наличност	Време с валидна функция / общо време	Работещо охранително покритие
Време за възстановяване	До проверена работна конфигурация	Практическа устойчивост

Единицата за анализ е събитие или независим клип, а не всеки кадър. Предварително се задават правило за съпоставяне с еталонната анотация, времеви толеранс и обработка на повторни тревоги. За атака срещу детектор се отчита и условният успех върху обектите, които базовата система разпознава без въздействие. Така естествените пропуски не се приписват погрешно на противника.

Конфигурациите се изпитват върху едни и същи сцени в балансиран ред. За пропорции се докладват брой опити и интервали на неопределеност; при групирани данни

се използва преизвадка по клипове или обекти. Само за независими бернулиеви събития приблизителният най-неблагоприятен размер за точност ±0,05 при 95% доверие е $n \approx 1{,}96^2 \cdot 0{,}25/0{,}05^2 = 385$. Зависимите кадри не изпълняват това допускане.

Аблационният анализ изключва последователно проверката на свежестта, втория сензор и контрола на версията. Критериите за приемане се задават предварително: допустим спад на recall, лимит на лъжливите тревоги и краен срок за известяване според охранявания обект. Общ резултат без разделяне по сценарии може да прикрие критичен неуспех и не е достатъчен за приемане.

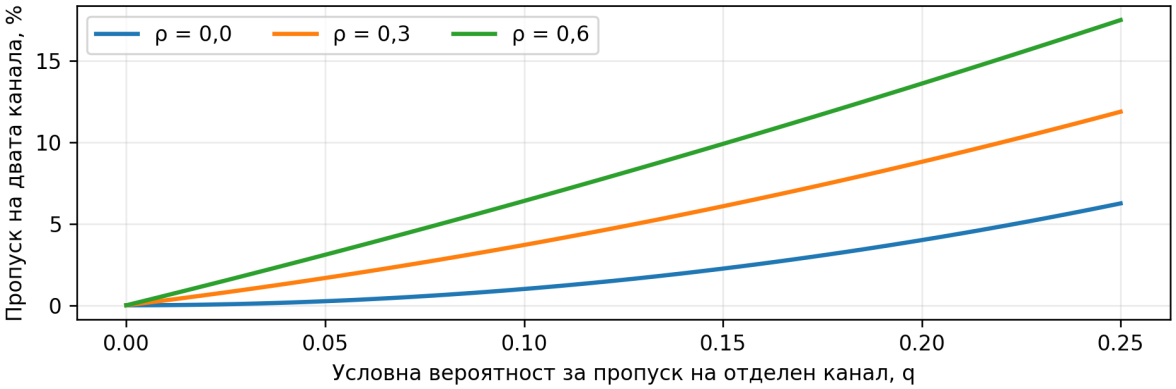
8 Аналитичен пример и чувствителност

Разглежда се един условен сценарий за фиксиран оценъчен прозорец. Приемат се a = 0,20, b = 0,30 и загуба L = 100 условни единици. Двата проверяващи канала имат еднаква вероятност за пропуск q = 0,15 след пробив. Стойностите са избрани за демонстрация и не произхождат от реална инсталация, статистика за атаки или експеримент. Формули (1)–(3) определят всички резултати.

Таблица 3. Изчислен остатъчен риск при примерните допускания

Конфигурация	m	p = 0,06m	R = 100p
Един канал	0,15000	0,009000	0,9000
Два канала; ρ = 0	0,02250	0,001350	0,1350
Два канала; ρ = 0,3	0,06075	0,003645	0,3645
Два канала; ρ = 0,6	0,09900	0,005940	0,5940

При независими пропуски $m = 0{,}15^2 = 0{,}0225$ и относителното намаление спрямо един канал е 85%. При ρ = 0,3 намалението е 59,5%, а при ρ = 0,6 – 34%. Това са следствия от зададения модел, а не доказана ефективност на конкретна технология. При ρ = 1 двата еднакви канала не дават подобрение по този показател.



Фиг. 2. Чувствителност на съвместния пропуск към q и ρ; аналитични криви

Фигура 2 показва, че положителната зависимост отслабва ползата от резервирането. За q = 0,15 производната $\partial m/\partial \rho = q(1 - q)$ е 0,1275. Увеличение на ρ с 0,1 повишава m с 0,01275, а R – с 0,0765 условни единици при останалите допускания. Следователно измерването на зависимостта може да бъде по-полезно от добавяне на втори идентичен детектор.

Правилото „тревога от поне един канал“ има цена: ако f_1 и f_2 са независими вероятности за лъжлива тревога в един и същ отрицателен прозорец, обединената вероятност е $f_1 + f_2 - f_1 f_2$. При $f_1 = f_2 = 0{,}01$ тя става 0,0199. В реалната система зависимостта се проверява отделно и за лъжливите тревоги. Намаленият пропуск трябва да се съпостави с времето и капацитета за операторска проверка.

Изчисленията подкрепят конкретен проектен избор: допълнителният канал да различава физическата модалност или начина на отказ, например видеодетекция и периметров сензор. Ползата остава условна, ако двата канала използват обща комуникация или захранване. За практическо решение примерните a, b, q и ρ трябва да бъдат заменени с локални оценки и интервали на неопределеност.

9 Обсъждане, приложимост и ограничения

Основният резултат от анализа е разграничаването между технически работеща инфраструктура и надеждна охранителна функция. Криптираният видеопоток може да съдържа подвеждаща сцена; провереният модел може да работи извън обучаващото разпределение; достъпният сървър може да обработва тревогите прекалено бавно. Затова приемането на системата изисква съвместно изпитване на достъп, данни, модел и оперативна реакция.

Практическото внедряване започва с инвентаризация на устройства и зависимости, следвана от ограничаване на административния достъп и проверка на защитения транспорт. Следва управление на версиите и добавяне на междусензорна проверка за най-критичните зони. При ограничен бюджет се приоритизират контроли с проверим ефект върху конкретен сценарий.

Автоматичната реакция трябва да е пропорционална. Изключването на подозрителна камера ограничава разпространението на инцидента, но може да премахне единствения поглед към зона. Предложеният подход изисква едновременно известяване за загубено покритие и активиране на резервна процедура. Възстановяването включва валидиране на конфигурацията и тест на охранителната функция, а не само рестартиране на устройството. Управлението на инциденти се свързва с целия процес на управление на риска [16, 22].

9.1. Лични данни и отчетност

Видеозаписите могат да съдържат лични данни, а AI анализът да създава допълнителни чувствителни изводи. Насоките на Европейския комитет по защита на данните за видео устройства разглеждат необходимостта, пропорционалността и прозрачността на обработването [17]. За конкретно внедряване се определят цел, основание, срок на съхранение и роли за достъп. Автоматизираното вземане на решения в контекста на GDPR е разгледано в [19]. Оценка на въздействието се прави, когато е приложима спрямо характера и риска на обработването.

Предлага се изпращане на минимално необходимите метаданни и ограничаване на достъпа до необработено видео. За разследване се запазва контролиран оригинал, а за обучение – отделно разрешено копие. Псевдонимизацията намалява свързваемостта, но не означава автоматично анонимност. Описаните мерки са инженерна рамка, а не удостоверение за нормативно съответствие.

9.2. Ограничения и бъдеща работа

Докладът не представя реализиран стенд, набор от измервания или сравнение на търговски продукти. Условният вероятностен модел опростява динамиката на противника и не включва всички последователни зависимости. Следващият етап е изпитване по раздел

7, включително комбинирани откази и продължителна експлоатация, с публикуване на анонимизирани анотации и точни конфигурации.

10 Заключение

Предложена е интегрирана рамка за киберсигурност на видеонаблюдение с ИИ, която обединява защитена инфраструктура, проследим жизнен цикъл на модела и проверка на оперативните решения. Формализиран е рискът от неоткрито въздействие, а аналитичният пример показва значението на зависимостта между резервирани канали. Разработената методика позволява бъдеща оценка чрез пропуски, лъжливи тревоги, закъснение и полезна наличност. Приложимостта към конкретен обект следва да се потвърди с измервания при предварително зададени критерии за приемане.

ЛИТЕРАТУРА:

[1] Николов Н. Р., Цанков Ц. С. Хардуерна реализация на генератор на псевдослучайни последователности, описван с полином от 1024 степен, и програмно управление на обратните връзки. Научна сесия 2010, сборник научни трудове, част I, НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, Шумен, 2011, с. 159–163. ISSN 1313-7433.

[2] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, сборник доклади, т. 1, Шумен, 2011, с. 229–232. ISSN 1314-3921.

[3] Стоянова, В. Интернет на нещата – анализ на сигурността при интелигентни структури. II International Scientific Conference CONFSEC, Borovets, 2018, Year 2, Issue 2 (4). ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[4] 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.

[5] Thys S., Van Ranst W., Goedemé T. Fooling automated surveillance cameras: adversarial patches to attack person detection. CVPR Workshops, 2019. arXiv:1904.08653. https://arxiv.org/abs/1904.08653

[6] Gu T., Dolan-Gavitt B., Garg S. BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. arXiv:1708.06733, 2017, revised 2019. https://arxiv.org/abs/1708.06733

[7] Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A. Towards Deep Learning Models Resistant to Adversarial Attacks. ICLR, 2018. https://arxiv.org/abs/1706.06083

[8] Athalye A., Carlini N., Wagner D. Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples. ICML, 2018. https://arxiv.org/abs/1802.00420

[9] Xiang C., Mittal P. DetectorGuard: Provably Securing Object Detectors against Localized Patch Hiding Attacks. ACM CCS, 2021. https://arxiv.org/abs/2102.02956

[10] Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207, 2020. DOI: 10.6028/NIST.SP.800-207.

[11] Fagan M., Megas K., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. NISTIR 8259A, 2020. DOI: 10.6028/NIST.IR.8259A.

[12] Antonakakis M. et al. Understanding the Mirai Botnet. 26th USENIX Security Symposium, 2017, pp. 1093–1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[13] ONVIF. Profile T: Advanced Video Streaming. https://www.onvif.org/profiles/profile-t/ (достъп: 08.09.2026).

[14] Souppaya M., Scarfone K., Dodson D. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST SP 800-218, 2022. DOI: 10.6028/NIST.SP.800-218.

[15] Selvaraju R. R., Cogswell M., Das A., Vedantam R., Parikh D., Batra D. Grad-CAM: Visual Explanations from Deep Networks via Gradient-based Localization. ICCV, 2017. https://arxiv.org/abs/1610.02391

[16] NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3, 2025. DOI: 10.6028/NIST.SP.800-61r3.

[17] European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices. Version 2.0, 2020. https://www.edpb.europa.eu/documents/guideline/guidelines-32019-on-processing-of-personal-data-through-video-devices_en (достъп: 08.09.2026).

[18] Vassilev A., Oprea A., Fordyce A., Anderson H., Davies X., Hamin M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2 E2025, 2025. DOI: 10.6028/NIST.AI.100-2e2025.

[19] Simeonova I. How GDPR treats automated decision-making. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2025, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 164–175. https://doi.org/10.46687/jsar.v29i1.461

[20] Iliev M. P., Nikolov N. R., Tsankov T. Sv. Hardware implementation of the shrinking-multiplexing generator of pseudo-random sequences. Electrotechnica & Electronica, Vol. 46, No. 7–8, 2011, pp. 29–33. ISSN 0861-4717.

[21] Nikolov, L. G. Wireless Network Vulnerabilities Estimation. Security & Future, Vol. 2, No. 2, 2018, pp. 80–82, ISSN 2535-0668 (Print), ISSN 2535-082X (Online).

[22] Dimanova, D., Kuzmanov, Z. Risk Management in Information Security. Conference Proceedings MATTEH 2018, Vol. 2, Part 1, Information, Technical and Economical Problems of Security Systems, Shumen, 2018, pp. 139–145, ISSN 1314-3921.

[23] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[24] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения. DefTech 2025, 2025, с. 723–731. ISSN 2815-4282.

[25] Манов Л., Кулев Н. Откриване и разпознаване на частично видими обекти в оптични изображения с използване на техниките на изкуствения интелект – мини ревю от 1970 г. до 2000 г. DefTech 2023, 2023, с. 444–450. ISSN 2815-4282.

DISTRIBUTED PARALLEL IMPLEMENTATION OF A MULTICRITERIA MODEL FOR STREAMING DATA QUALITY ASSESSMENT*

KOSTADIN D. KOSTADINOV, MILEN S. DAVIDKOV

ABSTRACT: *A distributed parallel implementation of a multicriteria model for assessing the quality of streaming data is presented. The quality of each incoming data record is described by seven normalized components: accuracy, completeness, timeliness, validity, consistency, provenance and reliability. The components are calculated independently by separate computing nodes and are subsequently combined by a coordinating node into an integral quality score. Context-dependent weights reflect the importance of the individual indicators under different operating conditions. Critical thresholds are additionally introduced to prevent a dangerously low component value from being compensated for by the remaining indicators. A formal model for distributing the component tasks, synchronizing the partial results and estimating the parallel processing time is developed. An illustrative numerical example demonstrates the calculation of speedup and parallel efficiency. The proposed approach is suitable for scalable real-time data quality control in distributed Edge–Fog–Cloud environments.*

KEYWORDS: *streaming data, data quality, multicriteria assessment, parallel processing, Edge–Fog–Cloud*

DOI: https://doi.org/10.46687/MT26KDK

РАЗПРЕДЕЛЕНА ПАРАЛЕЛНА РЕАЛИЗАЦИЯ НА МНОГОКРИТЕРИАЛЕН МОДЕЛ ЗА ОЦЕНЯВАНЕ КАЧЕСТВОТО НА ПОТОЧНИ ДАННИ

КОСТАДИН Д. КОСТАДИНОВ, МИЛЕН С. ДАВИДКОВ

АБСТРАКТ: *Представена е разпределена паралелна реализация на многокритериален модел за оценяване качеството на поточни данни. Качеството на всеки постъпващ информационен запис се описва чрез седем нормализирани компонента: точност, пълнота, навременност, валидност, съгласуваност, проследимост и надеждност. Компонентите се изчисляват независимо в отделни изчислителни възли, след което се обединяват от координиращ възел в интегрална оценка на качеството. Използват се контекстно изменяеми тегла, които отразяват значимостта на отделните показатели при различни режими на работа. Допълнително се въвеждат критични прагове, които не позволяват опасно ниската стойност на определен компонент да бъде компенсирана от останалите показатели. Разработен е формален модел за разпределяне на компонентните задачи, синхронизиране на частичните резултати и определяне на времето за паралелна обработка. Чрез илюстративен числен пример са показани изчисляването на ускорението и ефективността на паралелната реализация. Предложеният подход е приложим за мащабируем контрол на качеството на данните в разпределени Edge–Fog–Cloud среди.*

1 Въведение

Съвременните измервателни, комуникационни и управляващи системи обработват непрекъснато постъпващи данни от множество разпределени източници. За разлика от

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

данните, съхранявани в традиционни информационни масиви, поточните данни трябва да бъдат приети, проверени и оценени в ограничен времеви интервал. Закъснението, липсващите стойности, неправилният формат или несъответствието между свързани измервания могат непосредствено да повлияят върху резултатите от обработката и върху вземаните управленски решения.

Качеството на данните не може да бъде определено достатъчно точно само чрез един показател. Международният стандарт ISO/IEC 25012 представя качеството като съвкупност от характеристики, чието значение зависи от предназначението на данните и от изискванията на конкретната информационна система [3–7]. При поточните данни особено значение имат точността, пълнотата, навременността, валидността, съгласуваността, проследимостта и надеждността. Всяка от тези характеристики описва различна страна на качеството и изисква собствен начин за изчисляване.

Допълнително затруднение възниква поради голямата скорост на постъпване на данните. Последователното изчисляване на всички показатели може да увеличи времето за обработка и да предизвика натрупване на необработени записи. Това е особено неблагоприятно при системи, работещи в реално време, при които дори правилна, но закъсняла информация може да бъде практически неизползваема. Изследванията върху системите за поточна обработка показват необходимостта изчисленията да се извършват в рамките на ограничени времеви прозорци и с контролирано използване на изчислителните ресурси [8, 9].

Независимото определяне на отделните характеристики на качеството създава възможност изчисленията да бъдат разпределени между няколко работни възела. Принципът за разпределяне на задачи и обмен на резултати между изчислителни възли е използван при разработването на клъстерни системи, работещи в MPI среда [13]. Прилагането му към оценяването на качеството на поточни данни позволява отделните показатели да бъдат изчислявани паралелно, след което резултатите да бъдат обединени от координиращ възел.

Подобна организация съответства и на съвременните Edge–Fog–Cloud архитектури. Част от проверките могат да се изпълняват непосредствено до информационния източник, по-сложните зависимости могат да се анализират във Fog възли, а дългосрочните модели и архивите могат да се поддържат в Cloud среда [10, 11]. По този начин се намалява количеството на предаваните необработени данни и се съкращава времето за получаване на оценката.

Целта на настоящия доклад е да бъде разработена разпределена паралелна реализация на многокритериален модел за оценяване качеството на поточни данни. За постигането на тази цел се определят структурата на поточния информационен запис, компонентите на качеството, начинът за разпределяне на изчислителните задачи, правилата за синхронизиране и обединяване на частичните резултати и зависимостите за оценяване на времето, ускорението и ефективността на паралелната обработка.

2 Многокритериален модел за оценяване

За формалното описание на процеса нека е зададено множество от информационни източници

$$\mathcal{S} = \{S_1, S_2, \dots, S_n\}, \tag{1}$$

където всеки източник S_i генерира последователност от поточни информационни записи. Източниците могат да бъдат измервателни устройства, програмируеми контролери, комуникационни модули, информационни системи или други компоненти, които предават данни към системата за обработка.

Поточният информационен запис, получен от източника S_i в момент t, се представя чрез:

$$x_i(t) = \langle v_i(t), t_{e,i}, t_{a,i}, m_i(t), \tag{2}$$

където:
$v_i(t)$ – стойността на полученото измерване или информационен параметър;
$t_{e,i}$ – моментът на възникване на информацията при източника;
$t_{a,i}$ – моментът на приемане на записа от системата;
$m_i(t)$ – множество от метаданни, свързани със записа.

Метаданните могат да съдържат идентификатор на източника, тип на измерването, мерна единица, комуникационен канал, местоположение, версия на използвания алгоритъм, техническо състояние на устройството и сведения за извършените преобразувания. По този начин поточният запис се разглежда не само като отделна числова стойност, а като структуриран информационен обект, съдържащ необходимите данни за последващо оценяване на неговото качество.

За всеки поточен информационен запис xi(t) се определя многокомпонентен вектор на качеството:

$$Q_i(t) = \left[q_{A,i}(t), q_{C,i}(t), q_{T,i}(t), q_{V,i}(t), q_{S,i}(t), q_{P,i}(t), q_{R,i}(t)\right], \tag{3}$$

където:
$q_{A,i}(t)$ – оценка на точността;
$q_{C,i}(t)$ – оценка на пълнотата;
$q_{T,i}(t)$ – оценка на навременността;
$q_{V,i}(t)$ – оценка на валидността;
$q_{S,i}(t)$ – оценка на съгласуваността;
$q_{P,i}(t)$ – оценка на проследимостта;
$q_{R,i}(t)$ – оценка на надеждността.

Индексът i показва информационния източник, а аргументът t отчита момента, за който се извършва оценяването. Включването им в означенията позволява качеството да бъде проследявано отделно за всеки източник и да се отчита изменението му във времето.

Всички компоненти се нормализират в интервала:

$$0 \le q_{j,i}(t) \le 1, \qquad j \in \{A, C, T, V, S, P, R\}, \tag{4}$$

където стойност 0 означава напълно непригодни данни по съответния показател, а стойност 1 – максимално възможно качество. Нормализирането позволява да се сравняват и обединяват показатели с различен физически смисъл и различни методи за изчисляване. Повишаването на точността на измерванията при работа с технологични модули е разгледано в [1]. Подобен подход за оценяване е приложим и при обработката на информация от интелигентни устройства [14].

След изчисляването на отделните компоненти те се обединяват в интегрална оценка на качеството на поточния информационен запис:

$$Q_{\Sigma,i}(t) = \sum_{j\in J} w_j(t) q_{j,i}(t), \qquad J = \{A, C, T, V, S, P, R\}, \tag{5}$$

при изпълнение на условията:

$$w_j(t) \geq 0, \qquad \sum_{j\in J} w_j(t) = 1, \tag{6}$$

Във формула (5) $Q_{\Sigma,i}(t)$ е интегралната оценка на качеството на записа от източника S_i, $q_{j,i}(t)$ е стойността на съответния компонент, а $w_j(t)$ е неговото тегло. Теглата определят относителното значение на отделните характеристики при конкретния режим на работа.

Стойността на интегралната оценка принадлежи на интервала:

$$0 \leq Q_{\Sigma,i}(t) \leq 1, \tag{7}$$

По-високата стойност на $Q_{\Sigma,i}(t)$ показва по-високо общо качество на оценявания запис. Теглата могат да се изменят във времето според вида на данните, режима на работа, критичността на наблюдавания процес и изискванията към управленското решение.

Интегралната оценка може да прикрие критично ниска стойност на отделен показател. Поради това за всеки компонент се задава минимално допустим праг θ_j. Общият индикатор за риск се определя чрез:

$$R_i(t) = \max_{j\in J}\left\{I\left[q_{j,i}(t) < \theta_j\right]\right\}. \tag{8}$$

Тук $I[\cdot]$ е индикаторна функция, която приема стойност 1 при изпълнено условие и стойност 0 в останалите случаи. Когато $R_i(t) = 1$, поне един компонент е под допустимия праг и поточният информационен запис се определя като рисков независимо от неговата интегрална оценка. При $R_i(t) = 0$ всички минимални изисквания са изпълнени.

3 Разпределена паралелна реализация

За паралелното изчисляване на компонентите нека е зададено множество от налични изчислителни възли:

$$N = \{p_1, p_2, \dots, p_m\},$$

а множеството на компонентните задачи е:

$$(J = \{A, C, T, V, S, P, R\}).$$

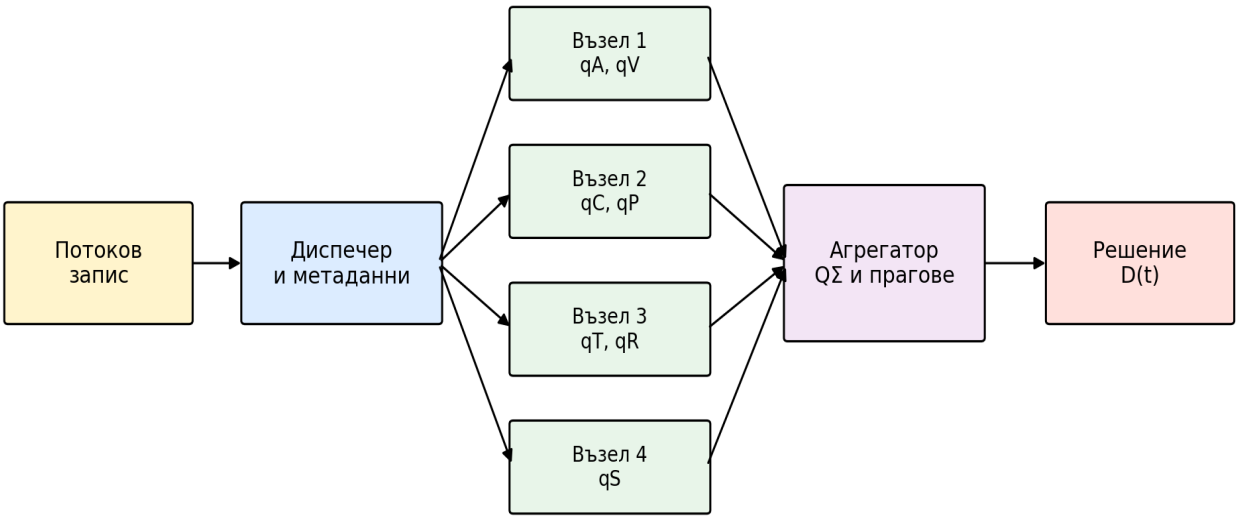
Всяка задача от множеството J съответства на изчисляването на един компонент от вектора на качеството. Разпределението на задачите между възлите се описва чрез двоичната променлива a_{jk}, която приема стойност 1, когато компонентът j се изчислява във възела n_k, и стойност 0 в останалите случаи.

Основното условие за разпределение е:

$$a_{jk} \in \{0,1\}, \qquad \sum_{k=1}^{m} a_{jk} = 1, \qquad j \in J\,. \tag{9}$$

Формула (9) гарантира, че всяка компонентна задача се разпределя към точно един изчислителен възел. Един изчислителен възел може да обработва повече от една компонентна задача, когато това се налага от броя на наличните възли, тяхното натоварване или избраната схема за разпределение.

Разпределената система включва диспечер, работни възли и агрегатор. Диспечерът приема поточния информационен запис, определя необходимите входни данни за всеки компонент и изпраща задачите към съответните възли. Работните възли изчисляват независимо възложените им показатели, а агрегаторът събира получените резултати, формира вектора на качеството и определя интегралната оценка.



Фиг. 1. Разпределена схема за паралелно оценяване на качеството

Всеки частичен резултат се предава към агрегатора заедно с идентификатора на информационния запис и означение на използвания времеви прозорец. Това не позволява обединяването на стойности, които принадлежат на различни записи или са получени в различни моменти. Агрегаторът изчаква необходимите компоненти, проверява тяхната съвместимост и едва след това изчислява интегралната оценка.

При закъснение или отказ на работен възел съответната задача може да бъде пренасочена към друг свободен възел. Пренасочването не променя математическата зависимост за изчисляване на компонента, а само мястото на нейното изпълнение. По този начин се повишава устойчивостта на системата и се намалява вероятността един отказ да прекъсне цялостното оценяване.

Ефективността на паралелната реализация зависи от равномерното натоварване на възлите. Затова задачите не трябва да се разпределят единствено според техния брой, а и според очакваното време за изчисляване, количеството на предаваните данни и наличните ресурси на всеки възел. Управлението на ресурси в компютърни индустриални мрежи е разгледано в [2]. Разпределянето на задачите е свързано и с организацията на

комуникационния обмен, тъй като количеството и структурата на предаваните данни влияят върху общото време за обработка [15, 16].

Таблица 1. Компонентни задачи при оценяване качеството на поточни данни

Компонент	Основни входни данни	Начин на оценяване	Подходящо ниво за обработка
Точност	Данни от калибрация, прогнозни и свързани измервания	Определя се отклонението от еталонна, прогнозна или изчислена стойност	Fog или Cloud
Пълнота	Очакван и действително получен брой записи	Определя се делът на получените спрямо очакваните записи	Edge или Fog
Навременност	Момент на възникване и момент на приемане	Оценява се комуникационното и обработващото закъснение	Edge
Валидност	Формат, тип, мерна единица и допустим диапазон	Проверява се изпълнението на предварително зададени правила	Edge
Съгласуваност	Свързани измервания и балансови зависимости	Сравняват се стойности, които трябва да удовлетворяват обща физическа или логическа зависимост	Fog
Проследимост	Идентификатори, история на обработката и метаданни	Проверява се възможността записът да бъде проследен до неговия източник	Fog или Cloud
Надеждност	Техническо състояние, история на отказите и диагностични данни	Оценява се вероятността източникът да функционира правилно	Cloud

Представеното разпределение не е задължително и може да се изменя според структурата и натоварването на конкретната система. Проверките за валидност и навременност изискват сравнително малко изчислителни ресурси, но трябва да бъдат извършени непосредствено след постъпването на записа. Поради това е целесъобразно те да бъдат разположени в Edge слоя.

Оценяването на точността и съгласуваността обикновено изисква сравнение с други измервания, прогнозни модели или балансови зависимости. Тези операции могат да бъдат изпълнявани във Fog възли, които разполагат с информация от няколко свързани източника. Оценките за проследимост и надеждност могат да използват по-продължителна история и затова част от тяхната обработка може да бъде извършвана в Cloud слоя.

Независимо от мястото на изпълнение, всички частични резултати се представят в нормализирания интервал от 0 до 1. Това позволява агрегаторът да ги обработва по единен начин и да прилага общите тегла и критични прагове.

4 Оценка на изчислителното време

Времето за обработка на един поточен информационен запис зависи от продължителността на отделните компонентни задачи, обмена на данни между възлите и обединяването на получените резултати. Нека T_j е времето, необходимо за изчисляване на компонента j, а T_a – времето за формиране на интегралната оценка и проверка на критичните прагове.

При последователна обработка всички компонентни задачи се изпълняват една след друга. Общото време се определя чрез:

$$T_{\text{seq}} = \sum_{j \in J} T_j + T_a \ . \tag{10}$$

При паралелна обработка отделните задачи се разпределят между наличните възли. Продължителността на компонентната обработка се определя от възела с най-голямо сумарно натоварване. Към това време се добавят времето за комуникация T_{comm} и времето за агрегация T_a:

$$T_{par} = \max_{1 \le k \le m} \left(\sum_{j \in J} a_{jk} T_j \right) + T_{comm} + T_a \ . \tag{11}$$

Формула (11) показва, че увеличаването на броя на възлите не води автоматично до пропорционално намаляване на времето. Ако задачите са разпределени неравномерно, най-силно натовареният възел определя продължителността на цялата обработка. Съществено влияние оказва и времето за предаване на входните данни и получените резултати.

За илюстриране на зависимостите нека времената за изчисляване на седемте компонента бъдат съответно 4,2; 2,6; 1,8; 1,1; 3,4; 1,2 и 2,8 ms. Общото време на компонентните задачи при последователна обработка е 17,1 ms. Ако времето за агрегация е 0,4 ms, пълното последователно време е 17,5 ms.

При използване на четири работни възела задачите могат да бъдат разпределени така, че времената за тяхното натоварване да бъдат 4,2; 4,5; 4,0 и 4,4 ms. Най-голямото натоварване е 4,5 ms. Ако комуникационното време е 0,9 ms, а времето за агрегация е 0,4 ms, общото паралелно време е 5,8 ms.

При тези примерни стойности паралелната обработка е приблизително три пъти по-бърза от последователната, а ефективността на използването на четирите възела е около 75%. Числеият пример показва начина на прилагане на модела и необходимостта задачите да бъдат разпределяни според тяхната изчислителна сложност, а не само според броя им.

5 Проверка на решението чрез прагове

Интегралната оценка представя общото качество на поточния информационен запис, но не е достатъчна за вземане на окончателно решение. Високите стойности на няколко компонента могат да компенсират недопустимо ниската стойност на друг компонент. При управление в реално време това може да доведе до използване на закъсняла, непълна или невалидна информация въпреки приемливия общ резултат.

Поради тази причина след изчисляването на интегралната оценка се проверява дали всеки компонент изпълнява определения за него минимален праг. В таблица 2 е представен пример, при който общата оценка е сравнително висока, но показателят за навременност е под допустимото ниво.

Таблица 2. Илюстративна проверка на компонентните прагове

Показател	**Стойност $q_{j,i}$**	**Праг θ_j**	**Резултат**
Точност	0,93	0,80	изпълнен
Пълнота	0,96	0,90	изпълнен
Навременност	0,62	0,70	нарушен
Валидност	1,00	0,95	изпълнен
Съгласуваност	0,88	0,80	изпълнен
Проследимост	0,92	0,85	изпълнен
Надеждност	0,90	0,80	изпълнен

При тегла 0,20; 0,15; 0,20; 0,10; 0,10; 0,10 и 0,15, зададени съответно за точност, пълнота, навременност, валидност, съгласуваност, проследимост и надеждност, чрез формула (5) се получава интегрална оценка 0,869.

Независимо от високата интегрална оценка, стойността на навременността е 0,62 при минимално допустим праг 0,70. Следователно условието за навременност е нарушено и според формула (8) общият индикатор за риск приема стойност 1.

Поточният информационен запис трябва да бъде маркиран като рисков и да не се използва непосредствено за управление в реално време. В зависимост от приложението системата може да поиска повторно измерване, да използва резервен източник или да подаде предупредителен сигнал.

Примерът показва, че интегралната оценка и проверката на критичните прагове трябва да се изпълняват като две последователни и независими операции.

6 Приложение в Edge–Fog–Cloud среда

Разпределената паралелна реализация позволява компонентите на качеството да бъдат изчислявани на различни нива от Edge–Fog–Cloud архитектурата. Мястото на обработка се избира според необходимите входни данни, допустимото закъснение, изчислителната сложност и наличните ресурси.

В Edge слоя се намират устройствата, които са най-близо до информационните източници. На това ниво могат да се изпълняват проверките за валидност, пълнота и навременност. Тези проверки използват данни от текущия запис или от кратък времеви прозорец и не изискват продължително съхраняване на информацията. Изпълнението им непосредствено до източника позволява бързо откриване на липсващи, неправилно форматирани или закъснели записи.

Fog слоят обединява информация от няколко свързани Edge устройства. На това ниво могат да се изчисляват точността и съгласуваността, тъй като тяхното определяне често изисква сравнение между различни измервания. Fog възлите могат да използват прогнозни модели, физически зависимости и текущи данни от няколко информационни източника.

Cloud слоят разполага с по-големи изчислителни и запаметяващи ресурси. В него могат да се съхраняват историческите данни, резултатите от предишни оценки и сведенията за техническото състояние на устройствата. Тези данни се използват при определяне на проследимостта и надеждността, както и при актуализиране на теглата и критичните прагове.

Разделянето на обработката между трите нива намалява необходимостта всички първични данни да бъдат изпращани към отдалечен изчислителен център. Към следващото ниво могат да се предават само необходимите записи, частичните оценки и свързаните с тях метаданни. Това намалява комуникационното натоварване и времето за получаване на окончателната оценка.

При реализация в MPI среда диспечерът може да изпраща компонентните задачи чрез операции за обмен на съобщения, а агрегаторът да събира частичните резултати чрез колективна операция [12, 13]. Използването на неблокиращи операции позволява комуникацията и изчисленията да се застъпват във времето, когато това е допустимо.

При хетерогенна Edge–Fog–Cloud система същият логически модел може да бъде реализиран чрез мрежови услуги или брокер на съобщения. Независимо от използваната технология трябва да бъдат запазени идентификаторът на поточния информационен запис, моментът на неговото възникване и версията на времевия прозорец. Това гарантира, че агрегаторът няма да обединява резултати, които принадлежат на различни записи.

Разпределената структура позволява системата да бъде разширявана чрез добавяне на нови изчислителни възли или информационни източници. Тя също така дава възможност задачите да бъдат пренасочвани при претоварване или отказ на определен възел. По този начин се подобряват мащабируемостта и устойчивостта на оценяването на качеството на поточни данни.

7 Научен принос и ограничения

Основният резултат от разработката е обвързването на многокритериалната оценка на качеството с разпределена схема за обработка. Всеки компонент се разглежда като самостоятелна изчислителна задача, която може да бъде изпълнена в различен възел. Това позволява моделът да се използва при поточни данни, без всички проверки задължително да се извършват последователно в една система.

Предложеното разпределение отчита както времето за изчисляване на отделните компоненти, така и разхода за предаване и обединяване на резултатите. Запазена е отделната проверка на критичните прагове, поради което високата интегрална оценка не може да прикрие неприемливо ниска стойност на определен показател.

Разработката има теоретичен характер и не включва резултати от изпитване върху конкретна Edge–Fog–Cloud инфраструктура. Използваният числен пример служи за онагледяване на изчисленията, а не за доказване на постигната производителност. За практическото прилагане на модела е необходимо да бъдат измерени времената за обработка и комуникация при различна интензивност на входния поток. Теглата и критичните прагове също трябва да бъдат определени съобразно особеностите и рисковете на конкретния технологичен процес.

8 Заключение

В доклада е представена разпределена паралелна реализация на многокритериален модел за оценяване качеството на поточни данни. Качеството на всеки информационен запис се определя чрез седем самостоятелни компонента, които могат да бъдат изчислявани едновременно в различни възли.

Частичните резултати се обединяват в интегрална оценка, като всеки компонент участва с определено тегло. Успоредно с това се проверяват минималните допустими прагове. По този начин ниската стойност на важен показател не може да остане скрита зад високите стойности на останалите компоненти.

Анализът на изчислителното време показва, че резултатът от паралелната обработка зависи от правилното разпределяне на задачите, натоварването на отделните възли и времето за комуникация. Добавянето на нови възли е ефективно само когато намаляването на изчислителното време е по-голямо от допълнителния разход за обмен и обединяване на данните.

Предложеният подход може да бъде използван в Edge–Fog–Cloud среда, като отделните проверки се разполагат според необходимите ресурси и допустимото закъснение. Следващ етап от работата е разработването на прототип и провеждането на експерименти с реални поточни данни.

ЛИТЕРАТУРА:

[1] Ананиев, В., Станева, Л. Метод за повишаване точността на измерванията при работа с технологични модули. Научна конференция с международно участие „Техника, технологии и образование“, Ямбол, 2007, с. 27–31. ISBN 978-954-9999-54-9.

[2] 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.

[3] ISO/IEC 25012:2008. Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Data Quality Model. International Organization for Standardization, Geneva, 2008.

[4] Batini C., Cappiello C., Francalanci C., Maurino A. Methodologies for data quality assessment and improvement. ACM Computing Surveys, Vol. 41, No. 3, 2009, Article 16. DOI: 10.1145/1541880.1541883.

[5] Cai L., Zhu Y. The challenges of data quality and data quality assessment in the big data era. Data Science Journal, Vol. 14, 2015, Article 2. DOI: 10.5334/dsj-2015-002.

[6] Wang R. Y., Strong D. M. Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, Vol. 12, No. 4, 1996, pp. 5–33. DOI: 10.1080/07421222.1996.11518099.

[7] Kahn B. K., Strong D. M., Wang R. Y. Information quality benchmarks: Product and service performance. Communications of the ACM, Vol. 45, No. 4, 2002, pp. 184–192. DOI: 10.1145/505248.506007.

[8] Babcock B., Babu S., Datar M., Motwani R., Widom J. Models and issues in data stream systems. In: Proceedings of the Twenty-First ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, 2002, pp. 1–16. DOI: 10.1145/543613.543615.

[9] Datar M., Gionis A., Indyk P., Motwani R. Maintaining stream statistics over sliding windows. SIAM Journal on Computing, Vol. 31, No. 6, 2002, pp. 1794–1813. DOI: 10.1137/S0097539701398363.

[10] Iorga M., Feldman L., Barton R., Martin M. J., Goren N. S., Mahmoudi C. Fog Computing Conceptual Model. NIST Special Publication 500-325, National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.SP.500-325.

[11] Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge computing: Vision and challenges. IEEE Internet of Things Journal, Vol. 3, No. 5, 2016, pp. 637–646. DOI: 10.1109/JIOT.2016.2579198.

[12] Message Passing Interface Forum. MPI: A Message-Passing Interface Standard. Version 4.1, 2 November 2023.

[13] Stanev S. St., Nikolov N. R., Tsankov Ts. S. Cluster parallel computer system in MPI environment. Proceedings of the Scientific Conference MATTEX 2010, Shumen University, 2010, pp. 229–232.

[14] Denev D. R., Tsankov Ts. S. A Survey of Data Quality and Processing of Information in Innovative Smart Devices. In: 2022 International Conference Automatics and Informatics (ICAI), IEEE, 2022, ISBN 978-1-6654-7625-6, pp. 1–4.

[15] Denev D. R., Tsankov Ts. S. Communication-based dynamic packet optimization for visual PLC monitoring. Annual University Scientific Conference of the National Military University “Vasil Levski”, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1259–1266.

[16] Denev D. R., Tsankov Ts. S. Design and implementation of a field level of an industrial communication network for the needs of the industry. In: 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2022, Ohrid, North Macedonia, 2022, pp. 1–4. DOI: 10.1109/ICEST55168.2022.9828607.

AN ADAPTIVE MECHANISM FOR STREAMING DATA QUALITY MANAGEMENT UNDER CONCEPT DRIFT*

MILEN S. DAVIDKOV, EKATERINA M. HRISTOVA

ABSTRACT: *An adaptive mechanism for streaming data quality management under concept drift is proposed. It combines seven data-quality components, statistical analysis in adjacent sliding windows, drift detection, and constrained online updating of weights and critical thresholds. Two independent criteria, hysteresis, a minimum persistence interval, and a post-adaptation control period reduce unnecessary model changes. The distribution of operations across PLC and Edge devices, Fog nodes, and Cloud infrastructure is discussed. A numerical example illustrates drift confirmation and parameter updating without interrupting streaming processing.*

KEYWORDS: *streaming data, data quality, concept drift, adaptive model, sliding window*

DOI: https://doi.org/10.46687/MT26MSE

АДАПТИВЕН МЕХАНИЗЪМ ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО НА ПОТОЧНИ ДАННИ ПРИ КОНЦЕПТУАЛЕН ДРЕЙФ

МИЛЕН С. ДАВИДКОВ, ЕКАТЕРИНА М. ХРИСТОВА

АБСТРАКТ: *Предложен е адаптивен механизъм за управление на качеството на поточни данни при изменение на статистическите характеристики на наблюдавания процес. Механизмът обединява текущо оценяване на седем компонента на качеството, статистически анализ в два съседни плъзгащи се прозореца, откриване на концептуален дрейф и ограничено актуализиране на теглата и критичните прагове. За намаляване на погрешните адаптации се използват потвърждение от два независими критерия, хистерезис, минимална продължителност на отклонението и контролен период с възможност за възстановяване на предходната конфигурация. Разгледано е разпределянето на операциите между PLC и Edge устройства, Fog възли и Cloud инфраструктура. Числен пример показва действието на комбинирания критерий и актуализирането на параметрите без прекъсване на поточната обработка.*

1 Въведение

Информационните системи за наблюдение и управление обработват непрекъснато измервания от датчици, програмируеми логически контролери и интелигентни устройства. За да бъдат използвани при управление, тези данни трябва да постъпват навреме, да имат правилна структура и да бъдат съгласувани с физическото състояние на процеса. Повишаването на точността на измерванията при работа с технологични модули е разгледано в [1]. Качеството не се свежда единствено до точността на измерената стойност. То включва пълнота, навременност, валидност, съгласуваност, проследимост и надеждност [2–4].

При поточна обработка оценяването се извършва в ограничен времеви интервал и без многократно прочитане на цялата история. Плъзгащите се прозорци дават възможност да се поддържат текущи статистики с ограничена памет [5, 6]. Този подход обаче не решава самостоятелно проблема с промяната на наблюдавания процес. Праг, определен при зимен

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

режим, може да бъде неподходящ през преходен сезон; нормалното изменение на натоварването може да бъде прието за повреда, а постепенното отклонение на датчик да остане незабелязано.

Концептуалният дрейф представлява изменение на статистическите зависимости, върху които е изграден моделът. Той може да бъде рязък, постепенен, повтарящ се или локален. Методите ADWIN и други алгоритми за обучение от изменящи се потоци показват, че адаптацията трябва да отчита едновременно мащаба и устойчивостта на промяната [7–9]. При системи за управление е необходимо допълнително условие: новата конфигурация не трябва да се приема, преди да е проверено, че тя действително намалява грешките и не създава нестабилност.

Целта на разработката е да се създаде затворен механизъм, който свързва оценяването на качеството, откриването на дрейф и актуализирането на параметрите. Разширението спрямо статичния модел се състои в използване на двоен сигнал за дрейф, ограничена стъпка на адаптация, контролен период и разпределена реализация, съобразена с особеностите на интелигентните устройства и индустриалните комуникационни мрежи [10–13].

2 Изходни данни и оценка на качеството

Нека i-тият поточен запис е $x_i=(v_i,t_i^e,t_i^r,s_i,m_i)$, където v_i е измерената стойност, t_i^e и t_i^r са моментите на възникване и приемане, s_i е идентификаторът на източника, а m_i съдържа метаданните. За записа се формира вектор на качеството:

$$Q_i = (A_i, C_i, T_i, V_i, S_i, P_i, R_i), 0 \le q_{j,\,i} \le 1 \quad (1)$$

Компонентите описват съответно точност A, пълнота C, навременност T, валидност V, съгласуваност S, проследимост P и надеждност R. Оценките се нормализират в интервала от 0 до 1, за да могат да бъдат обединени независимо от първоначалните мерни единици. Практиката при интелигентните устройства показва, че предварителната проверка на структурата, произхода и времевите маркери трябва да се извършва възможно най-близо до източника [10].

Интегралната оценка използва изменяеми тегла $w_j(t)$, чиято сума е единица. Теглата изразяват значимостта на показателите в текущия режим, но не отменят критичните минимални прагове $\theta_j(t)$:

$$I_i(t) = \sum_{j=1}^{7} w_j(t) q_{j,\,i}, \sum_{j=1}^{7} w_j(t) = 1 \quad (2)$$

Записът се приема за рисков, когато поне един критичен компонент е под определения праг. Така високи стойности на останалите показатели не могат да компенсират опасно закъснение, липса на произход или ниска надеждност. Това разделяне между интегрална оценка и задължителни условия е важно при управленски приложения.

3 Откриване на концептуален дрейф

Наблюдението се извършва чрез два съседни прозореца с еднакъв размер w: референтен W_r и текущ Wc. За всеки източник се поддържат средна стойност, дисперсия, честота на липсващи записи, средно закъснение и средни стойности на компонентите на качеството. Статистиките се обновяват инкрементално, поради което не е необходимо съхраняване на цялата история.

$$\mu_t = (1/w)\sum_x \in W_c\ x, \sigma_t^2 = (1/w)\sum_x \in W_c(x - \mu_t)^2 \quad (3)$$

Единичното отклонение не е достатъчно основание за адаптация. Първият критерий $D_x(t)$ оценява промяната в разпределението на измерванията чрез нормализирани разлики между средните стойности и дисперсиите. Вторият критерий $D_q(t)$ отчита промяната в средната интегрална оценка, честотата на нарушенията на праговете и дела на липсващите или закъснелите записи. Общият показател е:

$$D(t) = \lambda D_x(t) + (1 - \lambda)D_q(t), 0 \leq \lambda \leq 1 \quad (4)$$

Дрейф се потвърждава, когато D(t) превиши горен праг h_2 в продължение на k последователни обновявания и поне един от двата частни критерия е над своя локален праг. Долният праг $h_1<h_2$ служи за хистерезис. След задействане системата остава в състояние на наблюдение, докато D(t) не спадне под h_1. Това предотвратява многократно включване и изключване при стойности около границата.

Характерът на установената промяна определя начина на реакция. При рязък дрейф отклонението възниква в рамките на един или няколко прозореца и е допустима по-голяма стъпка на адаптация. При постепенен дрейф старото и новото състояние съществуват едновременно и параметрите трябва да се изменят плавно. Повтарящият се дрейф позволява да се използва по-рано съхранена конфигурация, ако текущите характеристики са достатъчно близки до вече наблюдаван режим. Локалният дрейф засяга само част от източниците или показателите и не трябва да води до обща промяна на модела.

Таблица 1. Реакция на механизма при основните видове концептуален дрейф

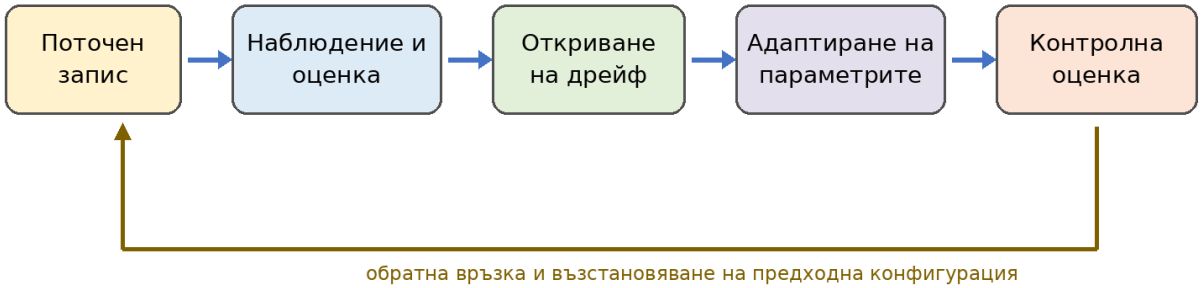
Вид на дрейфа	Наблюдаван признак	Основна реакция	Защитно условие
Рязък	бързо превишаване на h_2	по-голяма ограничена стъпка	потвърждение от двата критерия
Постепенен	устойчива тенденция в няколко прозореца	плавно обновяване	по-дълъг контролен период
Повтарящ се	сходство с предходен режим	извличане на запазена конфигурация	проверка върху текущите данни
Локален	промяна в отделен източник или компонент	локално адаптиране	без изменение на незасегнатите параметри

4 Адаптивен механизъм

Архитектурата включва наблюдение, оценка на качеството, откриване на дрейф, адаптиране и контролна оценка. Модулите са свързани чрез обратна връзка, която позволява връщане към последната устойчива конфигурация. Преди всяка промяна се запазват текущите тегла, прагове, размерът на прозореца и параметрите на прогнозния модел.

Нека Θ(t) е векторът на всички изменяеми параметри. След потвърден дрейф параметрите се обновяват с ограничена стъпка:

$$\Theta(t + 1) = \text{clip}[\Theta(t) + \alpha(t)\Delta\Theta(t),\ \Theta_{\min}, \Theta_{\max}] \quad (5)$$



Фиг. 1. Затворен цикъл на адаптивния механизъм

Функцията clip ограничава параметрите в предварително допустими граници. Коефициентът α(t) зависи от стойността на D(t), критичността на процеса и надеждността на данните. При плавна промяна той е малък, а при потвърдено рязко изменение може да бъде увеличен. Измервания с ниска надеждност не участват в актуализирането на референтния модел, защото биха могли да превърнат грешката в ново нормално състояние.

Теглата се актуализират според относителната информативност и стабилност на компонентите, след което отново се нормализират. Критичните прагове се изменят по-бавно от теглата и само когато промяната е потвърдена и от процесните данни. Тази разлика в скоростта е необходима, защото честата промяна на праговете може да прикрие реално влошаване на качеството.

След адаптацията започва контролен период от L прозореца. Новата конфигурация се потвърждава, ако намалява честотата на фалшивите аларми и пропуските, без да увеличава времето за реакция над допустимата стойност. При липса на подобрение системата възстановява запазената конфигурация. В дневника се записват причината за промяната, старите и новите параметри, използваните данни и резултатът от проверката.

5 Разпределена реализация в индустриална среда

Индустриалната реализация трябва да отчита едновременно ограничените ресурси на крайните устройства и комуникационното натоварване. При визуалния мониторинг на PLC размерът и честотата на пакетите влияят върху закъснението и върху възможността за своевременно обновяване на наблюдаваните стойности [11]. Затова системата не трябва да изпраща към централния слой всички необработени данни, когато част от проверките могат да се изпълнят локално.

Таблица 2. Разпределяне на операциите по изчислителни нива

Ниво	Основни операции	Използвани данни	Резултат
PLC/Edge	структурна проверка, времеви маркери, локални граници	текущ запис и кратък буфер	частични оценки и флагове
Fog	плъзгащи се прозорци, съгласуваност, откриване на дрейф	данни от свързани източници	D_x, D_q и предложение за адаптация
Cloud	история, обучение, сравнение на конфигурации	архив и дневник на адаптациите	актуализиран референтен модел

Полевото ниво осигурява непосредствената връзка с технологичния процес. Разгледаните в [12] принципи за изграждане на индустриална комуникационна мрежа могат да се използват за определяне на интерфейсите между PLC, устройства за събиране на данни и надзорни системи. Fog възелът обединява информацията от няколко източника и е подходящ за оценяване на съгласуваността и за откриване на локален дрейф. Cloud слоят поддържа дългосрочната история и по-сложните модели [14, 15].

Когато обработката се разпределя между няколко възела, задачите за отделните показатели могат да се изпълняват паралелно. Принципът за изпращане на задачи, събиране и синхронизиране на частични резултати е приложим и извън класическата MPI среда [13]. Координиращият възел формира общата оценка едва след получаване на всички задължителни компоненти или след изтичане на допустимото време.

6 Алгоритъм и числен пример

За всеки нов запис алгоритъмът проверява структурата и метаданните, извършва нормализация, определя компонентите на качеството и обновява статистиките в текущия прозорец. При достигане на края на прозореца се изчисляват $D_x(t)$, $D_q(t)$ и $D(t)$. Ако условията за устойчивост са изпълнени, се запазва текущата конфигурация и се изчислява предложение за адаптация. След контролния период предложението се потвърждава или се отменя.

1. Приемане и структурна проверка на новия поточен запис.
2. Изчисляване на седемте компонента и интегралната оценка.
3. Обновяване на статистиките в текущия плъзгащ се прозорец.
4. Изчисляване на двата частични критерия и общия показател D(t).
5. Потвърждаване на дрейфа чрез праг, продължителност и хистерезис.
6. Ограничено актуализиране на теглата, праговете и размера на прозореца.
7. Контролно оценяване и потвърждаване или отмяна на промяната.
8. Архивиране на параметрите, причината и получения резултат.

За илюстративния пример нека $\lambda=0,6$, $h_2=0,25$, $h_1=0,15$ и $k=3$. В три последователни прозореца са получени $D_x=0,31$; 0,34; 0,33 и $D_q=0,22$; 0,26; 0,28. За последния прозорец общият показател е:

$$D = 0,6 \cdot 0,33 + 0,4 \cdot 0,28 = 0,310 \quad (6)$$

Стойността е над горния праг и условието е изпълнено в три последователни прозореца, поради което дрейфът се приема за потвърден. Ако навременността се е влошила поради устойчиво увеличение на комуникационното закъснение, нейното тегло може да бъде увеличено от 0,15 на 0,18, а останалите тегла да бъдат пропорционално нормализирани. Прагът за навременност не се намалява автоматично, докато системата не установи, че промяната произтича от нов допустим режим, а не от претоварване или повреда.

Примерът показва разликата между адаптация и механично преместване на праговете. При временен комуникационен проблем системата запазва изискването и регистрира нарушение. При устойчив нов режим тя променя чувствителността постепенно и проверява резултата. Така се ограничава рискът моделът да се приспособи към дефектни данни.

Методика за експериментална проверка

За проверка на механизма е подходящо да се използва един и същ набор от поточни данни при две конфигурации: статичен модел с постоянни параметри и адаптивен модел. В

данните последователно се въвеждат нормален режим, рязка промяна, плавно изменение, временна комуникационна загуба и повтаряне на вече наблюдаван режим. Моментът и видът на всяко въздействие трябва да бъдат известни предварително, за да се разграничат правилните сигнали от фалшивите аларми.

Основните показатели са времето за откриване τ_d, делът на правилно откритите промени, делът на фалшивите сигнали и броят на ненужните актуализации. Допълнително се измерват средната интегрална оценка преди и след адаптацията, максималното комуникационно закъснение и натоварването на Edge и Fog възлите. За всяка промяна се пазят стойностите на D_x, D_q и D, за да може решението да бъде възпроизведено.

Адаптацията се приема за полезна само ако намалява сумарната грешка спрямо статичния модел и не нарушава ограничението за време на реакция. Това условие не позволява подобряване на един показател за сметка на недопустимо закъснение или нестабилно изменение на параметрите. Резултатите трябва да бъдат представени отделно за всеки вид дрейф, защото общата средна стойност може да прикрие слабост при конкретен режим.

7 Обсъждане

Предложеният механизъм съчетава процесните измервания и показателите за качество. Това е важно, защото промяната в средната стойност невинаги означава влошаване, а намаляването на качеството невинаги променя непосредствено статистиката на измерванията. Например загубата на пакети може да намали пълнотата и навременността, без средната стойност на получените измервания да се измени съществено. Обратно, сезонната промяна може да измени средната стойност, без данните да станат некачествени.

Съществено ограничение е необходимостта от начално определяне на размера на плъзгащите се прозорци, праговете и коефициента λ. Тези параметри зависят от честотата на измерване, динамиката на процеса и цената на пропуснатото нарушение. Механизмът не премахва нуждата от инженерна оценка, а осигурява проследим начин за постепенно изменение на параметрите. За практическа проверка са необходими сценарии с рязък, постепенен и повтарящ се дрейф, както и сравнение със статичен модел при еднакви входни данни.

Оценяването следва да включва време за откриване, дял на фалшивите сигнали, дял на пропуснатите промени, стабилност на параметрите и допълнително комуникационно натоварване. При разпределена реализация трябва да се измери и времето за събиране на частичните оценки. Добавянето на изчислителни възли е полезно само когато спестеното време е по-голямо от разхода за обмен и синхронизация.

8 Заключение

Разработен е адаптивен механизъм за управление на качеството на поточни данни при концептуален дрейф. Механизмът използва седем компонента на качеството, два независими сигнала за промяна, плъзгащи се прозорци, хистерезис и минимална продължителност на отклонението. Параметрите се изменят с ограничена стъпка, а резултатът се проверява в контролен период с възможност за връщане към предходната конфигурация.

Разпределянето между PLC/Edge, Fog и Cloud позволява бързите проверки да се изпълняват близо до източника, а сравнението на по-дълги периоди да използва общата инфраструктура. По този начин адаптацията не прекъсва обработката и остава проследима.

Следващ етап е експериментално калибриране върху реални поточни данни и сравнение със статичен базов модел.

ЛИТЕРАТУРА:

[1] Ананиев, В., Станева, Л. Метод за повишаване точността на измерванията при работа с технологични модули. Научна конференция с международно участие „Техника, технологии и образование“, Ямбол, 2007, с. 27–31. ISBN 978-954-9999-54-9.

[2] ISO/IEC 25012:2008. Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Data Quality Model. ISO, Geneva, 2008.

[3] Batini C., Cappiello C., Francalanci C., Maurino A. Methodologies for data quality assessment and improvement. ACM Computing Surveys, Vol. 41, No. 3, 2009, Article 16. DOI: 10.1145/1541880.1541883.

[4] Wang R. Y., Strong D. M. Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, Vol. 12, No. 4, 1996, pp. 5–33. DOI: 10.1080/07421222.1996.11518099.

[5] Babcock B., Babu S., Datar M., Motwani R., Widom J. Models and issues in data stream systems. Proceedings of PODS 2002, pp. 1–16. DOI: 10.1145/543613.543615.

[6] Datar M., Gionis A., Indyk P., Motwani R. Maintaining stream statistics over sliding windows. SIAM Journal on Computing, Vol. 31, No. 6, 2002, pp. 1794–1813. DOI: 10.1137/S0097539701398363.

[7] Bifet A., Gavaldà R. Learning from time-changing data with adaptive windowing. Proceedings of SDM 2007, pp. 443–448. DOI: 10.1137/1.9781611972771.42.

[8] Bifet A., Gavaldà R. Adaptive learning from evolving data streams. Advances in Intelligent Data Analysis VIII, 2009, pp. 249–260. DOI: 10.1007/978-3-642-03915-7_22.

[9] Gama J., Žliobaitė I., Bifet A., Pechenizkiy M., Bouchachia A. A survey on concept drift adaptation. ACM Computing Surveys, Vol. 46, No. 4, 2014, Article 44. DOI: 10.1145/2523813.

[10] Denev D. R., Tsankov Ts. S. A Survey of Data Quality and Processing of Information in Innovative Smart Devices. 2022 International Conference Automatics and Informatics (ICAI), IEEE, 2022, pp. 1–4, ISBN 978-1-6654-7625-6.

[11] Denev D. R., Tsankov Ts. S. Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring. Annual University Scientific Conference of the National Military University “Vasil Levski”, Veliko Tarnovo, 2022, ISSN 2367-7481, pp. 1259–1266.

[12] Denev D. R., Tsankov Ts. S. Design and Implementation of a Field Level of an Industrial Communication Network for the Needs of the Industry. ICEST 2022, Ohrid, 2022, pp. 1–4. DOI: 10.1109/ICEST55168.2022.9828607.

[13] Stanev S. St., Nikolov N. R., Tsankov Ts. S. Cluster Parallel Computer System in MPI Environment. Proceedings of the Scientific Conference MATTECH 2010, Shumen University, 2010, pp. 229–232.

[14] Iorga M., Feldman L., Barton R., Martin M. J., Goren N. S., Mahmoudi C. Fog Computing Conceptual Model. NIST Special Publication 500-325, 2018. DOI: 10.6028/NIST.SP.500-325.

[15] Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, Vol. 3, No. 5, 2016, pp. 637–646. DOI: 10.1109/JIOT.2016.2579198.

HBM PRODUCTION AND ITS EFFECT ON DDR5 MEMORY SUPPLY IN AI INFRASTRUCTURE*

GALIN P. PEYCHEV, VELISLAV I. STOYANOV

ABSTRACT: *This paper examines how the growth of high-bandwidth memory (HBM) for AI accelerators affects production capacity available for DDR5 DRAM. Research on the memory wall, thermal limits of stacked memory and CXL tiering is considered alongside primary manufacturer data. Based on a reported HBM3E to DDR5 wafer-supply trade ratio of approximately 3:1 for equal bit output, the authors construct a normalized allocation scenario and a sensitivity test. These models show how assumptions about wafer use change the potential DDR5 output under fixed capacity; they do not estimate market prices or actual production volumes. The study distinguishes the complementary roles of HBM and DDR5 and identifies the measurements needed for a future market model.*

KEYWORDS: *DRAM, HBM3E, HBM4, DDR5, wafer capacity, AI infrastructure, memory allocation*

DOI: https://doi.org/10.46687/MT26GPP

ПРОИЗВОДСТВОТО НА HBM И ВЛИЯНИЕТО МУ ВЪРХУ ПРЕДЛАГАНЕТО НА DDR5 ПАМЕТ ЗА AI ИНФРАСТРУКТУРА

ГАЛИН П. ПЕЙЧЕВ, ВЕЛИСЛАВ И. СТОЯНОВ

АБСТРАКТ: *Изследва се как нарастващото производство на памет с висока пропускателна способност (HBM) за ускорители с изкуствен интелект влияе върху капацитета за DDR5 DRAM. Съпоставени са изследвания за ограниченията на пропускателната способност, топлинните проблеми при многослойната памет и разширяването на сървърната памет чрез CXL. На основата на посочено от Micron приблизително съотношение 3:1 за използваните пластини при еднакъв обем произведени битове HBM3E и DDR5 авторите разработват сценарий за разпределение на капацитета и проверка на чувствителността. Изчисленията са илюстративни и не представляват прогноза за цени или реални производствени обеми.*

1 Въведение

Изчислителните системи за изкуствен интелект изискват едновременно висока пропускателна способност близо до ускорителя и значителен обем оперативна памет на сървъра. HBM обслужва първата задача, а DDR5 остава важна за централните процесори и общите сървърни натоварвания. Поради това развитието на HBM и DDR5 трябва да се разглежда едновременно като архитектурен и производствен въпрос [1, 2].

Целта на настоящия доклад е да се проследи по какъв механизъм пренасочването на ограничен производствен капацитет към HBM може да повлияе върху DDR5. Авторският принос е в подбора и съпоставката на първични технически данни, формулирането на прозрачен сценарий за разпределение на пластините и тълкуването на последствията за сървърната инфраструктура. Не са извършвани измервания в производствени предприятия и не се оценява пазарна цена.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Мотивът за бързото развитие на HBM е технически. Голяма част от изчисленията при генериране на текст изискват многократно четене на параметри на модела. Гхолами и съавтори показват, че при определени декодиращи модели и малки партиди заявки пропускателната способност на паметта може да ограничава производителността по-силно от пиковата изчислителна мощност [8]. Този резултат не важи еднакво за всяка задача: при големи партиди и други режими изчислителното натоварване може отново да стане водещо. Следователно търсенето на HBM има архитектурно основание, но размерът му зависи и от конкретните приложения.

2 Архитектура и производствени ограничения

DDR5 модулите използват два независими 32-битови подканала, докато HBM разчита на вертикално подредени DRAM кристали и широк интерфейс в близост до ускорителя. HBM3E достига над 1,2 TB/s за отделен стек при конкретни реализации; HBM4 удвоява броя на изводите за данни до 2048 според публикуваните данни на SK hynix [2–4]. Това са характеристики на различни продукти и не трябва да се тълкуват като универсални стойности за всички модули.

Таблица 1. Функционална съпоставка на DDR5 и HBM

Показател	DDR5	HBM
Основна роля	Оперативна памет на CPU и сървърни системи	Памет с висока пропускателна способност до ускорителя
Свързване	Модули и канали към контролера на процесора	Стекове от кристали и усъвършенствано корпусиране
Производствена особеност	Кристали и стандартно модулно сглобяване	Вертикално подреждане, TSV и допълнително сглобяване
Въпрос за доставките	Капацитет и наличност на модули	По-голям разход на производствен капацитет за същия обем битове

Източници: техническите материали на Micron и SK hynix [2–4].

Производството на HBM включва не само изработването на DRAM кристали, но и вертикално свързване и корпусиране. Тези операции увеличават сложността и могат да ограничават изхода на годни изделия. Конкретният рандеман зависи от процеса, броя слоеве и контрола на дефектите; затова не може коректно да се изчисли само като степен на един условен процент за всеки слой. В този доклад не се приема универсална стойност за технологичен брак.

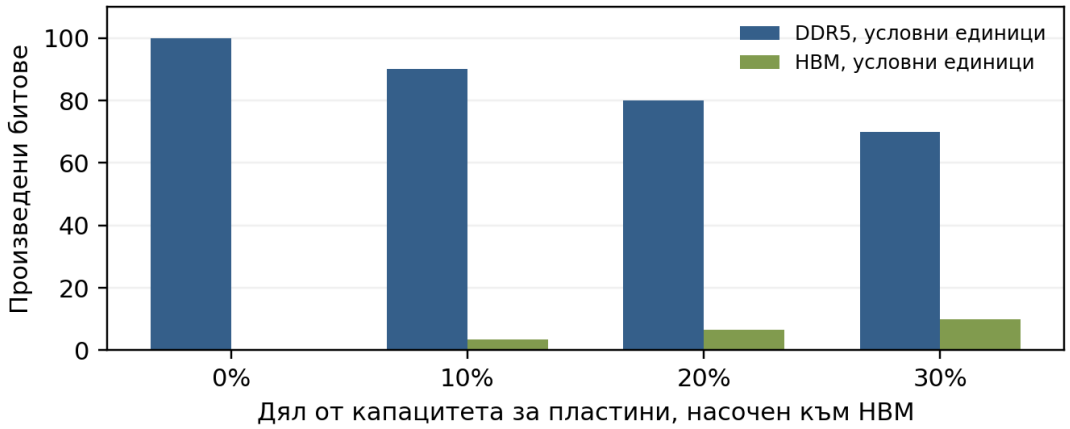
С увеличаването на броя слоеве възниква и топлинно ограничение. Обзорът на Лий и съавтори разглежда натрупването на топлина в стека, разликите в термичното разширение на материалите и риска от деформации и разслояване при хибридно свързване [9]. Той описва технологични направления за подобрение, но не дава обща стойност на брака, приложима за всеки производител. Затова разходът на пластини, капацитетът за сглобяване и качеството на крайния стек следва да се разглеждат като отделни ограничения.

3 Методика за оценка на заместването

Micron съобщава, че за еднакво количество битове HBM3E изисква приблизително три пъти повече капацитет за пластини от DDR5 при съпоставим технологичен възел. Компанията посочва и че съотношението може да нарасне при следващите поколения HBM

[1, 5]. Това е публично оповестена оценка на производител, а не измерване на авторите. Тя служи като входно допускане за следния илюстративен сценарий.

Нека общият наличен капацитет бъде 100 условни единици за обработка на пластини, а f е делът, насочен към HBM. При запазени производствени условия нормализираният изход на DDR5 е 100(1 - f), а изходът на HBM в съпоставими битови единици е 100f/3. Например при f = 0,20 се получават 80 единици DDR5 и приблизително 6,7 единици HBM. Сумата на двата изхода е под 100, защото HBM използва повече капацитет за единица произведена памет. Моделът не включва нови фабрики, промени в технологичния възел, търсене, договори или рандеман.



Фиг. 1. Илюстративен изход на памет при разпределение на фиксиран капацитет за пластини

Фигура 1 прави видим механизма на заместване: всеки допълнителен дял капацитет за HBM намалява капацитета, достъпен за DDR5, ако общият ресурс е фиксиран. Не следва автоматично заключение, че наличността или цената на DDR5 се изменя със същия процент. Те зависят и от запасите, новите мощности, договорите и търсенето.

За да се провери чувствителността към съотношението между продуктите, нека необходимият обем HBM е фиксиран на 5 условни единици битове, а k е необходимият капацитет за пластини за единица HBM спрямо DDR5. Тогава оставащият капацитет за DDR5 е 100 - 5k. Таблица 2 не представя наблюдавани стойности на k; стойността 3 е приблизителната оценка на Micron за HBM3E, а 2 и 4 са гранични допускания за сравнение [1].

Таблица 2. Чувствителност при еднакъв целеви обем HBM

Разход k	HBM, битови единици	Оставащ DDR5 капацитет
2	5	90
3	5	85
4	5	80

Изчисления на авторите при общ капацитет 100 условни единици. Стойностите са сценарии, а не измервания.

Двата сценария отговарят на различни въпроси. Фигура 1 фиксира дела на пластините за HBM, а таблица 2 фиксира търсеното количество HBM битове. При втория въпрос по-

високата производствена интензивност на HBM пряко намалява остатъчния капацитет за DDR5. Това разграничение е необходимо, за да не се смесват производствен дял и дял на готовата памет.

4 Последици за сървърните системи

В центровете за данни HBM и DDR5 се използват за различни задачи и често присъстват в една инфраструктура. HBM обслужва локалните потоци от данни към ускорителя, а DDR5 осигурява голям обем системна памет за CPU, предварителна обработка и други приложения [2]. Поради това ограниченото предлагане на DDR5 може да засегне и проекти, които не използват специализирани AI ускорители. Мащабът на този ефект не може да се изведе само от производственото съотношение.

В предходно изследване Николова и Цанков разглеждат адаптивното разпределение на мрежови ресурси в центрове за данни и облачни услуги [6]. Този подход е приложим като контекст за управление на натоварването и наличния капацитет, но публикацията не измерва производството на DRAM. Консорциумът CXL описва механизми за споделяне и групиране на памет между сървъри [7]. По-доброто използване на наличната памет може да намали локален недостиг при определени натоварвания, без да създава допълнителни DRAM чипове или да замества HBM до ускорителя.

Изследванията на CXL очертават и практическите граници на подобно решение. В публикацията TPP е показано, че преместването на рядко използвани страници към по-бавен паметен слой може да запази производителността при изследваните натоварвания, ако често използваните страници останат близо до процесора [10]. Левис, Лин и Тай предупреждават, че споделени CXL пулове могат да добавят разходи за инфраструктура, закъснение и сложност, които не се оправдават във всяка система [11]. Това са резултати за системно управление, а не основание да се отъждествяват CXL, DDR5 и HBM. Възможността за облекчаване на недостига зависи от профила на достъп до паметта.

5 От производствен капацитет към пазарно предлагане

За да се премине от резултатите на фигура 1 и таблица 2 към оценка на пазара, са необходими поне три отделни връзки. Първата е между разпределените пластини и годните битове, която зависи от технологичния възел и сглобяването. Втората е между произведените битове и доставените DDR5 модули, където участват корпусиране, тестове, складови запаси и продуктови договори. Третата е между доставките и цената, която зависи от търсенето в сървърния и потребителския сегмент. Настоящият модел изчислява само първата връзка при зададено съотношение.

Това разделение позволява да се формулират проверими хипотези. Ако делът на HBM в използваните пластини се повиши, а общият капацитет и рандеманът останат постоянни, потенциалният изход на DDR5 намалява. Ако междувременно се увеличат мощностите или плътността на битовете на пластина, намалението може да бъде частично или напълно компенсирано. Ако ограничението е в сглобяването на HBM стековете, простото пренасочване на повече пластини няма да осигури пропорционално повече готови изделия. Такива условия трябва да се проверяват с производствени данни, преди да се правят изводи за траен недостиг.

6 Заключение

Съпоставката на техническите данни и нормализираният сценарий показват конкретен канал, по който растежът на HBM може да ограничава производството на DDR5 при фиксиран капацитет за пластини. Публикуваното от Micron съотношение около 3:1 за

HBM3E и DDR5 дава основание да се изследва този ефект, но не позволява самостоятелна прогноза за цените или продължителността на недостига. Практическата стойност на предложения сценарий е, че отделя проверимото производствено допускане от променливите, за които са нужни допълнителни данни.

Следваща стъпка е моделът да се разшири с публични редове за реален капацитет, добив, продуктова структура и времеви лаг при увеличаване на мощностите. Така авторите ще могат да проверят чувствителността на резултатите, вместо да приписват целия пазарен натиск единствено на HBM.

ЛИТЕРАТУРА:

[1] Micron Technology. Fiscal Q2 2024 Earnings Call Prepared Remarks. 20 March 2024. https://micron.gcs-web.com/static-files/1a8d6c22-3b89-4806-930c-d30cbcd270d5

[2] Micron Technology. Micron Innovates From the Data Center to the Edge With NVIDIA. 18 March 2025. https://investors.micron.com/news/press-release/2025/Micron-Innovates-From-the-Data-Center-to-the-Edge-With-NVIDIA-03-18-2025/default.aspx

[3] Micron Technology. Micron DDR5 Client Module Features. Technical white paper. https://assets.micron.com/adobe/assets/urn%3Aaaid%3Aaem%3A5902f17e-8bde-4246-971c-8d7f274c6b1a/original/as/ddr5-key-module-features-wp-client.pdf

[4] SK hynix. SK hynix Completes World's First HBM4 Development and Readies Mass Production. 12 September 2025. https://news.skhynix.com/en/sk-hynix-completes-worlds-first-hbm4-development-and-readies-mass-production/

[5] Micron Technology. Fiscal Q1 2026 Earnings Presentation. 17 December 2025. https://micron.gcs-web.com/static-files/530bd7ed-a8c8-4687-af4a-8c129f740e09

[6] Nikolova S., Tsankov Ts. Intelligent resource management systems in computer networks. Annual of Konstantin Preslavsky University of Shumen, vol. XIV E, 2024, pp. 210-220. https://doi.org/10.46687/YT24SIS

[7] Bowman K. Explaining CXL Memory Pooling and Sharing. Compute Express Link Consortium, 2 August 2023. https://computeexpresslink.org/blog/explaining-cxl-memory-pooling-and-sharing-1049/

[8] Gholami A., Yao Z., Kim S., Hooper C., Mahoney M. W., Keutzer K. AI and Memory Wall. IEEE Micro, vol. 44, no. 3, 2024, pp. 33-39. https://doi.org/10.1109/MM.2024.3373763

[9] Lee S.-H., Kim S.-J., Lee J.-S., Rhi S.-H. Thermal Issues Related to Hybrid Bonding of 3D-Stacked High Bandwidth Memory: A Comprehensive Review. Electronics, vol. 14, no. 13, 2025, article 2682. https://doi.org/10.3390/electronics14132682

[10] Al Maruf H. et al. TPP: Transparent Page Placement for CXL-Enabled Tiered-Memory. ASPLOS 2023, vol. 3, pp. 742-755. https://arxiv.org/abs/2206.02878

[11] Levis P., Lin K., Tai A. A Case Against CXL Memory Pooling. HotNets 2023, 7 pp. https://doi.org/10.1145/3626111.3628195

EVOLUTION OF SILICON PACKAGING FROM MONOLITHIC DIES TO CHIPLETS AND 3D CACHE*

GALIN P. PEYCHEV, VELISLAV I. STOYANOV

ABSTRACT: *The paper compares monolithic dies, lateral chiplet integration and three-dimensional cache stacking as distinct ways to increase system complexity. The authors develop a qualitative comparison of interconnect, yield, thermal and testing constraints and illustrate the sensitivity of bare-die yield to area with a Poisson model. Published results for CoWoS, EMIB, hybrid bonding and UCIe are assessed. The calculations are illustrative and do not represent measured product yield or a cost forecast. The study identifies conditions under which modularity can be beneficial and the additional assembly risks that must be evaluated.*

KEYWORDS: *chiplets, advanced packaging, silicon interposer, hybrid bonding, 3D cache, yield, UCIe*

DOI: https://doi.org/10.46687/MT26GPV

РАЗВИТИЕ НА КОРПУСИРАНЕТО ОТ МОНОЛИТНИ КРИСТАЛИ КЪМ ЧИПЛЕТИ И 3D КЕШ

ГАЛИН П. ПЕЙЧЕВ, ВЕЛИСЛАВ И. СТОЯНОВ

АБСТРАКТ: *Съпоставят се монолитният кристал, страничното интегриране на чиплети и вертикалното подреждане на кеш памет. Авторите предлагат качествена рамка за оценка на свързаността, рандемана, топлинния режим и изпитването и изчисляват илюстративна зависимост между площта на кристала и добива при модел на Поасон. Анализирани са публикувани резултати за CoWoS, EMIB, хибридно свързване и UCIe. Примерът не е измерване на реален продукт и не служи за прогноза на себестойност.*

1 Въведение

Увеличаването на броя транзистори в един монолитен кристал среща ограничения, свързани с площта, производствения добив, захранването и отвеждането на топлината. Разделянето на функциите между отделни кристали позволява да се комбинират логика, входно-изходни блокове и памет, но пренася част от сложността към корпуса и връзките между кристалите [1, 2]. Целта на доклада е да се разграничат технологичните възможности от допусканията за ефективност, които зависят от конкретен проект.

Приносът на авторите е сравнителната рамка в таблица 1, подредбата на архитектурите във фигура 1 и изчислителният пример в таблица 2. Те свързват геометрията на кристала с добива и отделно отчитат риска при сглобяване. Докладът е аналитичен, без експериментално измерване на процесори или корпуси.

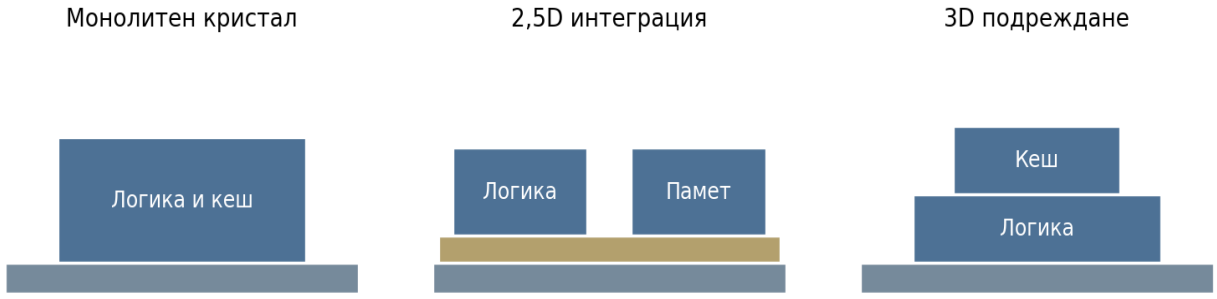
2 Архитектурни подходи и връзки

Монолитната схема разполага изчислителните блокове и част от кеша върху общ кристал. При 2,5D интеграция отделни кристали са поставени един до друг и се свързват през междинен слой или локален мост. CoWoS използва варианти на междинен слой за

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

съвместно интегриране на изчислителни кристали и HBM [3]. EMIB реализира локален силициев мост в подложката, без необходимост връзката между съседните кристали да минава през междинен слой с размер на целия корпус [4]. Това са различни реализации, чиито параметри зависят от приложението.

При вертикалната интеграция функционален слой се разполага над друг. TSMC-SoIC описва пряко свързване на кристали, а публикуваната реализация на 3D V-Cache поставя 64 MB кеш върху 7 nm x86-64 процесорен кристал чрез хибридно свързване [5, 6].



Фиг. 1. Схематично разположение на функционални кристали при трите подхода

Авторска схема по технологичните описания [3–6]. Изображението не е в мащаб.

Стандартът UCIe определя интерфейс за комуникация между кристали в общ корпус, включително физически слой и протоколни механизми. Наличието на стандарт облекчава съвместимостта, но само по себе си не гарантира еднакво закъснение, консумация или рандеман между различни корпуси. Версия 3.0 добавя режими до 64 GT/s при посочени от консорциума условия [7].

Таблица 1. Критерии за съпоставка на интеграционните подходи

Критерий	Монолитен кристал	2,5D чиплети	3D подреждане
Връзка	Вътрешнокристална	Между кристали през мост или междинен слой	Вертикална между подредени кристали
Основно предимство	Единна реализация и локални връзки	Модулност и избор на технологични процеси	Голяма плътност на вертикалните връзки
Водещ риск	Добив при голяма площ	Сглобяване, тест и междучипова комуникация	Топлина, подравняване и изпитване на стека

Качествена оценка на авторите по [1–7]; сравнението не задава универсална класация на производителност.

3 Разделяне на функции и избор на технология

Решението за разделяне започва от потока на данните между блоковете. Ако два блока обменят информация във всеки такт или изискват много тесен път към общ кеш, преместването им в различни кристали може да увеличи закъснението и консумацията за пренос. По-слабо свързаните функции, например някои входно-изходни блокове, допускат по-свободно разполагане. Обзорът на Лиу, Ли и Ин поставя разпределението на функциите и съвместната оптимизация на корпус и архитектура в центъра на проектирането [1]. Следователно броят чиплети не е самостоятелен показател за качество. Важни са границите, по които системата е разделена.

Модулният подход допуска кристалите да се изработват по различни технологични процеси. Плътната изчислителна логика може да има различни изисквания от аналоговите схеми, интерфейсите или паметта. Това дава проектна гъвкавост, но изисква съгласуване на захранващи напрежения, тактови области, механична геометрия и изпитване. Повторното използване на готов функционален блок носи полза само ако интерфейсът му и корпусът отговарят на новото приложение [1, 2].

При CoWoS големият междинен слой позволява плътно разполагане на логика и стекове HBM. При EMIB локалните мостове обслужват определени граници между кристали, като топологията на мрежата трябва да се предвиди при разполагането им [3, 4]. Двете решения не бива да се свеждат до едно и също понятие за 2,5D корпусиране. Изборът зависи от броя и разположението на интерфейсите, необходимата ширина на връзките и ограниченията на производството.

При 3D подреждане вертикалната близост може да намали дължината на част от връзките и да увеличи тяхната плътност. Тя обаче усложнява подравняването на повърхностите и достъпа до вътрешните слоеве след сглобяване. Обзорът в IEEE Electron Devices Reviews разглежда отделно свързването кристал към кристал, кристал към пластина и кристал към подложка, както и механичната и електрическата надеждност на различните методи [11]. Тази класификация е полезна, защото геометрично сходни крайни изделия могат да произхождат от различни технологични процеси.

4 Електрическа цена на комуникацията

Междучиповата връзка се оценява поне чрез пропускателна способност, закъснение, енергия за пренесен бит и площ на интерфейса. Увеличаването на броя физически линии може да повиши пропускателната способност, но заема периферия и изисква захранване и синхронизация. При конкретни реализации се добавят разходи за кодиране, буфериране или протокол. Затова публикуваната скорост на една линия не е равна на полезната скорост на приложение. Сравненията трябва да използват еднакви условия за трафик и еднаква граница на измерване [1, 2, 7].

Стандартизацията на UCIe създава обща основа за интерфейса между кристали, но физическият резултат остава зависим от корпуса. Например две системи могат да следват една и съща спецификация, а да се различават по дължина на връзката, брой линии, режим на работа и топлинен запас [7]. Авторите приемат за коректна съпоставка само измерване, което указва използваната версия на интерфейса, ефективния полезен трафик, консумацията на двата края и условията на температура. Без тези данни твърдението, че една архитектура има „по-бърза връзка“, е непълно.

5 Площ, рандеман и граници на модела

За илюстрация на връзката между площта на единичен кристал и дефектите се използва опростеният модел на Поасон $Y(A) = \exp(-D_0 A)$, където Y е вероятността кристалът да е годен, D_0 е плътността на критичните дефекти в cm^{-2}, а A е площта в cm^2 [1, 8]. Моделът приема случайно и независимо разпределение на дефектите. Реалният производствен добив зависи и от групиране на дефекти, повторяемост на блокове и възможности за резервиране; една формула не заменя измерванията.

Авторите избират условна плътност $D_0 = 0{,}1\ cm^{-2}$ и три площи за проверка на чувствителността. Например $200\ mm^2 = 2\ cm^2$ и $Y = \exp(-0{,}2) \approx 0{,}819$. За $600\ mm^2$ при същото допускане резултатът е приблизително 0,549. Тези числа са математически пример, а не данни за конкретен възел или процесор.

Таблица 2. Илюстративен добив на единичен кристал при $D_0 = 0{,}1\ cm^{-2}$

Площ A	Площ в cm^2	Y(A)
100 mm^2	1	0,905
200 mm^2	2	0,819
600 mm^2	6	0,549

Изчисления на авторите по модела [8], закръглени до три знака.

По-малките отделни кристали могат да се изпитват преди интеграцията като годни компоненти. Това не означава, че крайният многокристален корпус автоматично има добив 0,819 или че разходът намалява с определен процент. Към добива на кристалите се добавят загубите при свързване, дефекти на междинния слой, тест, захранване и охлаждане [1, 2]. При сравнение на себестойност следва да се отчита и броят изрязани кристали от пластина, площта на периферните връзки и цената на корпуса.

6 От годен кристал към годен корпус

Моделът в таблица 2 описва единичен кристал преди сглобяване. При модулна система производителят може да подбира предварително изпитани кристали, но всяка следваща операция има собствена вероятност за успешен резултат. Като мисловен пример, ако три вече годни кристала се сглобяват и условният добив на тази операция е 0,95, крайният добив сред започнатите с тези кристали сглобявания е 0,95, а не произведението на трите стойности 0,819. Стойността 0,95 е избрано допускане, не публикуван резултат. Разходът за предварително отхвърлените кристали все пак остава в общия производствен баланс.

За да се сравнят два проекта икономически, следва да се изчислят добивът и цената на всеки тип кристал, броят годни компоненти от пластина, разходът за междинен слой и сглобяване, както и цената на дефект, открит след тази операция. Съществена е последователността на тестовете. Когато дефектният елемент се открие едва след присъединяване на скъпи работещи компоненти, загубата може да бъде по-голяма от стойността на самия дефектен кристал. Обзорът на технологиите за хетерогенна интеграция свързва именно процеса на съединяване с надеждността на крайното изделие [11].

Хибридното свързване изисква подготовка на повърхностите, контрол на замърсяванията и точност на подравняване. Публикацията от ECTC 2024 за свързване на кристал към пластина посочва тези операции и риска от кухини при съединяването [12]. Това е технологично основание да се разглеждат отделно рандеманът на пластината и добивът след корпусиране. Не е достатъчно да се раздели един голям кристал на по-малки, ако интерфейсите и монтажът увеличат производствените загуби.

7 Топлинен режим и системна перспектива

Вертикалното подреждане скъсява част от пътя на сигналите, но изменя пътищата за отвеждане на топлината. Температурата на логическия слой, достъпът до кеша, честотният режим и надеждността трябва да се оценяват за конкретния процесор. Публикацията за 3D V-Cache доказва възможността за работещо хибридно свързване, но не дава основание всички реализации да се приемат за равни по закъснение или честота с монолитен кеш [6]. Изследванията върху автоматизацията на проектирането на чиплети също поставят съвместната оптимизация на разположението, комуникацията и топлината сред откритите задачи [2].

Свързаността има значение на различни мащаби. Цанков разглежда управлението на ресурси и комуникационни потоци в индустриални компютърни мрежи [9]. Станев, Николов и Цанков описват клъстер от изчислителни възли, свързани за паралелна работа в среда MPI [10]. Тези изследвания са контекст за системното разпределение на изчисления и комуникация. Връзката между чиплети в един корпус работи на друг физически мащаб и изисква отделни критерии за плътност, закъснение и енергия на пренос.

При избор на архитектура авторите предлагат последователно да се оценяват четири въпроса. Първо, кои функции могат да бъдат разделени без прекомерен обмен на данни. Второ, как се променя добивът на отделните кристали и какъв е рискът при сглобяването. Трето, дали електрическите и топлинните характеристики на връзките покриват целевия режим. Четвърто, може ли всеки слой да бъде изпитан преди и след интеграция. Тази рамка е приложима при предварителен анализ, но за избор на продукт са необходими технологични и измервателни данни.

8 Проверка на архитектурна хипотеза

За практическа проверка на предложената рамка авторите формулират три отделни хипотези. При разделяне на голям монолитен кристал добивът на отделните по-малки кристали трябва да се подобри при сходен процес и плътност на дефектите. При добавяне на междучипова връзка измерените закъснение и енергия могат да се увеличат спрямо вътрешнокристален път. При вертикално разполагане на кеша топлинният режим може да ограничи достъпния честотен режим. Всяка хипотеза изисква отделни измервания; потвърждението на първата не доказва останалите две.

Необходимият набор от данни включва площ и добив на всеки кристал, процент на успешното сглобяване, температура при еднакъв товар, действителен полезен трафик между блоковете и обща консумация при еднаква задача. Резултатите следва да се нормализират по изпълнена работа, например енергия за обработена заявка, а не само по пикова честота или теоретична пропускателна способност. Така се вижда дали предимството на модулното производство компенсира електрическата и технологичната цена на интеграцията. Подобна проверка е следващата задача на авторите и не се представя като вече проведен експеримент.

9 Заключение

Чиплетите и 3D кешът разширяват възможностите за интеграция, като преместват част от ограниченията от площта на монолитния кристал към корпуса, междучиповата връзка и топлинния режим. Авторският пример показва единствено чувствителността на добива на единичен кристал към площта при зададена плътност на дефектите. Предимството на даден подход следва да се проверява с данни за годни кристали, загуби при сглобяване, енергия, закъснение и надеждност. Така съпоставката остава проверима, без да се приписва универсално превъзходство на конкретна технология.

ЛИТЕРАТУРА:

[1] Liu Y., Li X., Yin S. Review of chiplet-based design: system architecture and interconnection. Science China Information Sciences, 2024, 67, 200401. https://doi.org/10.1007/s11432-023-3926-8

[2] Chen S., Zhang H., Ling Z., Zhai J., Yu B. The Survey of Chiplet-based Integrated Architecture: An EDA Perspective. 2024. https://arxiv.org/abs/2411.04410

[3] TSMC. CoWoS® advanced packaging technology. https://3dfabric.tsmc.com/english/dedicatedFoundry/technology/cowos.htm

[4] Intel Foundry. EMIB Technology Brief. 2025. https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2025-07/emib-product-brief.pdf

[5] TSMC. TSMC-SoIC® technology. https://3dfabric.tsmc.com/english/dedicatedFoundry/technology/SoIC.htm

[6] Wuu J. et al. 3D V-Cache: the Implementation of a Hybrid-Bonded 64MB Stacked Cache for a 7nm x86-64 CPU. ISSCC, 2022, pp. 428–429. https://doi.org/10.1109/ISSCC42614.2022.9731565

[7] UCIe Consortium. UCIe Specifications, version 3.0. 2025. https://www.uciexpress.org/specifications

[8] IEEE. Semiconductor yield modeling, Poisson model. IEEE Technology Navigator. https://technav.ieee.org/topic/integrated-circuit-yield/

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

[10] Станев С. С., Николов Н. Р., Цанков Ц. С. Клъстерна паралелна изчислителна система в среда MPI. MATTEX 2010, т. 1, Шумен, 2010/2011, с. 229–232. ISSN 1314-3921.

[11] Sahoo K., Harish V., Ren H., Iyer S. S. A Review of Die-to-Die, Die-to-Substrate and Die-to-Wafer Heterogeneous Integration. IEEE Electron Devices Reviews, vol. 2, 2025, pp. 6–31. https://doi.org/10.1109/EDR.2024.3501214

[12] Hung R. et al. Enabling Die-to-Wafer Hybrid Bonding for the Next Generation Advanced 3D Packaging. IEEE ECTC, 2024. https://doi.org/10.1109/ECTC51529.2024.00127

DESIGN AND IMPLEMENTATION OF A HYBRID LABORATORY ENVIRONMENT FOR PASSIVE NETWORK TRAFFIC ANALYSIS*

DENIS I. ZVEZDELINOV, ZDRAVKO Y. KUZMANOV

ABSTRACT: *In the current landscape of escalating cyber threats, the need for secure, isolated, and effective test setups for network analysis and training is critical. This report presents the design and implementation of a portable, hybrid laboratory infrastructure intended for passive monitoring and hands-on Deep Packet Inspection (DPI). The proposed architecture integrates a Raspberry Pi 4B single-board computer as the central analysis station, combined with a GL.iNet Beryl AX router and a Zyxel GS1200-5 managed switch. A key element of the setup is the implementation of a passive hardware network tap (Throwing Star LAN Tap Pro), which ensures physical traffic duplication with zero packet loss, without introducing additional latency or being detectable by network participants. The results demonstrate that the established configuration overcomes the limitations of traditional methods such as SPAN/Port Mirroring, providing a reliable, cost-effective, and fully transparent environment suitable for network forensics, cyberattack simulation, and educational purposes.*

KEYWORDS: *network analysis, cybersecurity, Raspberry Pi, Network TAP, Deep Packet Inspection (DPI)*

DOI: https://doi.org/10.46687/MT26DIZ

ПРОЕКТИРАНЕ И РЕАЛИЗАЦИЯ НА ХИБРИДНА ЛАБОРАТОРНА СРЕДА ЗА ПАСИВЕН АНАЛИЗ НА МРЕЖОВ ТРАФИК

ДЕНИС И. ЗВЕЗДЕЛИНОВ, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *В съвременната среда на нарастващи киберзаплахи, необходимостта от сигурни, изолирани и ефективни тестови постановки за мрежов анализ и обучение е критична. Този доклад представя проектирането и практическата реализация на портативна, хибридна лабораторна инфраструктура, предназначена за пасивен мониторинг и дълбоко инспектиране на пакети (DPI). Предложената архитектура интегрира едноплатков компютър Raspberry Pi 4B като централна аналитична станция, комбиниран с маршрутизатор GL.iNet Beryl AX и управляем комутатор Zyxel GS1200-5. Ключов елемент в постановката е внедряването на пасивен хардуерен мрежов ответвител (Throwing Star LAN Tap Pro), който гарантира физическото дублиране на трафика без загуба на пакети (Zero Packet Loss) и без да внася допълнителна латентност или да бъде откриваем за участниците в мрежата. Резултатите показват, че изградената конфигурация преодолява недостатъците на традиционните методи като SPAN/Port Mirroring и предоставя надеждна, финансово ефективна и напълно прозрачна среда, подходяща за мрежова форензика, симулиране на кибератаки и образователни цели.*

1 Въведение

В условията на непрекъснато еволюиращи киберзаплахи и все по-сложни мрежови архитектури, гарантирането на информационната сигурност изисква задълбочено разбиране на процесите, протичащи на ниво мрежов трафик. Основа за изграждането на ефективни стратегии за киберотбрана е способността за прецизен мониторинг, улавяне и анализ на пакети данни в реално време. За да бъдат изследвани векторите на атака, зловредният мрежов трафик или уязвимостите в комуникационните протоколи по

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

безопасен начин, специалистите и изследователите се нуждаят от строго изолирани тестови среди (т.нар. „пясъчници“ или sandboxes). Тези среди трябва да гарантират, че експериментите няма да компрометират продукционните мрежи и едновременно с това ще предоставят максимално реалистични данни за анализ. [1]

Използването на лабораторни модели и симулационни среди позволява изследването на сложни технически и мрежови процеси при контролирани условия, като същевременно се запазват съществените зависимости и характеристики на реалната система. [2]

В съвременната практика за образователни и тестови цели масово се прилагат изцяло софтуерни симулатори на мрежови топологии (като Cisco Packet Tracer) или виртуални среди (чрез платформи като VMware, VirtualBox). Въпреки тяхната безспорна гъвкавост и ниска цена, виртуалните постановки притежават съществени ограничения. Те абстрахират процесите на физическия слой (Layer 1) и каналовия слой (Layer 2) от OSI модела, което прави невъзможно пълноценното изследване на хардуерни аномалии, микросекундни закъснения в мрежата или поведението на специфично физическо оборудване. Освен това, чисто софтуерното улавяне на трафик във виртуална среда често филтрира повредени рамки (malformed frames) и не може да възпроизведе точно условията на атаки, разчитащи на физическа манипулация на мрежовите интерфейси. За нуждите на автентичната мрежова форензика (Network Forensics) и дълбокото инспектиране на пакети (Deep Packet Inspection – DPI), наличието на реален хардуер е критично условие за достоверността на резултатите.

Целта на настоящия доклад е да представи проектирането, изграждането и тестването на физическа, хибридна лабораторна инфраструктура за пасивен мрежов анализ, която преодолява ограниченията на виртуалните симулатори. Разработката предлага бюджетна, преносима и високоефективна алтернатива на скъпите индустриални решения, като интегрира достъпни хардуерни компоненти – едноплатков компютър Raspberry Pi 4B [12] като централна аналитична станция, маршрутизатор GL.iNet Beryl AX [9] и управляем комутатор Zyxel GS1200-5 [15]. За осигуряване на пълна прозрачност и нулево влияние върху изследвания трафик, в архитектурата е внедрен хардуерен мрежов ответвител (Throwing Star LAN Tap Pro by Great Scott Gadgets) [10]. Предложената постановка е подходяща както за провеждане на задълбочени експериментални изследвания в областта на киберсигурността, така и като надежден инструмент за академично обучение.

2 Архитектура и топология на лабораторната среда

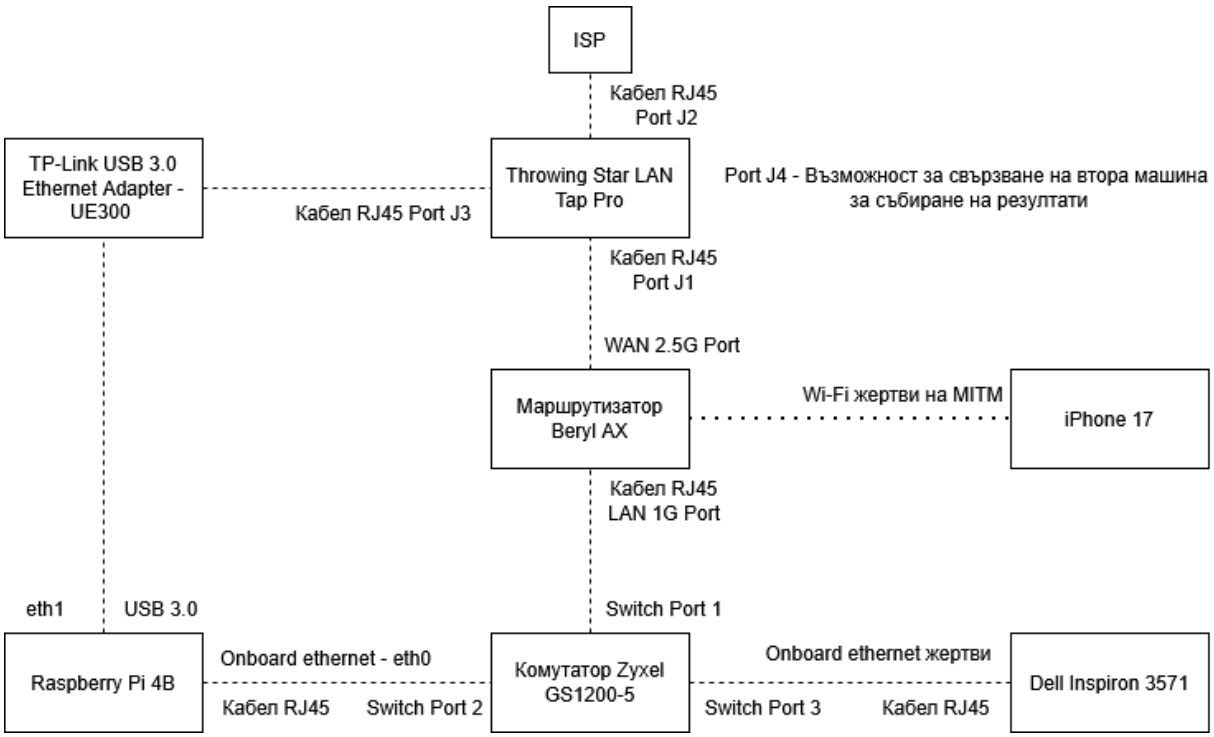
Архитектурата на лабораторната постановка е проектирана с основен фокус върху осигуряването на стриктна мрежова изолация на експерименталния трафик и гарантиране на пълна прозрачност при неговото улавяне. Концептуалният модел на изградената топология и физическата свързаност на отделните компоненти са илюстрирани на фиг. 1.

В логическо отношение, средата е конфигурирана така, че да предотврати неоторизирано изтичане на данни към външни или продукционни мрежи.

Основният тестов сегмент използва IPv4 адресиране и оперира в изолираното адресно пространство 192.168.8.0/24 [7]. В рамките на тази подмрежа, маршрутизаторът (GL.iNet Beryl AX) изпълнява функциите на шлюз по подразбиране (Default Gateway) и DHCP сървър, подсигурявайки базовата мрежова конфигурация за всички свързани крайни устройства.

Ключовата архитектурна специфика в топологията е позиционирането на хардуерния мрежов ответвител (Throwing Star LAN Tap). Той е интегриран последователно („in-line“) между изследвания мрежов възел и управляемия комутатор (Zyxel GS1200-5), създавайки пълно копие на преминаващите електрически сигнали на ниво физически слой. Тъй като

пасивният TAP разделя двупосочната комуникация на две независими еднопосочни линии – предаваща (TX) и приемаща (RX), аналитичната станция (Raspberry Pi 4B) е свързана към мониторинг портовете на ответвителя чрез два отделни мрежови интерфейса. Този подход гарантира паралелно, независимо и напълно скрито улавяне на двата потока данни.



Фигура 1. Физическа топология на лабораторната среда и използваните устройства

3 Хардуерно осигуряване и компоненти

Успешната реализация на преносима и независима лабораторна среда изисква внимателен подбор на хардуерни компоненти, които да балансират между висока производителност, компактност, ниска консумация на енергия и достъпна цена. Архитектурата залага на модулен принцип, при който всяко устройство изпълнява ясно дефинирана роля в процеса на осигуряване на свързаност, маршрутизация и улавяне на данните.

3.1. Аналитичен възел – Raspberry Pi4B

Централният елемент за събиране, съхранение и последваща обработка на мрежовия трафик е едноплатковият компютър Raspberry Pi 4B. Изборът му като главна аналитична станция е обоснован от няколко предимства. Четириядреният ARM Cortex-A72 процесор и наличната системна памет осигуряват достатъчен ресурс за обработка в реално време и изпълнение на специализиран софтуер (tcpdump, Wireshark, TShark) без опасност от препълване на системния буфер при интензивен трафик. Наличието на вграден Gigabit Ethernet порт и USB 3.0 шина позволява лесното добавяне на втори външен мрежов адаптер (USB-to-Ethernet). По този начин Raspberry Pi разполага с два независими физически интерфейса, необходими за приемане на предаващия (TX) и приемащия (RX) поток от пасивния мрежов ответвител. Ниската консумация на енергия (захранване през USB-C) прави системата изключително мобилна и удобна за бързо внедряване както в лабораторни, така и в теренни условия.

3.2. Мрежова архитектура

• Маршрутизатор GL.iNet Beryl AX (GL-MT3000): Компактен джобен рутер с поддръжка на Wi-Fi 6 и OpenWrt-базирана операционна система [11]. Основната му задача е да администрира изолираната подмрежа (192.168.8.0/24), да предоставя DHCP услуги за автоматична конфигурация, да управлява таблиците за маршрутизация и да осигурява криптиран VPN тунел при необходимост от защитен отдалечен достъп до лабораторията. [3]

• Управляем комутатор Zyxel GS1200-5: Компактен 5-портов гигабитов комутатор с възможност за уеб-управление. В топологията той служи за физическо групиране на експерименталните възли, като предоставя възможност за сегментация чрез виртуални мрежи (VLAN) и контрол върху портовете на Layer 2.

3.3. Мрежов ответвител: Throwing Star LAN Tap Pro

Сърцевината на пасивното прихващане в лабораторната постановка е хардуерният мрежов ответвител Throwing Star LAN Tap Pro. За разлика от активните TAP устройства или софтуерните SPAN портове, това пасивно платно оперира изцяло на физическия слой (Layer 1) за стандартите 10Base-T и 100Base-T Ethernet [4]. Устройството се свързва последователно („in-line“) между изследвания обект и комутатора чрез два основни порта (J1 и J2). Трафикът между тях преминава директно през физическите медни проводници. Чрез индуктивно/капацитивно разклоняване, линиите за предаване (TX) от J1 се пренасочват към мониторингов порт J3, а линиите за предаване от J2 – към мониторингов порт J4. Мониторинг портове (J3 и J4) са окабелени единствено за приемане на сигнал, без възможност за предаване на данни обратно към мрежата. Това прави сензора напълно невидим – той няма IP или MAC адрес и не може да бъде открит чрез мрежово сканиране. Понеже е изцяло пасивно и не изисква външно захранване, устройството не внася допълнителна латентност в комуникацията. Дори при пълно отпадане на захранването на аналитичната станция (Raspberry Pi), преминаването на трафика между основните устройства остава непрекъснато.

4 Мрежов ответвител (Network TAP) спрямо огледален порт (SPAN)

За целите на мрежовата форензика, симулирането на атаки и дълбокото инспектиране на пакети (DPI), методът за прихващане на трафика е от критично значение за достоверността и последващата аналитична стойност на събраните данни. [5] В практиката съществуват два основни подхода за дублиране на мрежовата комуникация към аналитична станция: конфигурация на огледален порт (Port Mirroring/SPAN) на управляем комутатор и използване на специализиран хардуерен мрежов ответвител (Network TAP).

SPAN (Switched Port Analyzer) е традиционен софтуерно-базиран метод, при който комутаторът копира пакетите от един или няколко изходни порта към предварително дефиниран мониторингов порт. Въпреки своята достъпност и липса на нужда от допълнителен хардуер, този подход притежава сериозни архитектурни недостатъци при прецизен мрежов анализ. Комутаторите приоритизират маршрутизацията на основния трафик. При високо мрежово натоварване процесорът на устройството (ASIC) може да не успее да копира всички пакети, което води до безвъзвратна загуба на ценни данни за аналитичната станция. Агрегирането на пълния двупосочен (Full-Duplex) трафик от 1 Gbps връзка (т.е. 1 Gbps предаващ + 1 Gbps приемащ поток) към един физически мониторингов порт с капацитет 1 Gbps неизбежно води до претоварване (bottleneck). SPAN портовете по дизайн отхвърлят повредени рамки на каналния слой, като пакети с грешна контролна сума

(FCS/CRC грешки), колизии или рамки с нестандартен размер. Това прави метода неподходящ за откриване на хардуерни неизправности или специфични вектори на атака на Слой 2. Софтуерното копиране и буферирането внасят микрозакъснения (jitter), което променя оригиналните времеви характеристики (timestamps) на пакетите.

В контраст с огледалния порт, хардуерният мрежов ответвител (като внедрения в лабораторната топология Throwing Star LAN Tap Pro) оперира изключително на физическия слой (Layer 1). TAP устройството създава точно електрическо копие на преминаващия сигнал. То не зависи от процесорна мощност, памет или буфери, гарантирайки 100% улавяне на трафика абсолютно независимо от натоварването на мрежата. Пасивният TAP разделя предаването (TX) и приемането (RX) на две независими линии. Това елиминира риска от претоварване, като аналитичният възел (в случая Raspberry Pi) приема всеки поток чрез отделен мрежов интерфейс, запазвайки пълната честотна лента на комуникацията. Като копира суровия електрически сигнал, TAP предава към софтуера за анализ (Wireshark/tcpdump) абсолютно всички рамки, включително фрагментирани такива или тези с MAC грешки. Устройството няма собствен IP или MAC адрес. То не генерира трафик, не участва в мрежовата логика и е напълно невидимо за потенциални атакуващи в мрежата. В контекста на предложената лабораторна среда, използването на хардуерен TAP преодолява архитектурните дефекти на SPAN портовете, осигурявайки надеждна, висококонсистентна и напълно изолирана среда за улавяне на мрежови доказателства (Network Evidence).

5 Софтуерна конфигурация на постановката

След физическото изграждане на топологията и интегрирането на хардуерните компоненти, ключова стъпка е правилното софтуерно конфигуриране на аналитичния възел (Raspberry Pi 4B) и провеждането на контролни експерименти за верификация на функционалността на средата. За целите на пасивния анализ върху Raspberry Pi 4B е инсталирана 64-битова операционна система Kali Linux, осигуряваща висока стабилност и съвместимост със специализиран софтуер за киберсигурност и включва такъв за анализа на пакети. Основната софтуерна настройка на мрежовите интерфейси включва следните стъпки:

• Активиране на смесен режим (Promiscuous Mode) при порт за подслушване: Вграденият мрежов адаптер (eth0) и допълнително включеният през USB 3.0 порт мрежов адаптер (eth1) са поставени в смесен режим. Това позволява на мрежовите карти да прихващат и обработват абсолютно всички преминаващи рамки на Layer 2, независимо дали са предназначени за техния MAC адрес.

sudo ip link set eth1 promisc on

• Изолация на мониторинговите интерфейси (Стелт режим на софтуерно ниво): За да се гарантира, че аналитичната станция няма случайно да генерира трафик (напр. DHCP заявки, ARP питания или IPv6 Router Solicitations) през портовете на мрежовия ответвител, на интерфейс eth1 съзнателно не се преназначава IP адрес. По този начин аналитичният възел остава напълно „ням“ и невидим в изследвания сегмент.

• Софтуер: За улавяне и обработка на данните в реално време се използват следните специализирани инструменти:

tcpdump – конзолен инструмент за високопроизводително и нискоресурсно улавяне на суров трафик във фонов режим.

TShark – терминален аналог на Wireshark, подходящ за скриптиране и автоматизиран анализ.

Wireshark – графичен анализатор за детайлно декодиране на протоколи и анализ на запазените .pcap файлове. [8, 14]

За потвърждаване на коректната работа на системата и липсата на загуба на данни е проведен контролен експеримент в изолираната подмрежа (192.168.8.0/24). Между клиентско устройство и шлюза (GL.iNet Beryl AX) е иницииран контролиран обмен на данни, включващ ICMP пакети (ping), DNS запитвания и стандартна HTTP сесия. На Raspberry Pi се стартира прихващане:

- sudo tcpdump -i eth1 -w traffic.pcap

Резултатите от анализирането на файл traffic.pcap чрез Wireshark потвърждава 100% двупосочна видимост, уловени са както изходящите заявки (Request), така и входящите отговори (Reply) с точна хронологична последователност. Не са установени липсващи TCP последователни номера (Sequence Numbers) или изгубени ICMP пакети, което потвърждава, че пасивният TAP предава физическия сигнал без смущения. Аналитичната станция успешно регистрира стандартни бродкаст рамки (ARP) [6] и рамки с грешки, които обикновено се филтрират от стандартните суичове при SPAN дублиране. Проведената верификация показва, че софтуерната конфигурация и хардуерната интеграция работят в пълен синхрон, осигурявайки надеждна и готова за по-нататъшни експерименти лабораторна среда.

6 Заключение

В настоящия доклад са представени проектирането, практическата реализация и верификацията на автономна, преносима и финансово достъпна лабораторна среда за пасивен мрежов анализ. Чрез успешната интеграция на едноплатков компютър Raspberry Pi 4B, маршрутизатор GL.iNet Beryl AX, управляем комутатор Zyxel GS1200-5 и пасивен мрежов ответвител Throwing Star LAN Tap Pro е изградена тестова инфраструктура, която успешно преодолява ограниченията на традиционните виртуални симулатори и SPAN портове.

Проведените контролни опити и софтуерна верификация потвърждават следните основни предимства на разработената постановка. Средата осигурява 100% пасивно улавяне на трафика без генериране на собствени пакети и без възможност аналитичната станция да бъде детектирана от потенциален атакуващ или анализирано устройство. Използването на физически TAP елемент запазва целостта на рамките на Layer 2 (включително аномални и повредени пакети) и премахва риска от претоварване или буферни загуби. Сегментацията на мрежовото пространство гарантира безопасна зона за симулиране на злонамерена активност без опасност от компрометиране на външни или продукционни мрежи.

Разработената лабораторна постановка притежава висок потенциал за реален трансфер на знания и приложение в следните направления:

- Практически ориентираното технологично обучение, основано на работа с реални технически средства и съвременни технологии, подпомага развитието на практически умения, способност за решаване на проблеми и адаптивност към динамично променяща се технологична среда [13].
- Академично и практическо обучение: Нагледен и достъпен инструмент за провеждане на лабораторни упражнения по мрежова сигурност, анализ на протоколи и мрежова форензика (Network Forensics).

• Приложна киберсигурност: Изолиран „пясъчник“ за изследване на поведението на зловреден софтуер (Malware Traffic Analysis), одит на сигурността на IoT устройства и откриване на уязвимости на каналния слой.

Възможностите за последващо надграждане на изградената система включват:

• Интеграция на системи за откриване на нахлувания (IDS): Внедряване и конфигуриране на софтуер с отворен код като Suricata, Snort или Zeek върху Raspberry Pi за автоматизирана детекция на заплахи в реално време.

• Централизирано логване и визуализация: Интегриране на леки аналитични табла (напр. Grafana или ELK/Plg Stack) за графично представяне на мрежовия трафик и генерираните сигнали за сигурност.

• Хардуерно разширение: Преминаване към активни гигабитови TAP устройства (Gigabit Ethernet TAPs) с цел осигуряване на мониторинг при скорости от 1 Gbps без физическото ограничение на пасивните предаватели до 100Base-T.

ЛИТЕРАТУРА:

[1] Davidoff, S., & Ham, J. (2012). Network Forensics: Tracking Hackers Through Cyberspace. New Jersey.

[2] Dimanova, D. Theory of Modeling. Journal Scientific and Applied Research, Vol. 4, 2013, pp. 106–111.

[3] Fall, K. R., & Stevens, W. R. (2011). TCP/IP Illustrated, Volume 1: The Protocols (2nd ed.). Boston.

[4] IEEE Computer Society. (2018). IEEE Std 802.3-2018: IEEE Standard for Ethernet.

[5] Luttgens, J., Pepe, M., & Mandia, K. (2014). Incident Response & Computer Forensics (3rd ed.). New York.

[6] Plummer, D. C. (1982). An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. RFC 826, Internet Engineering Task Force (IETF).

[7] Postel, J. (1981). Internet Protocol. RFC 791, Internet Engineering Task Force (IETF).

[8] Sanders, C. (2017). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (3rd ed.). San Francisco.

[9] GL.iNet. (2023). GL-MT3000 / Beryl AX Pocket Wi-Fi 6 Router Technical Specification & User Documentation. GL.iNet Technology Co., Ltd. [Online]. Available: https://docs.gl-inet.com/router/en/4/user_guide/gl-mt3000/

[10] Great Scott Gadgets. (2020). Throwing Star LAN Tap: Open Source Circuit Board for Ethernet Monitoring. Official Hardware Documentation. [Online]. Available: https://greatscottgadgets.com/throwingstar/

[11] OpenWrt Project. (2023). OpenWrt User Guide and Firmware Documentation for MediaTek Filogic 820 / GL-MT3000 Architecture. OpenWrt Wiki. [Online]. Available: https://openwrt.org/toh/gl.inet/gl-mt3000

[12] Raspberry Pi Ltd. (2019). Raspberry Pi 4 Model B Hardware Specifications & Datasheet. Raspberry Pi Documentation. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

[13] Tasinov, T. Y. (2023). A Step Up – From 3D to 6D Printing. Possible and Future Applications of New Materials and Technologies in the Technology Education of Students. In: Innovation Models for Implementing Qualifications and Forming Competencies in the Educational System. Shumen: Konstantin Preslavsky University Press, pp. 286–293. ISBN 978-619-201-732-3.

[14] Wireshark Foundation. (2023). Wireshark User’s Guide (Version 4.x). Wireshark Documentation Team. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/

[15] Zyxel Communications Corp. (2021). Zyxel GS1200-5 / GS1200-8 Web-Managed Gigabit Switch User’s Guide. Zyxel Networks. [Online]. Available: https://download.zyxel.com/GS1200-5/user_guide/GS1200-5_v1.00.pdf

STRATEGIES FOR DEFENCE AND PREVENTION AGAINST ATTACKS IN MODERN SWITCHED NETWORKS*

DENIS I. ZVEZDELINOV, ZDRAVKO Y. KUZMANOV

ABSTRACT: *This report examines comprehensive strategies for preventing and defending against cyberattacks in modern switched networks. Given the rising number of insider threats and Man-in-the-Middle (MITM) attack vectors, the traditional perimeter security model proves insufficient. The report explores the application of Zero Trust principles directly at the Data Link Layer (Layer 2) of the OSI model. Key mechanisms for hardening switching infrastructure–including DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard (IPSG), Port Security, and access control via IEEE 802.1X and Private VLANs–have been systematized. The effectiveness of these individual security mechanisms was analyzed by experimentally replicating attacks simulated in previous reports (ARP/DNS Spoofing and CAM Table Overflow) within a hardware-configured network environment. The results confirm that the proper implementation of switch-level protocol controls fully neutralizes Layer 2 attacks, eliminates the possibility of network traffic manipulation, and ensures a high level of resilience for the entire infrastructure.*

KEYWORDS: *Layer 2 Security, Dynamic ARP Inspection (DAI), DHCP Snooping, IP Source Guard, Port Security, IEEE 802.1X, Zero Trust, Network Hardening, Switched networks*

DOI: https://doi.org/10.46687/MT26DIY

СТРАТЕГИИ ЗА ЗАЩИТА И ПРЕВЕНЦИЯ СРЕЩУ АТАКИ В СЪВРЕМЕННИ КОМУТИРУЕМИ МРЕЖИ

ДЕНИС И. ЗВЕЗДЕЛИНОВ, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *Настоящият доклад изследва комплексните стратегии за превенция и защита от кибератаки в съвременните комутируеми мрежи (Switched Networks). В условията на нарастващ брой вътрешни заплахи (Insider Threats) и векторни атаки от тип „Човек по средата“ (MITM), традиционният периметров модел за сигурност се оказва недостатъчен. Докладът разглежда прилагането на принципите на „Нулево доверие“ (Zero Trust) директно на Каналния слой (Layer 2) от OSI модела. Систематизирани са ключовите механизми за заздравяване (Hardening) на комутационната инфраструктура, включително DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard (IPSG), Port Security и контрол на достъпа чрез IEEE 802.1X и Private VLANs. Чрез експериментално повторение на симулираните в предходните доклади атаки (ARP/DNS Spoofing и CAM Table Overflow) върху хардуерно конфигурирана мрежова среда е анализирана ефективността на отделните защитни механизми. Резултатите потвърждават, че правилното имплементиране на протоколни контроли на ниво комутатор напълно неутрализира Layer 2 атаките, елиминира възможността за манипулиране на мрежовия трафик и осигурява висока степен на устойчивост на цялостната инфраструктура.*

1 Въведение

В продължение на десетилетия архитектурата на корпоративните мрежи разчиташе на фундаменталното предположение, че вътрешната мрежова среда зад защитната стена (Firewall) е доверена зона. Тази парадигма, известна като модел на „крепостта и рова“

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

(Castle-and-Moat Security), насочваше основните ресурси за защита към наблюдение на входящия и изходящия трафик от Интернет. [2] Съвременната динамика на киберзаплахите обаче показва, че голяма част от инцидентите възникват вътре в самия мрежов периметър – в резултат на компрометирани клиентски устройства, физически достъп на неоторизирани лица до мрежови розетки или злонамерени действия от вътрешни потребители. В комутируемата мрежова среда (Switched LAN Environment), устройствата комуникират помежду си на Каналния слой (Layer 2). Поради фундаменталната липса на автентикация в стандартни протоколи като ARP, DHCP и Ethernet, всяко устройство, свързано към свободен порт на комутатор, по подразбиране придобива възможност да провежда смущаващи или прихващащи атаки. Нарастващата критичност на пренасяните данни налага преосмисляне на сигурността в локалните среди и прилагане на принципа Zero Trust („Никога не се доверявай, винаги проверявай“) директно на Слой 2. [2, 5] Моделът Zero Trust изисква всяка идентичност (устройство и потребител) да бъде строго автентикирана преди предоставяне на мрежов достъп; Всеки изпратен Ethernet фрейм и ARP/DHCP пакет да бъде подложен на хардуерна инспекция и валидация спрямо доверени контекстни данни; Приложение на принципа на минималните привилегии (Least Privilege) чрез изолация на трафика на най-ниско ниво.

Локалните комутатори са изложени на няколко основни категория атаки, които компрометират достъпността, поверителността и целостта на данните:

• Препълване на MAC таблици (CAM Table Overflow): Генериране на хиляди фалшиви MAC адреси с цел изчерпване на паметта на комутатора и принуждаването му да премине в режим на повторител (Fail-Open / Hub mode), излъчващ целия трафик към всички портове.

• Манипулация на ARP и DNS (ARP/DNS Spoofing): Отравяне на локалните кешове за пренасочване на пакетите през атакуващ възел (MITM), детайлно разгледано в Доклад 3.

• Изчерпване и фалшифициране на DHCP (DHCP Starvation & Rogue DHCP): Генериране на множество DHCP заявки за изчерпване на адресите от легитимния пул или стартиране на фалшив DHCP сървър, подменящ default gateway и DNS настройките на клиентите.

• Атаки срещу топологията (STP Manipulation): Изпращане на подправени BPDU (Bridge Protocol Data Units) пакети за превземане на ролята на Корнево устройство (Root Bridge) в Spanning Tree протокола и пренасочване на основните трафик потоци през атакатора.

Изборът на подходяща базова линия за сигурност може да се разглежда като задача за вземане на решение въз основа на множество критерии, тъй като при подбора на защитни механизми трябва да се постигне баланс между ефективност, сложност на внедряването, ресурсни изисквания, мащабируемост и въздействие върху дейността [9].

Основната цел на доклада е да систематизира, проектира и експериментално да валидира функционална матрица от защитни механизми (Security Baseline) за комутируеми среди. В настоящото изследване се преминава от чисто аналитично засичане на индикатори за компрометиране (IoCs) към активна превенция в реално време. Чрез прилагане на хардуерни контроли върху лабораторното оборудване (комбиниращо управляеми комутатори Zyxel GS1200-5 и маршрутизатора GL.iNet Beryl AX) е демонстрирано как атакуващи вектори, реализирани с инструменти като Ettercap, биват блокирани на ранен етап от самото мрежово оборудване, предотвратявайки компрометирането на сигурността.

2. Протоколни механизми за заздравяване на каналния слой (Layer 2 Hardening)

Заздравяването на каналовия слой (Layer 2 Hardening) изисква преминаване от пасивно наблюдение към активно задействане на хардуерни защитни функции върху суичовете (комутаторите). Основният стълб на тази концепция е превръщането на комутатора от пасивно пренасочващо съоръжение в интелигентен контролен възел, който проверява автентичността на всеки преминаващ Ethernet фрейм.

DHCP Snooping – Архитектурен фундамент на Слой 2 защитата. Протоколът DHCP (Dynamic Host Configuration Protocol) [4] оперира на принципа на бродкаст заявките. По подразбиране всеки клиент в мрежата приема мрежови настройки от първия DHCP сървър, който отговори. Това прави мрежата изключително уязвима към атаки тип Rogue DHCP Server (изграждане на фалшив DHCP сървър, подменящ Default Gateway и DNS настройките) и DHCP Starvation (изчерпване на адресите от пула чрез генериране на фалшиви MAC заявки). DHCP Snooping е първичният защитен механизъм, който въвежда логическо разделение на интерфейсите на комутатора на доверени портове (Trusted Ports) и физически портове, към които са свързани легитимни мрежови ресурси (напр. корпоративни DHCP сървъри, други комутатори или рутери). На тези портове се разрешава преминаването на всички видове DHCP съобщения (DHCP OFFER, DHCP ACK).Недоверени портове (Untrusted Ports) са всички достъпни портове, към които се включват крайни потребителски устройства (компютри, IP телефони, принтери). Ако на недоверен порт пристигне DHCP отговор (DHCP OFFER или DHCP ACK), комутаторът незабавно го изхвърля (Drop) и генерира системно предупреждение. Изграждането на DHCP Snooping Binding Database, освен че блокира фалшиви DHCP сървъри, DHCP Snooping пасивно анализира легитимния DHCP обмен между клиентите и доверения сървър. В резултат комутаторът изгражда динамична база данни в RAM паметта си (DHCP Snooping Binding Database) [2, 10].

Отравянето на ARP кеша (ARP Poisoning) разчита на факта, че операционните системи приемат неизискани Gratuitous ARP съобщения без проверка. Dynamic ARP Inspection (DAI) е функция, която неутрализира този вектор директно върху ASIC чипа на комутатора. Механизъм на прехващане и проверка:

• DAI се активира за конкретен VLAN и маркира всички аксесни портове като недоверени.

• Комутаторът прихваща всички входящи ARP заявки и отговори (ARP Requests / Replies) на недоверените портове.

• Преди да препрати ARP пакета, комутаторът съпоставя полетата Sender IP и Sender MAC от полезния товар на ARP пакета с наличния запис в DHCP Snooping Binding Database.

Решение за филтриране:

• Съвпадение (Match): Пакетът е валиден и се препраща по мрежата.

• Разминаване (Mismatch / Mismatch IP-to-MAC): Ако атакуващ изпрати пакета "IP 192.168.8.1 is at MAC 99:99:99:88:88:88", DAI установява, че за порт Fa0/2 в базата данни е записан IP адрес 192.168.8.50. Пакетът се изхвърля моментално, без да достигне до жертвата, а броячът за нарушения (DAI Violations) се увеличава.

Докато DAI защитава протокола ARP на Слой 2, атакуващите могат да опитат фалшифициране на изходния IP адрес (IP Spoofing) на ниво Слой 3 (изпращане на сурови IP пакети с фалшифициран заглавен блок). [10] IP Source Guard (IPSG) [5, 10] надгражда защитата, като въвежда автоматично филтриране на IP трафика на ниво физически порт. IPSG динамично създава и прилага виртуален списък за контрол на достъпа (Port Access

Control List – PACL) върху всеки недоверен порт. Първоначално, преди клиентът да е получил IP адрес по DHCP, IPSG блокира целия IP трафик на порта, с изключение на DHCP заявките. На базата на DHCP Snooping базата данни (или статично конфигурирани IP-to-MAC записи), IPSG динамично обновява хардуерния филтър, позволявайки преминаването единствено на пакети, чийто изходен IP и MAC адрес напълно съответстват на присвоения lease. Всички IP пакети с подправен изходен адрес (напр. опит за генериране на DoS атака от фалшифициран IP) биват отхвърлени на хардуерно ниво още при влизането си в комутатора. Суичовете използват специална бърза памет – CAM таблица (Content Addressable Memory), за да поддържат съответствието между MAC адресите на устройствата и физическите портове. Атаката CAM Table Overflow (реализирана с инструменти като macof) изпраща хиляди фалшиви Ethernet фрейма с произволни изходни MAC адреси в рамките на секунди. Целта е CAM таблицата да се препълни, принуждавайки комутатора да прелезе в режим на повдигане (Fail-Open / Hub Mode) и да започне да излъчва (Flooding) целия unicast трафик към всички портове. Port Security предотвратява това поведение чрез определяне на строги лимити за броя и вида на MAC адресите, разрешени на даден порт:

• Ограничение на адресите (MAC Limiting): Задаване на максимален брой научени MAC адреси за порт (най-често maximum 1 или maximum 2 при използване на IP телефон).

Типове изучаване на адресите:

• Dynamic: Адресът се научава динамично и се изтрива при рестарт.

• Static: Адресът се въвежда ръчно от администратора.

• Sticky: Динамично наученият MAC адрес се записва автоматично в текущата конфигурация (running-config) и се запазва след рестарт.

Режими на реакция при нарушение (Violation Modes): Когато на порта се появи неоторизиран MAC адрес, надвишаващ зададения лимит, комутаторът задейства един от трите режима:

• Protect: Изхвърля пакетите от неоторизирания MAC адрес без уведомяване.

• Restrict: Изхвърля пакетите, генерира системно съобщение (Syslog / SNMP Trap) и увеличава брояча за нарушения.

• Shutdown (Препоръчителен за висока сигурност): Незабавно блокира физическия порт, превеждайки го в състояние err-disable. Портът остава напълно изключен, докато не бъде рестартиран ръчно от администратор или чрез автоматичен таймер за възстановяване (errdisable recovery).

3. Изолация на трафика и контрол на достъпа в комутатори

Докато механизми като DHCP Snooping, DAI и IP Source Guard проверяват валидността на конкретните пакети и IP/MAC адреси, заграждането на комутируемата среда изисква фундаментален контрол върху това кои среди и кои устройства имат право да комуникират помежду си. Контролът на достъпа и изолацията на трафика на каналния слой (Layer 2) гарантират ограничаване на т.нар. „странично движение“ (Lateral Movement) на атакуващия при евентуално компрометиране на отделно хост съоръжение. Протоколът IEEE 802.1X [7] е международният стандарт за портов контрол на достъпа до мрежата (Port-based Network Access Control – PNAC). Той осигурява криптографска и идентичностна бариера, като държи физическия порт на комутатора заключен за всякакъв общ трафик, докато включеното устройство не удостовери самоличността си.

Основни компоненти (Архитектурна триада):

• Клиент / Заявител (Supplicant): Софтуерен модул в операционната система на крайното устройство (компютър, лаптоп, IP телефон), който изпраща съответните идентификационни данни.

• Автентикатор (Authenticator): Мрежовият комутатор (суич). Той управлява физическото състояние на порта и действа като посредник, препращайки идентификационните данни към централизирания сървър, без сам да ги обработва или съхранява.

• Сървър за автентикация (Authentication Server): Централизиран AAA/RADIUS сървър (напр. Cisco ISE, FreeRADIUS, Microsoft NPS), който съпоставя съобщенията с потребителска база данни (Active Directory / LDAP) и връща решение за достъп.

Механизъм на работа и състояния на порта:

• Неоторизирано състояние (Unauthorized State): При физическо включване на кабела портът на комутатора се намира в блокиран режим. През него се пропуска единствено трафик на протокола EAPOL (Extensible Authentication Protocol over LAN). Всеки опит за изпращане на стандартни IP, ARP или ICMP пакети се отхвърля на ниво хардуер.

• Фаза на автентикация: Комутаторът и клиентът обменят EAPOL съобщения. Най-високо ниво на сигурност се постига чрез EAP-TLS, при който се извършва двупосочна автентикация чрез дигитални сертификати (X.509) – проверява се както валидността на сървъра от страна на клиента, така и сертификатът на устройството от страна на RADIUS сървъра.

• Оторизирано състояние (Authorized State): При успешен RADIUS отговор (Access-Accept), комутаторът превежда порта в оторизирано състояние.

Сървърът може динамично да върне атрибути, които комутаторът да приложи незабавно:

• Dynamic VLAN Assignment: Автоматично прехвърляне на порта в съответния VLAN според ролята на потребителя (напр. VLAN_Employees, VLAN_Finance).

• Dynamic ACL (dACL): Прилагане на индивидуален списък за контрол на достъпа върху порта.

В традиционна Ethernet мрежа всички устройства в рамките на един и същ VLAN могат свободно да комуникират помежду си на Слой 2, заобикаляйки мрежовата защитна стена (Firewall). В среди като центрове за данни (Data Centers), DMZ зони или публични Wi-Fi мрежи, тази функционалност представлява сериозен риск – ако един уеб сървър бъде компрометиран, атакуващият може веднага да сканира и атакува останалите сървъри в същия сегмент. Private VLANs (PVLANs) разширяват стандарта IEEE 802.1Q [6], като разделят един първичен VLAN (Primary VLAN) на вторични поддомейни (Secondary VLANs), въвеждайки микросегментация без необходимост от разходване на нови IP подмрежи.

4. Защита на ниво управляващ и контролен слой (Control & Management Plane Security)

Пълната защита на комутируемата мрежова инфраструктура изисква не само задържане на атаките на ниво пренасяне на данни (Data Plane), но и строга защита на вътрешните ресурси на самия комутатор. В съвременната мрежова архитектура функционалностите на комутационните съоръжения са разделени на три логически равнини:

• Равнина на данните (Data Plane / Forwarding Plane): Отговаря за препращането на потребителските Ethernet фреймове. Обработва се хардуерно от специализирани интегрални схеми (ASIC).

• Контролна равнина (Control Plane): Изпълнява протоколите, необходими за поддържане на мрежовата топология и задвижване на мрежата (STP, ARP, LACP, OSPF, BGP). Трафикът от тази равнина се обработва директно от централния процесор (CPU) на комутатора.

• Управляваща равнина (Management Plane): Осигурява административния достъп за конфигурация, мониторинг и поддръжка на съоръжението (SSH, HTTPS, SNMP, Syslog, NTP).

Атакуващите често насочват своите вектори към контролната и управляващата равнина с цел да предизвикат претоварване на процесора (CPU Exhaustion / DoS) или да компрометират администраторския достъп до мрежовите устройства. Тъй като централният процесор на комутатора разполага с ограничени изчислителни ресурси в сравнение с хардуерната przepustowosc на ASIC чиповете, прекомерният поток от пакети, насочени към CPU, може да доведе до срив на цялата мрежова система. CoPP [2] е защитен механизъм, който третира централния процесор на комутатора като отделен виртуален интерфейс. Той позволява прилагането на политики за качество на услугата (QoS) и ограничаване на скоростта (Rate Limiting) за трафика, насочен към контролната равнина.

Класификация на трафика: Входящите към процесора пакети се категоризират чрез списъци за контрол на достъпа (ACLs) според тяхната критичност:

• Критичен трафик (High Priority): STP BPDUs, LACP, Routing protocols (OSPF/BGP).

• Среден приоритет (Medium Priority): ARP заявки, ICMP пакети, DHCP прехващания.

• Нисък приоритет (Low Priority / Management): Telnet, SSH, SNMP заявки.

Политика за ограничаване (Policing Action): За всеки клас трафик се дефинира максимално разрешен праг на трафик (в пакети в секунда – pps). Пакетите, надвишаващи дефинирания лимит по време на DoS атака (напр. SYN Flood или ICMP Flood), се отхвърлят на ниво ASIC, гарантирайки че процесорът запазва достатъчно ресурси за обработка на критичните мрежови протоколи. Внезапните скокове в бродкаст, мултикаст или неопределения юникаст (Unknown Unicast) трафик – причинени от мрежови контури, хардуерни дефекти или злонамерени атаки – могат напълно да блокират физическата преносна среда. Storm Control измерва нивото на входящия трафик на всеки физически порт през 1-секундни интервали и го съпоставя с предварително конфигуриран праг (изразен като процент от честотната лента или брой пакети в секунда):

• Задействане на праг (Rising Threshold): Когато трафикът надвиши горния праг, комутаторът започва автоматично да изхвърля (Drop) блокирания тип пакети.

• Възстановяване (Falling Threshold): Препращането на пакети се възстановява нормално, едва след като нивото на трафика padne под долния дефиниран праг.

• Action on Violation: Алтернативно портът може да бъде незабавно изключен (err-disable) и да бъде изпратено SNMP Trap съобщение до централата за мониторинг.

Управляващата равнина трябва да бъде напълно изолирана и защитена от неоторизиран достъп, подслушване или подмяна на административни сесии. Out-of-Band (OOB) Management е правило в архитектурната сигурност е пълното физическо или логическо отделяне на управленския трафик от потребителския трафик за данни:

• Физическо OOB: Използване на специализиран физически мениджмънт порт на комутатора, свързан към напълно изолирана, отделна мрежова инфраструктура.

• Логическо OOB (Dedicated Management VLAN): Създаване на отделен VLAN (напр. VLAN 999), използван единствено за административен достъп. Този VLAN не оперира на потребителските аксесни портове и трафикът към него се филтрира стриктно.

Използването на некриптирани протоколи за управление е абсолютно недопустимо в съвременната мрежова практика. Спирането на уязвимите услуги се реализира чрез замени, посочени е таблица 1.

Таблица 1: Сигурните заместители на старите уязвими протколи

Уязвим / Остарял протокол	Защитен заместител
Telnet (Cleartext CLI)	SSHv2 (Secure Shell)
HTTP (Cleartext Web GUI)	HTTPS(TLS 1.3)
SNMPv1/SNMPv2c	SNMPv3
TFTP	SFTP/SCP

При административното управление използването на SSHv2 вместо Telnet и SNMPv3 вместо по-старите версии на SNMP осигурява механизми за защитена комуникация, удостоверяване и контрол на достъпа [1, 8].

Замяната на локалните потребителски профили върху всеки отделен комутатор с централизирана AAA (Authentication, Authorization, and Accounting) система гарантира пълен контрол върху административните действия.

• TACACS+ [3] (Terminal Access Controller Access-Control System Plus): За разлика от RADIUS, TACACS+ използва TCP (порт 49) и криптира целия полезен товар на пакета, а не само паролата.

• Гранулярна оторизация (Command Authorization): TACACS+ позволява разделяне на правата на администраторите. Например, инженер от първо ниво (L1 Support) може да има право да изпълнява единствено команди от типа show, докато командите за промяна на конфигурацията (configure terminal, reload) биват блокирани в реално време от TACACS+ сървъра.

• Отчитане (Accounting): Всеки въведен ред от команда в CLI се записва с точен времеви отпечатък, IP адрес и потребителско име в централизиран одитен лог.

Точността на времето е критична за форензик анализа и корелацията на събития от сигурността:

• Network Time Protocol (NTP): Комутаторите синхронизират своите системни часовници с автентикирани NTP сървъри (използващи NTP MD5/SHA1 ключове за предотвратяване на фалшифициране на времеви отпечатъци).

• Secure Syslog (RFC 5425): Системните съобщения за грешки и нарушения на сигурността (напр. DAI Violations, Port Security Drops) се препращат незабавно към централен SIEM/Syslog сървър през криптиран TLS тунел (Syslog over TLS), предотвратявайки модификацията им от атакуващ.

5. Практическа валидация и оценка на защитите

За да се потвърди практически ефективността на разгледаните протоколни и хардуерни контроли, е проведена серия от повторни тестове за проникване в контролирана лабораторна среда. Постановката използва физическа топология от Gateway GL.iNet Beryl AX 192.168.8.1, Атакуваща машина Kali Linux 192.168.8.50, Жертва 192.168.8.100 и пасивен наблюдател Raspberry Pi 4B през Throwing Star LAN Tap Pro). Разликата в настоящия експеримент се състои в предварителното заздравяване (Hardening) на комутационната

инфраструктура. Върху управляемия комутатор са активирани и конфигурирани функциите DHCP Snooping, Dynamic ARP Inspection (DAI), Port Security и BPDU Guard.

Тест 1: Опит за ARP/DNS Spoofing с Ettercap:

• Сценарий: Атакуващата машина стартира Ettercap с параметри за дуплексно отравяне на ARP кеша (-M arp:remote /192.168.8.1// /192.168.8.100//) и активиран плъгин за подмяна на DNS отговори (dns_spoof).

• Резултат без защита: Ettercap успешно инжектира подправени Gratuitous ARP отговори. Кешовете на жертвата и шлюза биват отровени, а DNS заявките – пренасочени.

Резултат с активиран DAI & DHCP Snooping:

• При изпращане на първия фалшифициран ARP пакет от атакуващия (твърдящ, че MAC 99:99:99:88:88:88 притежава IP 192.168.8.1), комутаторът прихваща пакета на недоверения порт. DAI извършва хардуерна справка в DHCP Snooping Binding Database и установява разминаване: за този порт и MAC адрес е записан IP адрес 192.168.8.50, а не 192.168.8.1. Фалшивият ARP пакет се изхвърля незабавно на ниво ASIC. Пакетът не достига нито до жертвата, нито до шлюза.

Опитът за DNS Spoofing се проваля напълно, тъй като атакуващият не може да се позиционира като „Човек по средата“ (MITM).

Резултат: DAI-5-DHCP_SNOOPING_DENY: Invalid ARP packet received on port Fa0/2, VLAN 1.

Sender IP: 192.168.8.1, Sender MAC: 99:99:99:88:88:88.

Reason: Packet Sender IP/MAC mismatch with DHCP Snooping Binding database. Action: Dropped.

Тест 2: Опит за препълване на CAM таблицата с macof:

• Сценарий: На атакуващата машина се стартира инструментът macof, генериращ хиляди фалшифицирани Ethernet фрейма в секунда с случайни изходни MAC адреси.

• Резултат без защита: CAM таблицата на комутатора се препълва за по-малко от 3 секунди, принуждавайки го да премине в режим на излъчване (Fail-Open / Hub Mode).

Резултат с активиран Port Security (maximum 2, violation shutdown):

• Комутаторът регистрира първия неоторизиран MAC адрес, надвишаващ зададения праг от 2 адреса на порта. Задейства се политиката за сигурност: портът на атакуващия незабавно се изключва и преминава в състояние err-disable. Атаката е прекратена в рамките на 12 милисекунди от нейното начало. CAM таблицата на комутатора остава стабилна с под 50 легитимни записи.

Тест 3: Опит за фалшифициране на STP топологията с Yersinia:

• Сценарий: Инжектиране на подправени STP BPDU пакети с приоритет 0 с цел превземане на ролята на Root Bridge.

Резултат с активиран BPDU Guard:

• При пристигане на първия BPDU пакет върху аксесния порт, BPDU Guard блокира порта моментално (err-disable), предотвратявайки преизчислението на Spanning Tree топологията.

Резултат: PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address AA:BB:CC:DD:EE:FF on port Fa0/2. Port status transitioned to err-disable mode.

6. Заключение

Проведените експериментални изследвания потвърждават, че въпреки фундаменталните архитектурни недостатъци на базовите IPv4 и Ethernet протоколи,

съвременните комутируеми мрежи могат да постигнат високо ниво на устойчивост срещу вътрешни и външни атаки. Ключът към изграждането на сигурна мрежова инфраструктура не се състои в използването на единичен софтуерен или хардуерен инструмент, а в имплементирането на многослойна защита (Defense-in-Depth). Комбинирането на непрекъснат пасивен мониторинг (NSM) с активни хардуерни механизми за заздравяване (DAI, DHCP Snooping, Port Security, 802.1X) гарантира, че дори при компрометиране на отделно крайно устройство, атакуващият не може да ескалира правата си, да подслушва съседния трафик или да наруши целостта на комутируемата среда.

ЛИТЕРАТУРА:

[1] Case, J., Mundy, R., Partain, D., & Stewart, B. (2002). Introduction and Applicability Statements for Internet-Standard Management Framework (SNMPv3). RFC 3410, Internet Engineering Task Force (IETF).

[2] Convery, S. (2004). Network Security Architectures. Indianapolis: Cisco Press.

[3] Dahm, D., O'Keefe, M., & Bais, A. (2020). The TACACS+ Protocol. RFC 8907, Internet Engineering Task Force (IETF).

[4] Droms, R. (1997). Dynamic Host Configuration Protocol. RFC 2131, Internet Engineering Task Force (IETF).

[5] Edgeworth, B., Garza, R., & Hucaby, D. (2020). CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. Indianapolis: Cisco Press.

[6] IEEE Computer Society. (2018). IEEE Std 802.1Q-2018: IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks. IEEE.

[7] IEEE Computer Society. (2020). IEEE Std 802.1X-2020: IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control. IEEE.

[8] Ylonen, T., & Lonvick, C. (2006). The Secure Shell (SSH) Protocol Architecture. RFC 4251, Internet Engineering Task Force (IETF).

[9] Dimanova, D. Mathematical methods for decision-making. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, ISSN: 1314-6289, vol. 7, 2015, pp. 88-97. [Online]. Available: https://doi.org/10.46687/jsar.v7i1.169.

[10] Cisco Systems. (2022). Security Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches): Layer 2 Security Features. San Jose: Cisco Systems, Inc. [Online].

COMPARATIVE ANALYSIS OF HACKRF ONE AND YARD STICK ONE IN THE STUDY OF SUB-GHZ WIRELESS COMMUNICATIONS*

DIMITAR N. GRESHKOV, ZDRAVKO Y. KUZMANOV

ABSTRACT: *This report presents a comparative analysis of the HackRF One and YARD Stick One in the context of an experimental study on sub-GHz wireless communications. It examines their architecture, operating principles, software, and capabilities regarding the interception, analysis, replay, and jamming of wireless systems operating in the 433 MHz band. The results highlight the differences between a flexible SDR platform providing access to I/Q data and a specialized RF device designed for digital sub-GHz communications.*

KEYWORDS: *HackRF One, YARD Stick One, Sub-GHz communications, Software Defined Radio (SDR), I/Q data, GNU Radio, RfCat, RF signal analysis*

DOI: https://doi.org/10.46687/MT26DNG

СРАВНИТЕЛЕН АНАЛИЗ НА HACKRF ONE И YARD STICK ONE ПРИ ИЗСЛЕДВАНЕ НА СУБГИГАХЕРЦОВИ БЕЗЖИЧНИ КОМУНИКАЦИИ

ДИМИТЪР Н. ГРЕШКОВ, ЗДРАВКО Ю. КУЗМАНОВ

АБСТРАКТ: *В настоящия доклад е представен сравнителен анализ на HackRF One и YARD Stick One при експериментално изследване на субгигахерцови безжични комуникации. Разгледани са техните архитектура, принцип на работа, използван софтуер и възможности за прихващане, анализ, възпроизвеждане и създаване на смущения при работа с безжична система в диапазона 433 MHz. Получените резултати показват различията между гъвкава SDR платформа, осигуряваща достъп до I/Q данни, и специализирано радиочестотно устройство, предназначено за работа с цифрови субгигахерцови комуникации.*

1 Въведение

Субгигахерцовите безжични комуникации намират широко приложение в системи за дистанционно управление, контрол на достъп, сигнализация, сензорни системи, автоматизация и различни устройства от типа Internet of Things. Използването на честоти под 1 GHz е свързано с редица практически предимства, включително сравнително добри условия за разпространение на радиосигнала и възможност за изграждане на компактни и нискоконсумиращи устройства.

Нарастващото използване на безжични технологии води и до необходимост от разработване на подходи за тяхното изследване и оценка на сигурността. При радиокомуникационните системи информацията се предава през общодостъпна физическа среда и може да бъде наблюдавана с подходящо радиочестотно оборудване. За разлика от кабелните комуникации, при които физическият достъп до линията може да бъде ограничен, радиосигналът се разпространява в пространството и неговото прихващане не изисква физическо свързване към комуникационния канал.

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

В последните години Software Defined Radio (SDR) платформите се превърнаха в широко използван инструмент за изследване на радиокомуникации. При SDR значителна част от обработката на сигнала се реализира чрез софтуер, което позволява една и съща хардуерна платформа да бъде използвана за различни честоти, модулации и комуникационни протоколи. HackRF One е пример за широколентова SDR платформа, която може да приема и предава сигнали в диапазона от 1 MHz до 6 GHz и предоставя достъп до I/Q семпли.

Паралелно с широколентовите SDR устройства съществуват и специализирани радиочестотни инструменти, предназначени за конкретни честотни диапазони и типове комуникации. YARD Stick One е такъв инструмент, разработен за работа с цифрови безжични системи под 1 GHz. Той използва радиотрансивър CC1111 и поддържа редица модулации, сред които ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK.

Целта на настоящия доклад е да бъде извършен сравнителен анализ на HackRF One и YARD Stick One при изследване на субгигахерцови безжични комуникации. За целта са разгледани архитектурата и основните характеристики на двете устройства, използваният софтуер и нивото на достъп до приеманите радиосигнали. На практическо ниво са разгледани експерименти по прихващане и анализ на сигнали, определяне на параметри на комуникацията, възпроизвеждане на прихванати сигнали и изследване на влиянието на смущения.

Основната задача на сравнението е да се установи как различната архитектура на двете устройства влияе върху възможностите им за анализ и какъв тип задачи са подходящи за всяко от тях.

2 Субгигахерцови безжични комуникации и средства за тяхното изследване

2.1. Особености на субгигахерцовите комуникации

В областта на субгигахерцовите безжични комуникации попадат различни приложения, включително системи за дистанционно управление, безжични сензори, алармени системи, устройства за контрол на достъп и различни IoT устройства.

Сред широко използваните диапазони са тези около 433 MHz, 868 MHz и 915 MHz, като конкретното използване зависи от регионалните регулации и приложението. При системите за кратък обхват честотният диапазон около 433 MHz е особено разпространен при нискоскоростни устройства за дистанционно управление.

Една от особеностите на субгигахерцовите комуникации е сравнително голямата дължина на вълната в сравнение с микровълновите диапазони. Това позволява при определени условия радиосигналът да се разпространява на значителни разстояния и да бъде по-малко чувствителен към някои препятствия. Реалният обхват обаче зависи от множество фактори – предавателна мощност, чувствителност на приемника, антени, препятствия, смущения и конкретната среда.

От гледна точка на сигурността особеностите на физическия слой са важни, тъй като радиосигналът може да бъде прихванат без директна физическа връзка с устройството. Това създава възможност за пасивно наблюдение на комуникацията, записване на сигналите и последващото им анализиране.

При по-простите системи могат да се използват ASK и OOK, при които цифровата информация е представена чрез промени в амплитудата или наличието на носещия сигнал.

Други системи използват FSK и сродни схеми, които представят информацията чрез промяна на честотата.

Изборът на модулация оказва влияние върху начина, по който сигналът може да бъде наблюдаван и обработван. За изследователя обаче е необходимо да се разграничат характеристиките на физическия сигнал от структурата на протокола. Модулацията определя начина на предаване на информацията по радиоканала, но не представлява сама по себе си механизъм за сигурност.

2.2. Software Defined Radio (SDR)

Софтуерно-дефинираното радио представлява подход, при който част от традиционните хардуерни функции на радиосистемата се реализират чрез софтуер. Вместо всяка функция да бъде фиксирана в специализиран хардуер, цифровият сигнал може да бъде подаван към програмна среда, в която да бъде филтриран, демодулиран, визуализиран и анализиран.

В приемен режим SDR устройството приема радиосигнала и го преобразува в цифрови семпли. При системи, работещи с I/Q представяне, всеки комплексен семпъл се състои от две компоненти – In-phase (I) и Quadrature (Q). Тези компоненти позволяват да се запази информация за амплитудата и фазата на сигнала и са основа за последваща цифрова обработка. GNU Radio например използва комплексни I/Q семпли при работа с SDR системи.

Едно от основните предимства на SDR е гъвкавостта. При промяна на изследваната комуникационна система често не е необходимо да бъде сменен хардуерът. Вместо това могат да бъдат променени честотата, честотната лента, филтрите, усилването или алгоритмите за обработка.

Тази гъвкавост прави SDR особено подходящ за изследване на неизвестни или частично известни радиосистеми. Например при първоначален анализ може да бъде извършено спектрално наблюдение, след което да се определят приблизителната честота и широчината на сигнала. След това могат да бъдат изследвани времевата структура и модулацията.

Най-големият недостатък при тези устройства е тяхната цена. Те са много по-скъпи от стандартни RF трансивъри. Друг недостатък на този подход е по-голямата сложност. Изследователят трябва да разбира както основните принципи на радиокомуникациите, така и начина на работа на използвания софтуер. При някои задачи е необходимо създаването на сигнални схеми и настройване на множество параметри.

2.3. Специализирани радиочестотни устройства

За разлика от широколентовите SDR системи, специализираните радиочестотни устройства са разработени за конкретен набор от честоти и комуникационни характеристики. Те обикновено предоставят по-високо ниво на абстракция и позволяват директно задаване на параметри като честота, модулация и скорост на данните.

YARD Stick One е пример за подобна специализирана платформа. Той е проектиран за цифрови безжични системи под 1 GHz и използва CC1111 радиотрансивър. Официалните работни диапазони са 300-348 MHz, 391-464 MHz и 782-928 MHz. Поддържат се ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK, а максималната посочена скорост на данните е до 500 Kbps.

Тази специализация има както предимства, така и ограничения. От една страна, устройството е удобно за работа с нискоскоростни цифрови радиосистеми и не изисква изграждане на сложна SDR обработка за всяка основна операция. От друга страна, достъпът

до суровата форма на радиосигнала е по-ограничен в сравнение с широколентов SDR. Това също прави пресъздаването на прихванатия сигнал значително по-трудно.

Следователно изборът между SDR платформа и специализиран радиочестотен инструмент зависи от конкретната задача. При спектрален анализ и изследване на неизвестен сигнал SDR предоставя по-голяма гъвкавост. При работа с вече известен тип цифрова комуникация специализираният инструмент може да осигури по-бърз и удобен начин за експериментиране.

3 HackRF One

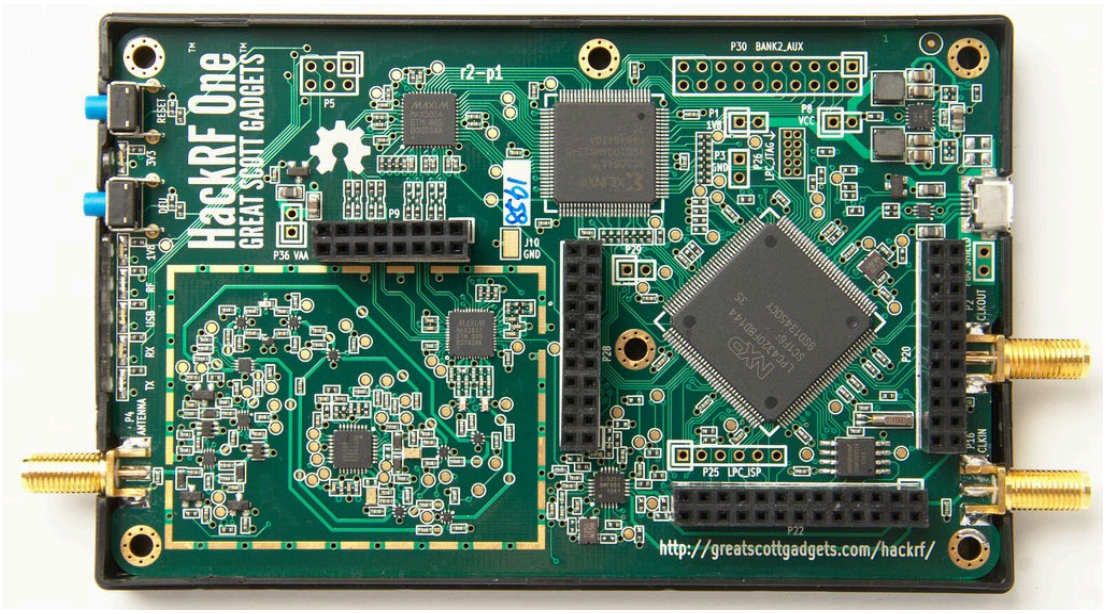
3.1. Архитектура и основни характеристики

HackRF One е широколентова SDR платформа, предназначена за приемане и предаване на радиосигнали. Устройството работи в диапазона от 1 MHz до 6 GHz, използва half-duplex режим и поддържа до 20 милиона семпъла в секунда. I/Q семплите са с 8-битова резолюция.

Хардуерът разполага със SMA конектор за антена, USB интерфейс за връзка с компютър и възможност за софтуерно управление на усилването и базовия филтър. Устройството може да бъде използвано както за приемане, така и за предаване, което го прави подходящо за контролирани експерименти с радиосигнали.

Широкият честотен диапазон е едно от основните предимства на HackRF One. Едно устройство може да бъде използвано за изследване на комуникации в различни части на радиочестотния спектър, без необходимост от специализиран хардуер за всяка отделна честота.

При изследване на субгигахерцови комуникации това позволява например наблюдение на системи около 433 MHz, 868 MHz и други подходящи честоти. Важно е при предаване да се спазват приложимите регулаторни ограничения, тъй като HackRF One е тестово оборудване и самото устройство не гарантира съответствие с изискванията за радиопредаване.



Фиг. 1. HackRF One

3.2. Работа с I/Q данни

Основна характеристика, която отличава HackRF One от YARD Stick One, е възможността за работа със сурови I/Q семпли.

При цифровото представяне на комплексния сигнал I компонентата представя една от ортогоналните компоненти на сигнала, а Q компонентата – другата. Комбинирани заедно, те предоставят информация, която може да бъде използвана за анализ на честотата, амплитудата, фазата и времевата структура на радиосигнала.

В GNU Radio комплексните семпли могат да бъдат обработвани от различни блокове. Те могат да бъдат визуализирани, филтрирани, записвани във файл или подавани към последваща обработка. GNU Radio описва комплексните семпли като последователности от I и Q компоненти, които могат да бъдат съхранявани и обработвани като цифрови данни. Това позволява един и същ сигнал да бъде анализиран многократно, без повторно задействане на оригиналния предавател.

Тази възможност е особено полезна при анализ на неизвестни сигнали. Изследователят може първоначално да наблюдава спектъра, след това да разгледа времевата форма и накрая да извърши по-подробен анализ на модулацията.

Тази особеност има голямо значение при експерименталното изследване, защото позволява отделяне на етапите на прихващане и анализ. Един сигнал може първо да бъде записан, след което да бъде разглеждан при различни настройки на филтри, визуализация и обработка.

3.3. Използван софтуер

За работа с HackRF One в лабораторната постановка е използван софтуерът GNU Radio. GNU Radio е програмна среда за цифрова обработка на сигнали, която позволява изграждането на сигнални вериги чрез свързване на отделни функционални блокове.

При експериментите входният сигнал от HackRF One се подава към блок за визуализация на спектъра. По този начин може да се наблюдава активността около зададената централна честота.

За изследването около 433 MHz е използвана честота на семплиране от 1 MHz. При задаване на централна честота около 433 MHz натискането на бутон на дистанционното управление води до появата на отчетлив сигнален пакет.

Към сигналната схема може да бъде добавен и File Sink, чрез който приеманите данни се записват за последващ анализ. За възпроизвеждане на записан сигнал се използва обратна структура, при която записаните данни се подават към предавателната част на HackRF One.

Този подход демонстрира основната концепция на SDR: хардуерът осигурява достъп до радиосигнала, а конкретната обработка се определя чрез софтуера.

4 YARD Stick One

4.1. Архитектура и основни характеристики

YARD Stick One (фиг. 2) е специализиран инструмент за работа с цифрови безжични сигнали под 1 GHz. За разлика от HackRF One, той не е широколентова SDR платформа, а използва специализиран радиотрансивър CC1111. Официалните работни честоти включват диапазоните 300-348 MHz, 391-464 MHz и 782-928 MHz.

Устройството работи в half-duplex режим и може както да приема, така и да предава цифрови радиосигнали. Поддържаните модулации включват ASK, OOK, GFSK, 2-FSK, 4-FSK и MSK.



Фиг. 2. YARD Stick One

YARD Stick One разполага със SMA конектор за антена и се свързва към компютър чрез USB. За разлика от HackRF One, устройството е тясно свързано с възможностите на CC1111. Това означава, че работата му е по-ограничена по отношение на честоти и обработка, но същевременно предоставя директен достъп до функции, предназначени за цифрови радиосистеми под 1 GHz.

4.2. CC1111 и начин на работа

CC1111 е интегриран радиотрансивър с микроконтролер, предназначен за нископотребителски субгигахерцови безжични приложения. Именно използването на този радиочип определя основните възможности на YARD Stick One.

При работа с устройството не се получава същият тип сурови I/Q данни, характерен за SDR платформите. Вместо това радиотрансивърът трябва да бъде конфигуриран с параметри като честота, модулация и други настройки на радиокомуникацията. Вместо да се получи самият радиосигнал, това устройство записва самата информация, която се изпраща през радиосредата (стига параметрите да са зададени правилно).

Този модел на работа е по-близък до начина, по който функционира готов радиомодул. Изследователят задава параметрите на радиочипа и получава цифров резултат от неговата обработка.

Това е съществено различие спрямо HackRF One. При HackRF анализът може да започне от самия физически сигнал и постепенно да премине към по-високо ниво. При YARD Stick One значителна част от обработката вече се извършва от радиочипа.

Тази архитектура е подходяща, когато типът на радиокомуникацията е приблизително известен. Например ако се предполага, че дадено устройство използва OOK около 433 MHz, YARD Stick One може да бъде конфигуриран директно за тази честота и модулация.

4.3. Използван софтуер

YARD Stick One се използва с RfCat – софтуерна среда, която позволява управление на CC1111 чрез Python интерфейс. Официалната информация за устройството посочва, че YARD Stick One се доставя с RfCat firmware, а самият RfCat позволява управление на радиотрансивъра от интерактивна Python среда или от собствена програма.

В лабораторната постановка RfCat се използва за настройване на работната честота и режима на модулация. След стартиране на интерактивната среда могат да бъдат зададени параметри за приемане и предаване.

При експериментите са изследвани различни комбинации от честота и модулация, включително 169 MHz ASK/OOK, 315 MHz ASK/OOK, 868 MHz ASK/OOK, 915 MHz ASK/OOK, 433 MHz GFSK и 433 MHz ASK/OOK.

Особено внимание е отделено на 433 MHz ASK/OOK, тъй като именно в този режим е наблюдавана комуникацията на изследваното дистанционно управление.

При използване на RfCat могат да бъдат изпълнявани функции за слушане и предаване. Това предоставя сравнително лесен начин за експериментиране с поддържаните радиорежими, без да е необходимо изграждането на сложна GNU Radio схема.

5 Експериментално изследване с HackRF One и YARD Stick One

5.1. Прихващане и анализ на сигнали

Първоначалното експериментално изследване е проведено с HackRF One. Целта е да бъде установена работната честота на изследваното дистанционно управление и да бъде анализирана структурата на предаваните сигнали.

При наблюдение около 433 MHz се установява, че при натискане на бутон се появява кратък сигнален пакет. При липса на натискане на бутон се наблюдава основно фонов радиошум.

Използването на GNU Radio позволява сигналът да бъде разгледан в честотната област. При няколко последователни предавания се наблюдава повторяемост на сигналната структура.

След това са направени записи на I/Q данните. Тези записи могат да бъдат използвани за последващ анализ и сравнение.

Предимството на HackRF в този етап е, че изследването може да започне без предварително точно познаване на структурата на комуникацията. Спектърът предоставя информация за това къде се намира сигналът и кога се активира.

След определяне на приблизителната честота е проведено изследване с YARD Stick One. Чрез RfCat са зададени 433 MHz и OOK като предполагаем режим на модулация. При приемане се наблюдава активност при натискане на бутон.

При YARD Stick One обаче получената информация е на по-високо ниво и не предоставя същия достъп до суровия физически сигнал, който е наличен при HackRF.

При допълнителни тестове са разгледани и други честоти и режими. Това показва практическата възможност на YARD Stick One да бъде използван за бързо тестване на различни конфигурации, но също така демонстрира зависимостта му от възможностите на CC1111.

5.2. Определяне на параметрите на комуникацията

При използване на HackRF One работната честота се определя чрез спектрално наблюдение. При изследваната система се установява честота около 433.92 MHz.

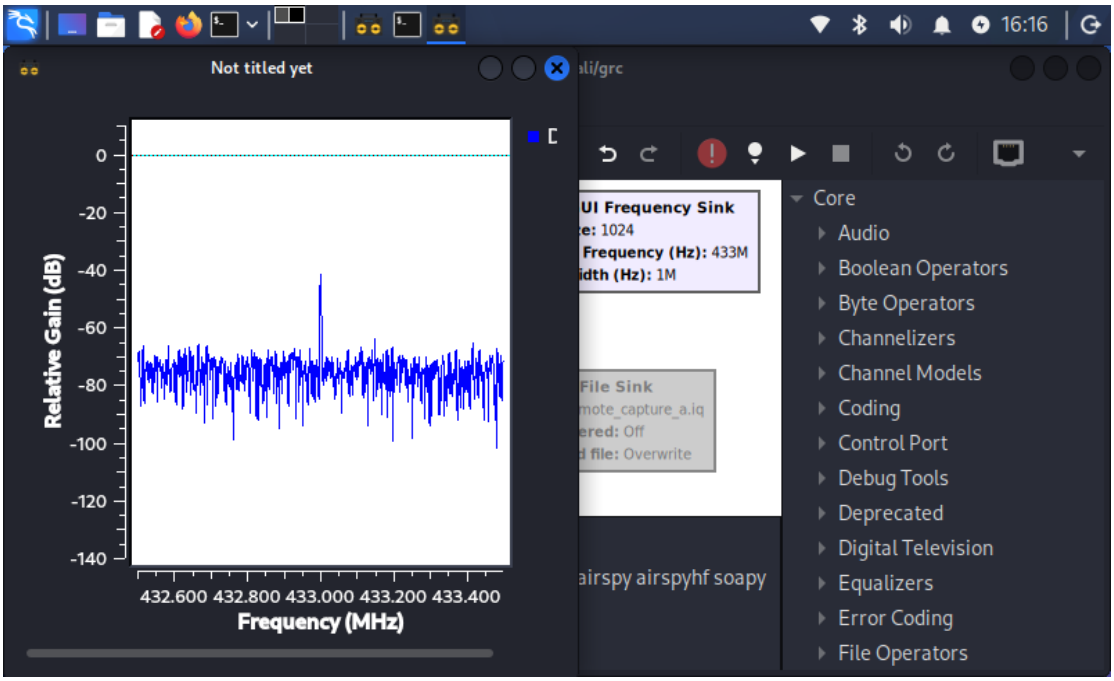
Чрез времевия анализ на сигнала се установява, че предаването се състои от кратки импулси и се активира при подаване на команда. Структурата е съвместима с OOK, при която наличието и отсъствието на носещ сигнал се използват за представяне на цифрова информация.

HackRF предоставя възможност за допълнителен анализ на честотната широчина и времевата структура. Това е особено полезно при неизвестни комуникации, защото параметрите могат да бъдат изведени експериментално.

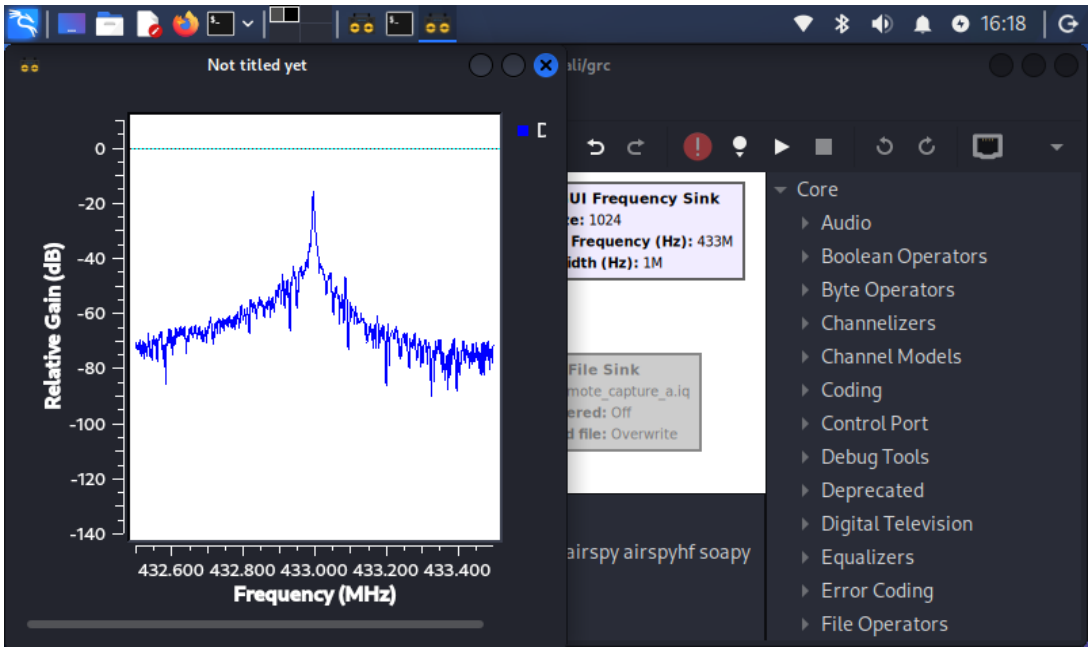
При YARD Stick One определянето на параметрите се извършва по различен начин. Вместо директно наблюдение на спектъра се задават предполагаемите параметри и се проверява дали устройството може да приема активността.

При експериментите е установено, че при 433 MHz ASK/OOK се получава структурирана информация, съответстваща на наблюдаваната комуникация. При други настройки, например 433 MHz GFSK, резултатът е различен.

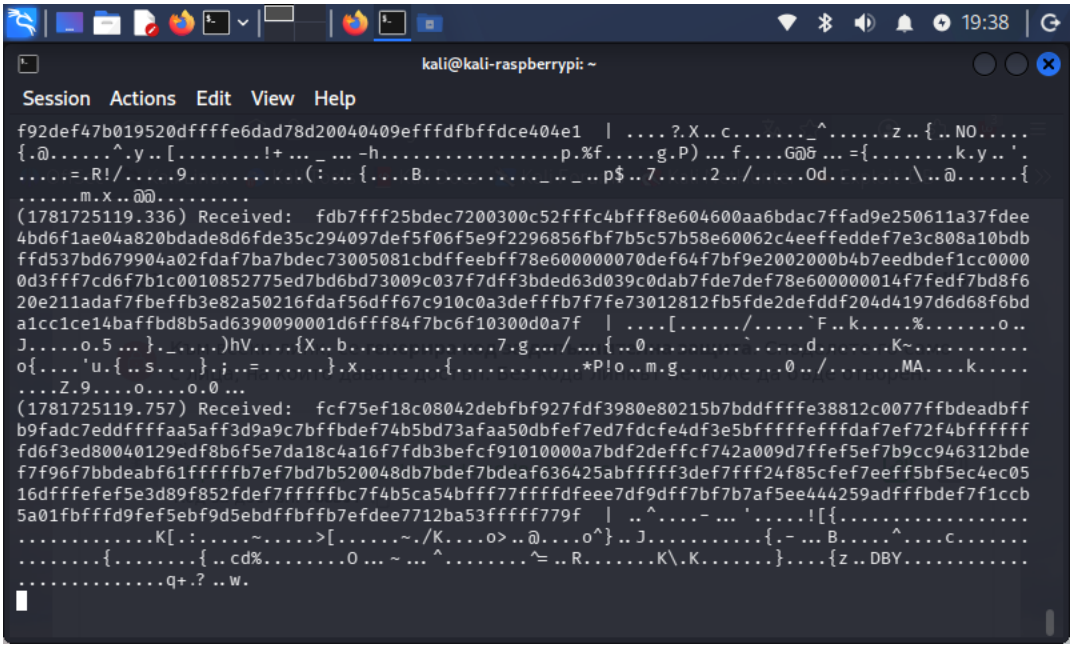
Това показва различния подход на двете устройства. HackRF е по-подходящ за откриване и характеризиране на неизвестен сигнал, докато YARD Stick One е по-подходящ за работа с вече определени параметри.



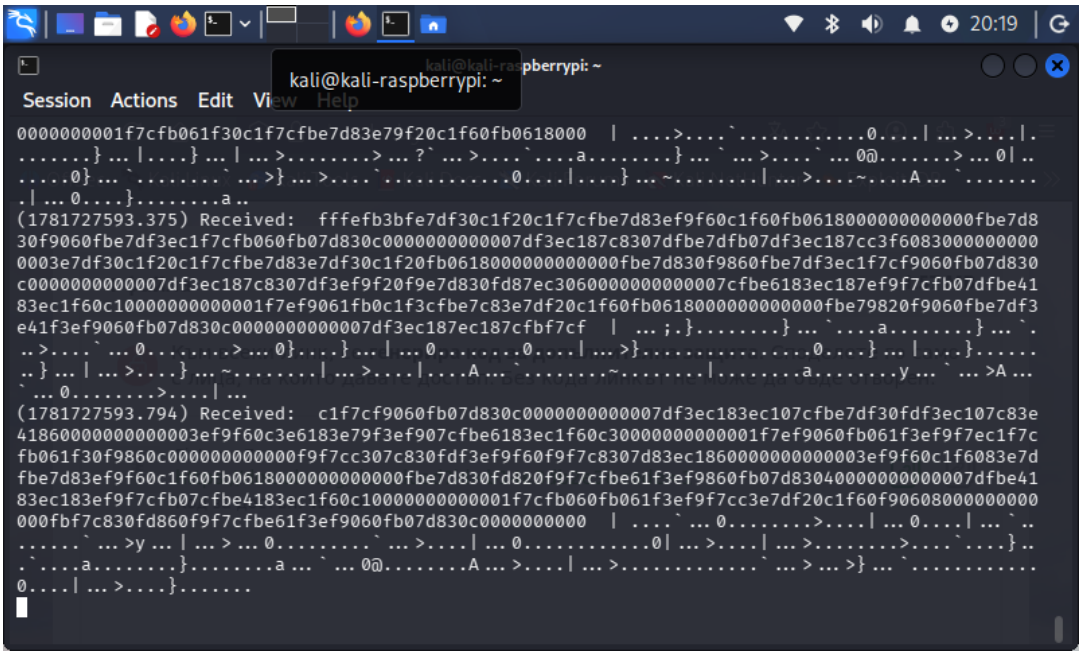
Фиг. 3. HackRF One / GNU Radio / нормално състояние



Фиг. 4. HackRF One / GNU Radio / получаване на сигнал



Фиг. 5. YARD Stick One / RfCat / нормално състояние



Фиг. 6. YARD Stick One / RfCat / получаване на сигнал

5.3. Възпроизвеждане на прихванати сигнали

След записването на сигналите с HackRF One е проведен експеримент за тяхното повторно предаване.

Записаните I/Q данни са използвани като вход на предавателната схема в GNU Radio. При повторното предаване успешно е извършена replay атака на устройство, използващо фиксиран код.

Този резултат показва, че HackRF може да бъде използван за възпроизвеждане на конкретен прихванат физически сигнал. Причината за това е възможността да се съхрани самата форма на радиосигнала, а не само извлечена от него цифрова последователност.

При YARD Stick One е направен различен подход. Чрез RfCat получените данни са представени като цифрова последователност, която може да бъде подадена към функция за предаване.

При директно предаване на прихванатата последователност устройството не реагира по същия начин, както при HackRF.

Това е един от най-съществените практически резултати от сравнението. При YARD Stick One получената информация не представлява непременно пълно описание на физическата форма на оригиналния RF сигнал. При OOK комуникациите времевата структура на импулсите е важна и простото представяне на резултата като поредица от байтове не винаги е достатъчно за точно възпроизвеждане на оригиналното предаване.

HackRF, от друга страна, запазва физическата форма на сигнала чрез I/Q семплите. Това позволява записаният сигнал да бъде възпроизведен с много по-малка промяна спрямо оригинала.

5.4. Създаване на смущения

Допълнителният експеримент има за цел да покаже възможностите на двете устройства при създаване и наблюдение на радиосмущения в контролирана лабораторна среда.

При HackRF One е използван шумов източник в GNU Radio, който се подава към предавателната част. При настройване около работната честота се създава допълнителна радиочестотна активност.

При нормални условия на експеримента изследваната система демонстрира надеждна работа на разстояние приблизително 25-30 m. При наличие на контролирано смущение около работната честота надеждният обхват е намален до приблизително 8-10 m.

Този експеримент демонстрира предимството на HackRF при задачи, при които е необходимо генериране на специфичен радиосигнал. Чрез GNU Radio може да бъде определен типът на сигнала и начинът, по който той се подава към предавателната част.

YARD Stick One също разполага с предавателни възможности, но възможностите му за генериране на произволен широколентов шум са по-ограничени. Устройството има значително по-малка мощност от HackRF One. Предназначено е преди всичко за работа с поддържаните цифрови модулации на CC1111, а не за свободно формиране на произволна I/Q форма.

При проведените експерименти не е установено сравнимо ефективно въздействие върху обхвата чрез YARD Stick One. Това показва практическата разлика между широколентовия SDR подход и специализирания радиотрансивър.

Експериментите със смущения са проведени в контролирана лабораторна среда. При реално предаване на радиосигнали трябва да бъдат спазвани приложимите национални и европейски изисквания за използване на радиочестотния спектър.

6 Сравнителен анализ на резултатите

6.1. Предимства и ограничения на HackRF One

Основното предимство на HackRF One е неговата гъвкавост. Широкият честотен диапазон от 1 MHz до 6 GHz позволява използването на едно устройство за изследване на множество различни радиосистеми. Поддържането на I/Q семпли позволява достъп до физическата форма на сигнала и последващата му цифрова обработка.

Това прави HackRF особено подходящ за първоначално изследване на неизвестни радиосигнали. Чрез спектрално наблюдение може да бъде установена честотата, след което да бъдат анализирани широчината, времевата структура и модулацията.

Друго важно предимство е възможността за запис на I/Q данни. Записаният сигнал може да бъде анализиран многократно и при подходяща конфигурация да бъде възпроизведен.

HackRF е подходящ и за експерименти, при които е необходимо генериране на различни видове сигнали. GNU Radio позволява изграждането на сложни сигнални вериги и промяна на параметрите без промяна на основния хардуер.

Основното ограничение, изключвайки високата цена, е сложността на работа. За пълното използване на възможностите на HackRF е необходимо разбиране на SDR концепциите, I/Q представянето, семплирането, филтрацията и цифровата обработка на сигнали. Създаването на подходяща GNU Radio схема също може да изисква повече време.

Допълнително ограничение е 8-битовата резолюция на I/Q семплите, която поставя ограничения върху динамичния диапазон в сравнение с някои по-нови и по-висок клас SDR системи. Това не пречи на използването му за голям брой практически експерименти, но е характеристика, която трябва да бъде отчетена при по-прецизни измервания.

6.2. Предимства и ограничения на YARD Stick One

Основното предимство на YARD Stick One е специализацията му. Устройството е разработено именно за цифрови безжични системи под 1 GHz и поддържа типични за тази област модулации.

Работата с RfCat позволява бързо задаване на честота и режим на модулация и извършване на приемане или предаване. Това намалява необходимостта от изграждане на сложна цифрова сигнална обработка.

YARD Stick One е особено удобен при експерименти, при които вече са известни основните параметри на комуникацията. Например при известна честота 433.92 MHz и предполагаема OOK модулация устройството може да бъде конфигурирано директно за съответната задача.

Друг плюс е компактността на устройството и сравнително простият начин на работа. RfCat предоставя програмируем интерфейс, чрез който радиотрансивърът може да бъде използван от Python. Официалният проект описва YARD Stick One именно като платформа, предназначена за RfCat.

Основното ограничение е по-ниското ниво на достъп до сигнала. За разлика от HackRF One, YARD Stick One не предоставя общ SDR интерфейс със сурови I/Q семпли. Анализът е ограничен от възможностите на CC1111 и поддържаните от него режими.

Това се проявява особено ясно при възпроизвеждането на прихванати OOK сигнали. Прихванатата цифрова информация не винаги съдържа достатъчно информация за точно възстановяване на оригиналната времева форма на RF сигнала. В резултат директното предаване на получените данни може да не доведе до успешна replay атака.

6.3. Сравнение на приложимостта им при различни задачи

Резултатите от експериментите показват, че HackRF One и YARD Stick One не трябва да се разглеждат като напълно взаимозаменяеми устройства.

При първоначално изследване на неизвестна комуникация HackRF One предоставя значително по-широки възможности. Чрез спектралното наблюдение може да бъде открита активността, а I/Q записът позволява сигналът да бъде запазен в оригиналната му цифрова форма.

При анализ на вече идентифицирана цифрова комуникация YARD Stick One може да бъде по-удобен. Ако са известни честотата, модулацията и приблизителните параметри, те могат директно да бъдат зададени чрез RfCat.

При подробен физически анализ HackRF има предимство поради достъпа до I/Q данни. Това позволява изследване на характеристиките на сигнала, които могат да бъдат загубени при по-високо ниво на обработка.

При стандартни операции по приемане и предаване на поддържани цифрови модулации YARD Stick One предлага по-специализиран подход. Неговият хардуер и софтуер са оптимизирани за работа с възможностите на CC1111, което опростява някои задачи.

При генериране на произволни или нестандартни радиосигнали HackRF отново има по-голяма гъвкавост. GNU Radio позволява сигналът да бъде изграден програмно от различни блокове и да бъде променян според експерименталната задача.

При създаване на смущения също се наблюдава разлика. HackRF позволява генериране на шумови и други сигнали чрез SDR обработка, докато YARD Stick One е ограничен от функционалността на радиотрансивъра CC1111.

От гледна точка на обучението двете устройства също предоставят различни възможности. Използването на съвременни технологични платформи в практически ориентирано обучение подпомага развитието на технически компетентности, умения за експериментиране и способност за решаване на практически задачи [8]. HackRF позволява по-добро изучаване на физическия слой на радиокомуникацията – спектър, семплиране, I/Q представяне и модулация. YARD Stick One от своя страна предоставя по-пряк начин за експериментиране с цифрови субгигахерцови комуникации и програмиране на радиотрансивър.

Следователно сравнението показва не толкова, че едното устройство е универсално по-добро от другото, а че те са предназначени за различни нива на анализ. HackRF One е по-гъвкав инструмент за изследване на самия радиосигнал, докато YARD Stick One е по-специализиран инструмент за работа с определен клас цифрови радиосистеми.

7 Заключение

В настоящия доклад е извършен сравнителен анализ на HackRF One и YARD Stick One при изследване на субгигахерцови безжични комуникации. Разгледани са техните архитектурни особености, начинът им на работа, използваната софтуерна среда и приложимостта им при различни експериментални задачи.

HackRF One представлява широколентова SDR платформа с работен диапазон от 1 MHz до 6 GHz, възможност за приемане и предаване и достъп до I/Q семпли. Тези характеристики го правят подходящ за спектрален анализ, изследване на неизвестни сигнали, запис на радиосигнали и тяхното последващо цифрово обработване.

YARD Stick One е специализиран субгигахерцов радиочестотен инструмент, базиран на CC1111. Той поддържа редица цифрови модулации и е предназначен за работа с радиосистеми под 1 GHz. Управлението му чрез RfCat позволява сравнително лесно задаване на основните параметри и извършване на приемане и предаване.

Проведеното експериментално изследване показва съществена разлика между двата подхода. При HackRF One сигналът може да бъде наблюдаван на физическо ниво, записан като I/Q данни и впоследствие обработван или възпроизвеждан. Това предоставя голяма свобода при анализа на неизвестни комуникации.

При YARD Stick One работата се извършва на по-високо ниво. Радиотрансивърът обработва сигнала според зададените настройки, а RfCat предоставя интерфейс за управление на тази функционалност. Този подход е по-ограничен, но е удобен при работа с вече известни честоти и поддържани модулации.

Експериментите с изследваната 433 MHz система показват, че HackRF One е по-подходящ за първоначално характеризиране на сигнала и за запазване на неговата физическа структура. YARD Stick One може успешно да се използва за приемане на цифрова комуникация, когато нейните основни параметри са предварително определени, но директното възпроизвеждане на прихванатите данни не винаги е достатъчно за точно възстановяване на оригиналния RF сигнал.

При експериментите със смущения също се установява разлика. HackRF One позволява програмно генериране на шумови сигнали чрез GNU Radio и предоставя по-голяма свобода при формирането на предаването. YARD Stick One е ограничен от възможностите на CC1111 и не е предназначен за същото ниво на произволна I/Q обработка.

В крайна сметка двата инструмента допълват по-скоро, отколкото заменят един друг. HackRF One е подходящ за широк спектър от задачи, свързани с наблюдение, запис и анализ на физическия радиосигнал, докато YARD Stick One предоставя специализиран и по-опростен подход към цифрови субгигахерцови комуникации.

Използването на двата инструмента в една лабораторна постановка позволява радиокомуникацията да бъде разглеждана от различни нива – от физическата форма на сигнала до параметрите на цифровия радиотрансивър. Това прави комбинирания подход подходящ за експериментално изследване на различни безжични системи и за оценка на техните технически характеристики и сигурност.

ЛИТЕРАТУРА:

[1] OFCOM IR 2030 - Licence Exempt Short Range Devices. https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir-2030.pdf

[2] Qinuo Electronics Co.,Ltd. "What is the difference between rolling code and fixed code remote?" https://www.qinuo.net/news/64.html

[3] Great Scott Gadgets – HackRF One. https://greatscottgadgets.com/hackrf/one/

[4] Great Scott Gadgets – YARD Stick One. https://greatscottgadgets.com/yardstickone/

[5] Youngblood, G. "A Software-Defined Radio for the Masses, Part 1". https://www.arrl.org/files/file/Technology/tis/info/pdf/020708qex013.pdfhttps://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.2117-0-201809-I!!PDF-E.pdf

[6] International Telecommunication Union. "Data format definition for exchanging stored I/Q data for the purpose of spectrum monitoring". https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.2117-0-201809-I!!PDF-E.pdf

[7] atlas0fd00m/rfcat: RfCat - swiss-army knife of ISM band radio. https://github.com/atlas0fd00m/rfcat

[8] Tasinov, T. Y. (2023). A Step Up – From 3D to 6D Printing. Possible and Future Applications of New Materials and Technologies in the Technology Education of Students. In: Innovation Models for Implementing Qualifications and Forming Competencies in the Educational System. Shumen: Konstantin Preslavsky University Press, pp. 286–293. ISBN 978-619-201-732-3.

A CONCEPTUAL MODEL OF AUTONOMY LEVELS IN AUTOMATED INFORMATION SYSTEMS FOR EDUCATIONAL PROCESS MANAGEMENT*

DESISLAVA N. IVANOVA

ABSTRACT: *The digital transformation of education is changing the role of automated information systems (AIS) by expanding their participation in the management of educational processes. Advances in artificial intelligence and data analysis and prediction methods create opportunities for a transition from automation to higher levels of management autonomy. This paper proposes the conceptual EAAL (Educational AIS Autonomy Levels) model, which distinguishes six levels of autonomy, ranging from informational to adaptively autonomous. The model defines the roles of the system and the human at each level and introduces the principle of minimum necessary autonomy. EAAL is intended as a theoretical framework for the assessment, design, and comparative analysis of automated information systems in education.*

KEYWORDS: *automated information systems, educational institution management, autonomy, automated decision-making, artificial intelligence, learning analytics, human-in-the-loop, human oversight*

DOI: https://doi.org/10.46687/MT26DNI

КОНЦЕПТУАЛЕН МОДЕЛ НА НИВАТА НА АВТОНОМНОСТ НА АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ОБРАЗОВАТЕЛНИ ПРОЦЕСИ

ДЕСИСЛАВА Н. ИВАНОВА

АБСТРАКТ: *Дигиталната трансформация на образованието променя ролята на автоматизираните информационни системи (АИС), като разширява участието им в управлението на образователните процеси. Развитието на изкуствения интелект и методите за анализ и прогнозиране на данни създава предпоставки за преминаване от автоматизация към по-висока степен на управленска автономност. В статията се предлага концептуален модел EAAL (Educational AIS Autonomy Levels), който разграничава шест нива на автономност – от информационно до адаптивно автономно. Моделът определя ролята на системата и човека при всяко ниво и въвежда принцип на минимално необходимата автономност. EAAL е предназначен като теоретична основа за оценяване, проектиране и сравнителен анализ на АИС в образователната сфера.*

1 Въведение

Дигитализацията на образователните организации вече не се ограничава до внедряването на отделни електронни системи. Приложението на технологиите в обучението представлява самостоятелно направление на педагогическите изследвания [21]. Съвременната цифрова образователна екосистема обхваща технологичните средства, тяхната взаимна свързаност, управлението на данните и ролята на човешкия фактор. В педагогически аспект значение имат и дигиталните компетентности на учителя [22].

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Ефективната цифрова трансформация предполага интегрирането на тези компоненти в обща институционална среда [6, 13].

Развитието на изкуствения интелект разширява възможностите на информационните системи в образованието. Първоначалните приложения са насочени основно към подпомагане на обучението и оценяването [17], докато по-новите изследвания обхващат и административни и управленски дейности. Наред с това остават открити въпроси, свързани с етиката и организационното внедряване на тези технологии [4, 5]. Отделно направление е оценяването на Web-базираното учебно съдържание, за което е предложена рамка в [18].

Особено значение придобива използването на образователни данни за анализ и подпомагане на управленските решения. Подобни подходи позволяват прогнозиране на академичен риск и подкрепа на обучаваните, но доказателствата за устойчивата им ефективност в различни институционални условия все още са ограничени [9]. Изкуственият интелект навлиза и в управлението на висшето образование, където наред с ефективността все по-голямо значение имат прозрачността, отчетността и разпределението на управленските роли [10].

Това развитие поставя въпроса за степента, в която информационната система участва самостоятелно в управленския процес. Понятията автоматизация и автономност не са равнозначни, тъй като автоматизацията може да обхваща различни управленски функции и да се реализира на различни нива [14]. Поради това е необходимо ясно разграничаване на ролята на системата и мястото на човека при вземането и изпълнението на решения. Програмните модели за автоматизиране на когнитивни процеси са анализирани в [20].

Целта на настоящата статия е да се разработи концептуален модел за определяне на нивата на автономност на информационните системи за управление на образователни процеси, който свързва степента на технологична самостоятелност с ролята на човека в управленския процес.

2 От автоматизация към автономно управление

При моделирането на информационни системи в управленски контекст е важно да се разграничат управленските функции, механизмите за контрол и отговорностите на участниците в процеса [1].

Автоматизацията се свързва с изпълнение на предварително определени операции и правила без непосредствено човешко участие във всяка стъпка. Автономността надхвърля това ниво, тъй като системата участва в избора на действие въз основа на наличната информация и зададените цели. При автоматично изпращане на уведомление след достигане на определен брой отсъствия системата изпълнява предварително зададено правило. Анализът на академичен риск и изборът на подходяща интервенция вече предполагат участие в управленското решение.

Нарастването на автоматизацията не премахва необходимостта от човешко участие, а променя неговия характер. В образователна среда човешкият фактор включва и професионално-педагогическите компетентности на учителя [23]. При автоматизиране на рутинните операции човекът запазва отговорността за сложните и нетипичните ситуации, което е в основата на т.нар. „иронии на автоматизацията“ [3]. Този проблем е съществен и за образователните АИС, при които институцията продължава да носи отговорност за последствията от автоматизираните действия.

Риск представлява и прекомерното доверие в автоматизираните препоръки, което може да ограничи критичната им проверка [6, 7]. Поради това формалното човешко одобрение не е достатъчно условие за действителен контрол върху решенията на системата.

В настоящото изследване управленската автономност се определя като степента на самостоятелно участие на информационната система в управлението на даден процес. Тя обхваща способността на системата да обработва информация, да участва в избора на решение и да предприема действия в предварително определени граници. Степента на човешки контрол зависи от характера и значимостта на управлявания процес. Следователно автономността се разглежда като степенувана и контекстно ограничена характеристика.

3 Концептуален модел EAAL (Educational AIS Autonomy Levels)

EAAL представя степента на участие на АИС в управленския процес. Нивото се определя от самостоятелността на системата и от ролята на човека при управлението. Използваната технология сама по себе си не е основание за определяне на по-висока степен на автономност. Концептуалният модел EAAL е представен на фиг. 1.:



Фиг. 1. Концептуален модел EAAL

➢ EAAL 0 - информационно ниво

При EAAL 0 системата има информационна функция. Тя обработва и представя данни, без самостоятелно да определя значението им за конкретно управленско решение. Към това ниво могат да бъдат отнесени различни информационни и отчетни системи в образователните организации.

Човекът интерпретира предоставената информация и определя последващото действие. В педагогически контекст взаимодействието между педагога и учениците е съществен елемент на образователния процес [24]. Системата улеснява достъпа до данни, но не променя субекта на управленското решение. Внедряването на цифрови технологии не води непременно до съществена промяна на съществуващите процеси [13].

➢ EAAL 1 - автоматизирано ниво

При EAAL 1 системата изпълнява предварително определени правила. Управленската логика е зададена от човек и не предполага самостоятелен избор от страна на системата.

Пример за това е автоматичното изпращане на уведомление при настъпване на предварително определено условие. Подобна автоматизация намалява необходимостта от ръчно изпълнение, но не прехвърля управленската преценка към системата. Поради това автоматизацията на изпълнението трябва да се разграничава от самостоятелния избор на решение [14].

➢ EAAL 2 - аналитично ниво

При EAAL 2 системата интерпретира наличните данни и установява зависимости в тях. Аналитичните възможности могат да се използват за оценяване на академичен риск и прогнозиране на резултати [9].

Получената информация подпомага управленското решение, но системата не определя самостоятелно последващото действие. Отговорността за оценката и решението остава при човека. Следователно аналитичната способност не е равнозначна на автономност при вземането на решения. Доказателствата за устойчивия ефект от подобни подходи в различни институционални условия все още са ограничени [9].

➢ EAAL 3 - препоръчващо ниво

При EAAL 3 системата използва резултатите от анализа, за да предложи конкретно управленско действие. Окончателното решение остава при човека, който може да промени или отхвърли направената препоръка [8].

При това ниво възниква риск човешкото одобрение да придобие формален характер. Прекомерното доверие в автоматизирани препоръки може да ограничи тяхната критична проверка [6]. Поради това ефективният контрол изисква човекът да разполага с достатъчно основания за оценка на предложението и с реална възможност за намеса.

➢ EAAL 4 - условно автономно ниво

При EAAL 4 системата може самостоятелно да взема определени решения и да ги изпълнява в предварително установени граници. Човекът преминава от непосредствено одобрение към наблюдение, като запазва правото си на намеса [8].

В образователната среда подобна автономност е приложима предимно към процеси с ограничен риск. При решения със съществено влияние върху обучаваните е необходим по-висок интензитет на човешки и нормативен контрол [12, 16]. Третирането на автоматизираното вземане на решения според GDPR е разгледано в [19].

➢ EAAL 5 - адаптивно автономно ниво

При EAAL 5 представлява най-високата степен на автономност в предложения модел. Системата самостоятелно управлява действията си и проследява резултата от тях. Получената обратна връзка се използва за приспособяване на последващото поведение в предварително определени граници.

Ролята на човека се измества към стратегически контрол. Той определя границите на самостоятелност и оценява резултатите от функционирането на системата. Запазва се възможността за ограничаване или прекратяване на автономното ѝ действие [8].

EAAL 5 не представлява задължителна крайна цел. Подходящото ниво зависи от особеностите на конкретния образователен процес и от възможните последствия от

решенията. Поради това по-високата автономност не означава непременно по-добро управление.

4 Критерии за определяне на EAAL ниво

Предлагат се пет критерия, които могат да се използват за профилиране на конкретна система. Тези критерии следват логиката, че автономността трябва да бъде оценявана по различни функции, а не чрез един общ етикет [13].

C1 - автономност на анализа. Критерият оценява до каква степен системата самостоятелно интерпретира данни, открива аномалии, изчислява риск или прогнозира бъдещи състояния. При ниските нива анализът е човешки или предварително зададен. При по-високите системата извършва сложна интерпретация.

C2 - автономност на избора. Оценява дали системата само представя информация, предлага алтернативи или самостоятелно избира между възможни управленски действия. Именно този критерий е един от най-важните за разграничаване на аналитична система от система с реална управленска автономност.

C3 - автономност на изпълнението. Оценява дали предприемането на действие изисква предварително човешко одобрение. Възможно е система да има висока аналитична автономност, но ниска автономност на изпълнението - например да изчислява риск и да предлага интервенция, която задължително се одобрява от човек.

C4 - адаптивност. Оценява дали системата може да използва обратна връзка от последствията на предишни действия и да променя бъдещото си поведение. Този критерий отличава статичната автоматизация от адаптивния управленски механизъм.

C5 - форма на човешкия контрол. Оценява къде се намира човекът в цикъла: като пряк решаващ субект, одобряващ, наблюдаващ, управляващ изключения или стратегически контролиращ системата. Европейската рамка за надежден изкуствен интелект (Trustworthy AI) показва, че формите на надзор могат да варират и следва да бъдат съобразени с риска и приложението [8].

Съвместното прилагане на петте критерия позволява всяко ниво на EAAL да бъде описано според степента на самостоятелност на системата и ролята на човека в управленския процес. В табл. 1 е представено обобщено съпоставяне на нивата на модела по отделните критерии.

С повишаването на нивото на EAAL се променя не само степента на самостоятелност на системата, но и характерът на човешкото участие. Непосредственият контрол постепенно намалява, докато ролята на човека се измества към стратегическо наблюдение и определяне на границите на автономност. Тази концептуална зависимост е представена на фиг. 2.

Представената зависимост има концептуален характер и илюстрира общата логика на модела EAAL. Стойностите във фигурата не представляват резултати от емпирично измерване.

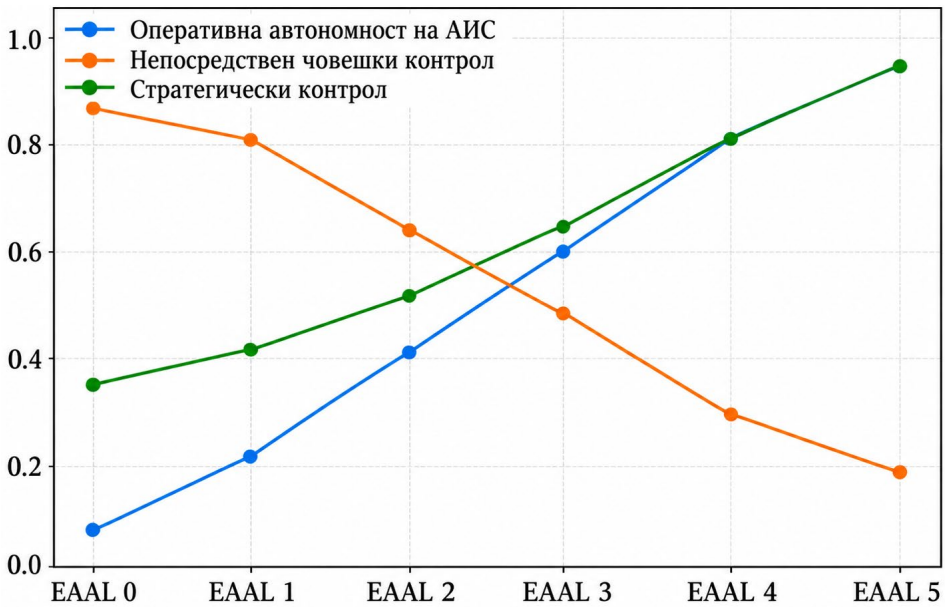
5 Взаимодействие между автономността на АИС и човешкия контрол

Един от основните акценти на модела EAAL е, че нарастването на автономността на информационната система не означава премахване на човешкия контрол. Високата степен на автоматизация може да бъде съчетана с ефективен надзор при запазена възможност за човешка намеса [15]. Следователно по-високата автономност променя ролята на човека, без да го изключва от управленския процес. Развитието на информационните системи и

навлизането на нововъзникващи дигитални технологии предполагат и съответстващо развитие на компетентностите на техните потребители, тъй като ефективното им използване изисква не само технически умения, а разбиране на техните възможности, ограничения и рискове, критично оценяване и безопасно приложение [3].

Таблица 1. Критерии за разграничаване на нивата на автономност в модела EAAL

Ниво	C1 Анализ	C2 Избор	C3 Изпълнение	C4 Адаптация	C5 Човешки контрол
EAAL 0	от човека	от човека	от човека	няма	пълен
EAAL 1	по зададени правила	по зададени правила	автоматично	няма	определя правилата
EAAL 2	от системата	от човека	от човека	няма	оценява и решава
EAAL 3	от системата	препоръка от системата	след одобрение	ограничена	одобрява или отхвърля
EAAL 4	от системата	от системата в определени граници	от системата в определени граници	контролирана	наблюдава и се намесва
EAAL 5	от системата	от системата	от системата	висока	стратегически контрол



Фиг. 2. Концептуална трансформация на човешкия контрол при повишаване на автономността

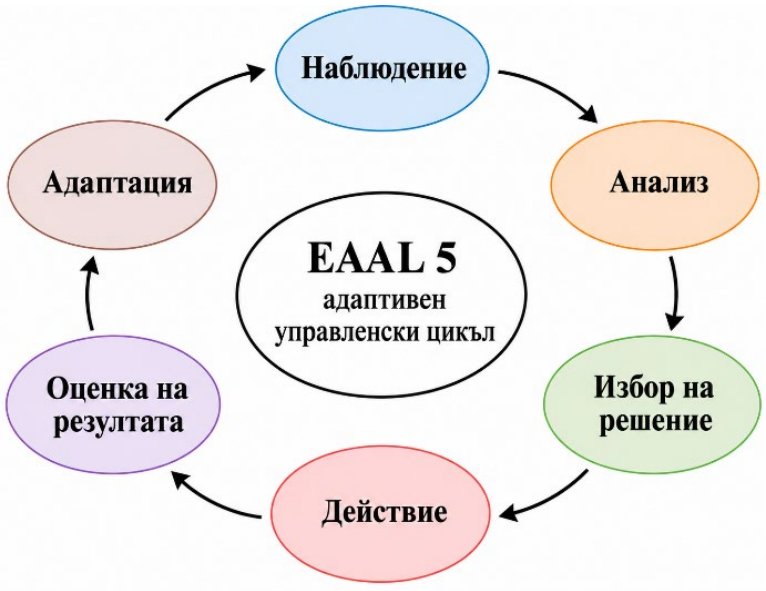
На тази основа се въвежда понятието „споделена управленска автономност“, което описва разпределението на управленските функции между човека и информационната система. При по-ниските нива на EAAL решенията се определят основно от човека. С повишаването на автономността системата придобива по-активна роля, а човешкото

участие постепенно се измества от непосредствено вземане на решения към контрол върху нейното функциониране.

Тази промяна засяга и характера на човешката отговорност. При по-високите нива човекът определя допустимите граници на автономност и оценява резултатите от работата на системата. Европейските насоки за надежден изкуствен интелект свързват човешкия надзор с характера и риска на конкретното приложение [8]. ЮНЕСКО също определя човешкия надзор като съществен елемент при отговорното използване на изкуствения интелект [16].

Формалното човешко участие обаче не е равнозначно на действителен контрол. Прекомерното доверие в автоматизираните препоръки може да ограничи тяхната критична оценка [6, 7]. Поради това при определяне на автономността е важно да се отчита реалната възможност за човешка намеса, а не само формално предвиденото участие.

При EAAL 5 автономността включва и способността на системата да използва резултатите от своите действия за последващо адаптиране на поведението. По този начин се формира затворен управленски цикъл, в който обратната връзка влияе върху следващите действия на системата. Тази зависимост е представена на фиг. 3.:



Фиг. 3. Затворен адаптивен управленски цикъл при EAAL 5

6 Принцип на минимално необходимата автономност

В модела EAAL най-високата технически постижима автономност не се приема непременно за най-подходяща. Образователните процеси се различават по значимост и възможни последствия. Поради това автоматизирането на рутинна административна дейност не може да се разглежда по същия начин като решение, което засяга академичния статус на обучавания.

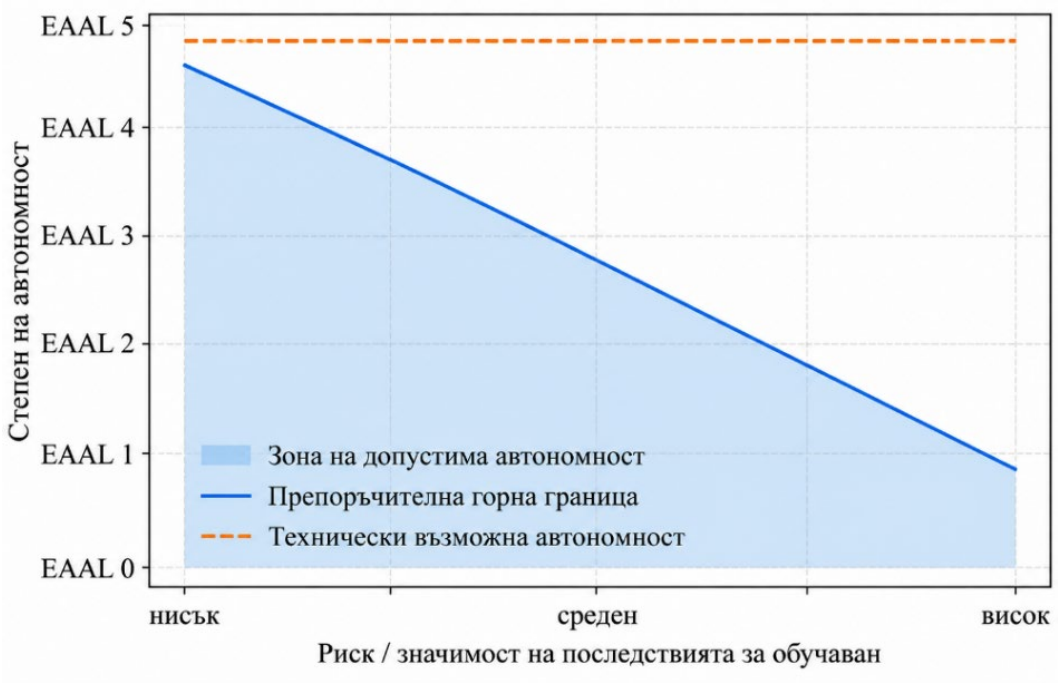
На тази основа се предлага принципът на минимално необходимата автономност. Според него на информационната система следва да се предоставя най-ниската степен на самостоятелност, достатъчна за ефективното управление на конкретния процес при приемлив риск. Изборът на ниво трябва да се определя от особеностите на процеса, а не само от техническите възможности на системата.

Нивата на EAAL не представляват задължителни етапи на развитие, а различни форми на участие на системата в управлението. В една образователна институция могат да се прилагат различни нива според характера на процеса. По-висока автономност може да бъде подходяща за рутинни дейности, докато решенията със съществено въздействие върху обучаваните изискват по-голямо човешко участие. При определянето на подходящата степен на автономност следва да се отчитат и рисковете, свързани с обработването и защитата на информацията, особено при използването на генеративен изкуствен интелект [11].

Степента на автономност следва да бъде съобразена с риска и последствията от решенията [8, 12, 16]. При по-значимо въздействие необходимостта от ефективен човешки контрол нараства. Затова подходящото ниво на EAAL трябва да осигурява баланс между ползите от автоматизацията и възможността за човешка намеса.

Значение има и рискът от прекомерно доверие в автоматизираните решения [6, 7]. Формалното участие на човек не осигурява действителен контрол, когато решението на системата трудно може да бъде проверено. В такива случаи ограничаването на автономността може да осигури по-ефективно човешко участие.

Връзката между риска на управленското решение и подходящата степен на автономност е представена концептуално на фиг. 4.:



Фиг. 4. Концептуална илюстрация на принципа на минимално необходимата автономност

7 Концептуален сценарий: управление на риск от отпадане на обучаван

Практическото приложение на модела може да се представи чрез сценарий за управление на риск от отпадане. Анализът на образователни данни позволява ранно установяване на обучавани с повишен риск от затруднения или прекъсване на обучението [9]. Сценарият показва как при различните нива на EAAL се променят ролите на системата и човека.

При EAAL 0 системата предоставя информация за учебното представяне на обучавания. Преценката за наличието на риск и необходимостта от действие се извършва изцяло от човек.

При EAAL 1 системата изпълнява предварително определени правила. Например при достигане на определен брой отсъствия тя автоматично изпраща уведомление. Условията и съответното действие са предварително определени от човек.

При EAAL 2 системата анализира данните и оценява вероятността от отпадане. Полученият резултат подпомага преценката, но изборът на последващо действие остава при човека.

При EAAL 3 системата може да предложи конкретна мярка за подкрепа на обучавания. Предложението има препоръчителен характер, а човекът запазва правото на окончателно решение.

При EAAL 4 системата може самостоятелно да предприема разрешени действия с ограничен риск. По-значимите случаи се насочват към човек, който определя последващото действие.

При EAAL 5 системата проследява резултатите от предприетите действия и използва обратната връзка за адаптиране на бъдещото си поведение. Човешката роля се измества към определяне на границите на автономност и контрол върху резултатите.

Сценарият показва, че една и съща управленска задача може да бъде реализирана при различна степен на автономност. Подходящото ниво зависи от начина на функциониране на системата и риска на конкретния процес. Така EAAL позволява да се определи степента, в която изпълнението на дадена управленска функция може да бъде предоставено на информационната система.

8 Приложимост и значение на модела EAAL

Моделът EAAL развива съществуващите постановки за автоматизация в контекста на управлението на образователни процеси. Степента на автономност се определя не само от техническите възможности на системата, а и от ролята ѝ в управленското решение. Отчита се и отговорността, която остава при човека.

Приложението на изкуствения интелект във висшето образование постепенно обхваща и институционалното управление. Наред с възможностите за повишаване на ефективността остават въпроси относно прозрачността и разпределението на отговорността [10]. EAAL позволява да се определи каква част от дадена управленска функция е предоставена на информационната система.

Съществено за модела е разграничението между способността за анализ и правото на самостоятелно действие. Система със сложни аналитични възможности може да остане на EAAL 2, когато управленското решение се взема от човек. Система с по-ограничен анализ може да достигне EAAL 4, когато самостоятелно изпълнява разрешени действия. Следователно технологичната сложност не определя пряко нивото на автономност.

Това разграничение е важно и при внедряването на АИС в образователните институции. Водещо значение има каква част от управленската дейност е целесъобразно да бъде предоставена на системата и каква отговорност трябва да остане при човека. Така технологичното решение се съобразява с особеностите на конкретния образователен процес.

EAAL може да се използва като концептуална основа за оценяване на автономността на АИС. Моделът позволява да се определи ролята на системата и да се прецени необходимата степен на човешки контрол. Практическата му стойност се състои във

възможността подходящото ниво на автономност да бъде определяно спрямо конкретния образователен процес.

9 Заключение

Развитието на информационните системи в образованието показва преход от информационно подпомагане към по-активно участие в управленските процеси. Прилагането на изкуствен интелект разширява възможностите на АИС, но поставя и въпроси за допустимата автономност и ролята на човешкия контрол [8–10, 12, 13, 16].

Предложеният модел EAAL представя автономността чрез шест нива, които отразяват различна степен на самостоятелност на системата. Основна постановка на модела е, че по-високата автономност не означава непременно по-подходящо управление. Принципът на минимално необходимата автономност свързва избора на ниво с характера на образователния процес и риска от съответното управленско решение.

Бъдещото развитие на EAAL е свързано с практическото му изследване и разработването на измерими показатели за отделните нива. Това би позволило моделът да се прилага при оценяване на съществуващи АИС и при проектиране на нови системи за управление на образователни процеси.

ЛИТЕРАТУРА:

[1] Симеонова, И., Методиева, Ц. „Модел за управление на административна сигурност в община“. JSAR, бр. 26, 2024, стр. 93–105. ISSN 1314-6289 (print), ISSN 2815-4622 (online).

[2] Тасинов, Т. Ю., Тончева, С. К. „Изпреварваща технологична подготовка и дигитални здравни компетентности в обучението на медицински сестри и акушерки“. Сборник доклади – XIX Национален форум на специалистите по здравни грижи и постерна секция за студенти „Справедлив достъп до качествени здравни грижи“, 24–25 октомври 2025 г., Шумен, 2025, стр. 97–103.

[3] Bainbridge, L. Ironies of automation. Automatica, Vol. 19, No. 6, 1983, pp. 775–779. DOI: 10.1016/0005-1098(83)90046-8.

[4] Chiu, T. K. F., Xia, Q., Zhou, X., Chai, C. S., Cheng, M. Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence in education. Computers and Education: Artificial Intelligence, Vol. 4, 2023, Article 100118. DOI: 10.1016/j.caeai.2022.100118.

[5] Crompton, H., Burke, D. Artificial intelligence in higher education: the state of the field. International Journal of Educational Technology in Higher Education, Vol. 20, 2023, Article 22. DOI: 10.1186/s41239-023-00392-8.

[6] Dimanova, D., Kuzmanov, Z. Development of an Integrated Security and Communication System. International Scientific Refereed Online Journal, No. 63, November 2019, ISSN 2367-5721, pp. 83–91.

[7] Goddard, K., Roudsari, A., Wyatt, J. C. Automation bias: a systematic review of frequency, effect mediators, and mitigators. Journal of the American Medical Informatics Association, Vol. 19, No. 1, 2012, pp. 121–127. DOI: 10.1136/amiajnl-2011-000089.

[8] High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. European Commission, 2019.

[9] Ifenthaler, D., Yau, J. Y.-K. Utilising learning analytics to support study success in higher education: a systematic review. Educational Technology Research and Development, Vol. 68, 2020, pp. 1961–1990. DOI: 10.1007/s11423-020-09788-z.

[10] Jiang, X., Abdullah, Z. AI-enabled governance in higher education: a systematic review of applications, outcomes, and emerging implications. Frontiers in Education, Vol. 11, 2026, Article 1856440. DOI: 10.3389/feduc.2026.1856440.

[11] Kuzmanova, E., Dimanova, D. Technical privacy risks in Generative AI (GenAI) – Lessons from OWASP and Real-World Failures. 10th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE

2025), 5–7 November 2025, Starozagorski Bani, Bulgaria. IEEE, 2025. ISBN 979-8-3315-1299-6. DOI: 10.1109/EEAE65901.2025.11273791. (Scopus).

[12] Miao, F., Holmes, W., Huang, R., Zhang, H. AI and Education: Guidance for Policy-makers. UNESCO, 2021.

[13] OECD. OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. OECD Publishing, 2023. DOI: 10.1787/c74f03de-en.

[14] Parasuraman, R., Sheridan, T. B., Wickens, C. D. A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics – Part A, Vol. 30, No. 3, 2000, pp. 286–297. DOI: 10.1109/3468.844354.

[15] Shneiderman, B. Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy. International Journal of Human-Computer Interaction, Vol. 36, No. 6, 2020, pp. 495–504. DOI: 10.1080/10447318.2020.1741118.

[16] UNESCO. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2022.

[17] Zawacki-Richter, O., Marín, V. I., Bond, M., Gouverneur, F. Systematic review of research on artificial intelligence applications in higher education – where are the educators? International Journal of Educational Technology in Higher Education, Vol. 16, 2019, Article 39. DOI: 10.1186/s41239-019-0171-0.

[18] Atanasov, V., Ivanova, A. A framework for evaluation of web-based learning content. International Journal on Information Technologies and Security, Vol. 14, No. 4, 2022, pp. 13–24, ISSN 1313-8251.

[19] Simeonova I. How GDPR treats automated decision-making. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2025, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 164–175. https://doi.org/10.46687/jsar.v29i1.461

[20] Атанасов В., Иванова А. Анализ на програмните модели за автоматизиране на когнитивни процеси. Стратегии на образователната и научната политика, Vol. 32, № 5s, 2024, ISSN 1310-0270. https://doi.org/10.53656/str2024-5s-24-ana

[21] Бурова И. Същност на технологиите и приложението им в обучението. Е-списание „Образование и развитие“, бр. 17, 2026, с. 78–83. ISSN 2603-3577.

[22] Бурова И. Разкриване съдържанието на понятията педагогически и дигитални компетентности като основа за изграждане на визуален йерархичен модел на професионално-педагогическите компетентности на учителя. Е-списание „Образование и развитие“, бр. 12, 2023, с. 72–80.

[23] Бурова И. Компетенции и компетентности в обучението – професионална и педагогическа компетентност на учителя. Годишник на Шуменския университет „Епископ Константин Преславски“, Педагогически факултет, т. XXIX D, 2025, с. 424–430.

[24] Бурова И. Взаимодействието между педагога и учениците. Е-списание „Образование и развитие“, бр. 17, 2026, с. 84–91. ISSN 2603-3577.

ANALYSIS OF THE OPERATING PRINCIPLES AND EFFICIENCY OF THE TCP AND UDP TRANSPORT PROTOCOLS*

DESISLAV M. HRISTOV

ABSTRACT: *This paper examines the main characteristics, operating principles, and applications of the transport protocols TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) within the TCP/IP architecture. Their key features are presented in terms of connection establishment, data transmission reliability, flow control, error handling, and communication speed. A comparative analysis highlights the advantages, limitations, and application areas of both protocols. Examples of their use in various network services and applications are discussed, where either reliable information delivery or minimal transmission latency is a primary requirement. The aim of the paper is to clarify the functional differences between TCP and UDP and to demonstrate the importance of selecting the appropriate transport protocol according to the specific requirements of a network application.*

KEYWORDS: *TCP, UDP, TCP/IP, transport layer, network protocols, reliability, data transmission*

DOI: https://doi.org/10.46687/MT26DMH

АНАЛИЗ НА ПРИНЦИПИТЕ НА РАБОТА И ЕФЕКТИВНОСТТА НА ТРАНСПОРТНИТЕ ПРОТОКОЛИ TCP И UDP

ДЕСИСЛАВ М. ХРИСТОВ

АБСТРАКТ: *Настоящият доклад разглежда основните характеристики, принципите на функциониране и приложението на транспортните протоколи TCP (Transmission Control Protocol) и UDP (User Datagram Protocol) в архитектурата TCP/IP. Представени са техните основни особености по отношение на установяването на връзка, надеждността на предаването на данни, контрола на потока, управлението на грешките и скоростта на комуникация. Направен е сравнителен анализ на двата протокола, като са откроени техните предимства, ограничения и области на приложение. Разгледани са примери за използването им в различни мрежови услуги и приложения, при които водещо значение имат или надеждното доставяне на информацията, или минималното закъснение при предаването ѝ. Целта на доклада е да изясни функционалните различия между TCP и UDP и да покаже значението на правилния избор на транспортен протокол според конкретните изисквания на мрежовото приложение.*

1 Въведение

Съвременните компютърни мрежи представляват основа за обмен на информация между различни устройства, системи и приложения. За осъществяването на този обмен се използват мрежови протоколи, които определят правилата и механизмите за предаване и получаване на данни. В архитектурата TCP/IP особено важна роля има транспортният слой, който осигурява комуникацията между приложенията, работещи на крайни устройства. Сред основните протоколи на транспортния слой са TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). Въпреки че изпълняват сходна основна функция, двата протокола се различават съществено по начина, по който организират предаването на

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

информация. TCP осигурява надеждно предаване на данни чрез механизми за установяване на връзка, потвърждение на получаването и повторно изпращане на загубена информация. UDP, от своя страна, предлага по-опростен механизъм за предаване без предварително установяване на връзка, което го прави подходящ за приложения, при които бързината и ниското закъснение са от съществено значение. Изборът между TCP и UDP зависи от специфичните изисквания на съответното приложение, включително необходимата надеждност, допустимото закъснение и ефективността на комуникацията. Поради това познаването на особеностите на двата протокола е важно за разбирането на принципите на функциониране на компютърните мрежи и на различните услуги, предоставяни чрез интернет. На фиг.1 е показано позиционирането на протоколите TCP и UDP



Фиг. 1. Позициониране на протоколите TCP и UDP в архитектурата на TCP/IP

2 Ролята на TCP и UDP в архитектурния модел TCP/IP

Съвременните интернет комуникации се осъществяват чрез съвкупност от протоколи, които определят начина, по който устройствата обменят информация. За да бъде комуникацията организирана и предвидима, различните функции се разделят между отделни слоеве. Всеки слой изпълнява определени задачи и използва услугите на слоя под него. Този подход улеснява разработването на мрежови приложения, съвместимостта между различни системи и откриването на проблеми при предаването на данни. В архитектурата TCP/IP транспортният слой осигурява комуникация между приложения, работещи на различни крайни устройства. Докато интернет слоят отговаря за логическото адресиране и пренасянето на IP пакетите между мрежите, транспортният слой позволява данните да бъдат насочени към конкретното приложение на крайното устройство. За тази цел се използват транспортни портове. Основните транспортни протоколи, разглеждани в настоящия доклад, са Transmission Control Protocol (TCP) и User Datagram Protocol (UDP). Те изпълняват сходна обща задача – пренасяне на данни между приложения – но използват различни механизми. TCP предоставя надежден, ориентиран към връзка пренос, докато UDP изпраща дейтаграми без предварително установяване на транспортна връзка и без гаранция за доставката им. Изборът между двата протокола зависи от изискванията на конкретното приложение [2, 3].

Моделът TCP/IP описва архитектурата на протоколите, използвани в интернет. Обикновено той се представя чрез четири слоя: приложен, транспортен, интернет и слой за мрежов достъп. Всеки от тях има определена роля в процеса на комуникация. Приложният слой обединява протоколите и механизмите, чрез които мрежовите приложения предоставят услуги на потребителите или обменят информация помежду си. Примери за

такива протоколи са HTTP и HTTPS за уеб комуникация, SMTP за изпращане на електронна поща и DNS за преобразуване на домейн имена в IP адреси. Транспортният слой осигурява обмена на данни между приложенията на крайните системи. TCP и UDP работят на това ниво. Чрез номерата на портовете се определя към кое приложение или мрежова услуга трябва да бъдат предадени получените данни. Портът не заменя IP адреса: IP адресът идентифицира мрежовия интерфейс или крайното устройство в рамките на IP комуникацията, а портът подпомага разграничаването на комуникационните крайни точки на транспортно ниво. Интернет слоят използва IP за логическо адресиране и маршрутизация на пакетите през свързани мрежи. IP предоставя механизъм за доставка на пакети до определен адрес, но сам по себе си не гарантира, че пакетът ще достигне до получателя, нито че пакетите ще пристигнат в първоначалния ред. Допълнителните механизми, необходими на приложенията, се осигуряват от транспортния протокол или от други протоколи и механизми в системата. Слоят за мрежов достъп обхваща механизмите за предаване на данни през конкретната мрежова технология. Той включва взаимодействието с локалната мрежова среда и физическото предаване на сигналите. Примери за технологии, използвани на това ниво, са Ethernet и Wi-Fi. При изпращане на данни приложението предава информацията към транспортния слой. TCP или UDP добавя необходимата транспортна информация, след което данните се предават към IP за адресиране и маршрутизация. На приемащото устройство процесът се извършва в обратна посока: IP обработва получените пакети, транспортният слой използва информацията за протокола и портовете, а данните се предават към съответното приложение.

Мрежовите портове са логически номера, които се използват от транспортните протоколи TCP и UDP за разграничаване на различни комуникационни крайни точки. Номерът на порт сам по себе си не представлява физически конектор и не означава непременно, че съответната услуга е достъпна. Той е част от информацията, чрез която операционната система обработва входящия и изходящия трафик. TCP и UDP използват отделни пространства от номера на портове. Поради това един и същ номер може да се използва независимо от двата протокола, когато това е предвидено от съответните приложения и конфигурации. В практиката често се срещат стандартно асоциирани портове: например TCP порт 22 се свързва със SSH, TCP порт 25 – със SMTP, а DNS обичайно използва порт 53 както с UDP, така и с TCP според вида на заявката и условията на комуникацията. При разглеждането на мрежовите услуги е важно да се прави разлика между номер на порт и самия протокол или услуга. Портът обозначава транспортна крайна точка, TCP и UDP определят начина на транспортен обмен, а приложният протокол задава правилата за интерпретиране на съобщенията. Например при SSH TCP осигурява транспортната връзка, докато SSH определя механизмите за защитен отдалечен достъп. Съчетанието от IP адрес, транспортен протокол и номер на порт позволява да се разграничават комуникационните крайни точки. Това е важно за работата на сървъри, които могат едновременно да обслужват множество клиенти и различни услуги.

Макар TCP и UDP да работят на един и същ слой от архитектурата TCP/IP, техните характеристики са различни и определят подходящите области на приложение. TCP включва механизми за потвърждение, повторно предаване на загубени данни, подреждане на байтовия поток и управление на потока и претоварването. Тези механизми са полезни, когато приложението изисква надеждно и подредено предаване на информация. UDP има по-малко функции на транспортно ниво. Той позволява изпращането на отделни дейтаграми без предварително установяване на връзка и не осигурява вградено повторно предаване или гарантирано подреждане. Това може да бъде полезно за приложения, които

предпочитат ограничено протоколно натоварване и могат да обработват загуба на данни или да реализират собствени механизми за надеждност. Не е правилно обаче UDP автоматично да се определя като по-бърз във всички ситуации. Реалната производителност и закъснение зависят от мрежовите условия, размера и честотата на съобщенията, поведението на приложението и използваните допълнителни механизми. По същия начин TCP не е подходящ за всяка задача само защото предоставя надеждност. Изборът трябва да се основава на изискванията към доставката, последователността, времето за реакция и обработката на загубени данни. Разглеждането на архитектурата TCP/IP, ролята на портовете и функциите на транспортния слой създава необходимата основа за по-подробното представяне на TCP и UDP в следващите глави. На фиг. 2 е показана ролята на транспортния слой [2, 3].



Фиг. 2. Роля на транспортния слой при осъществяване на комуникация

3 Принцип на работа и характеристики на протокол TCP

Transmission Control Protocol (TCP) е транспортен протокол от архитектурата TCP/IP, предназначен да осигурява надежден и подреден обмен на данни между приложения, работещи на различни крайни устройства. За разлика от UDP, TCP е ориентиран към връзка: преди предаването на данни страните установяват логическа транспортна връзка, а по време на обмена протоколът използва механизми за потвърждение, контрол на последователността и повторно предаване при определени случаи на загуба. TCP предоставя на приложението поток от байтове. Това означава, че протоколът гарантира подреденото предаване на данните в рамките на връзката, но не запазва непременно границите на отделните съобщения, които приложението подава към транспортния слой. Ако приложението изпрати информация на няколко отделни части, получаващата страна трябва да използва правилата на съответния приложен протокол, за да определи къде завършва едно съобщение и започва следващото. Една от основните характеристики на TCP е надеждността. Протоколът използва номерация на предаваните данни и потвърждения от приемащата страна, за да проследява кои части от потока са получени. Ако данни се загубят по пътя, TCP може да ги предаде повторно. Освен това протоколът поддържа механизми за контрол на потока и контрол на претоварването. Те помагат да се ограничи изпращането на данни според възможностите на получателя и състоянието на мрежата. Тези механизми правят TCP подходящ за приложения, при които е важно информацията да бъде доставена правилно и в определен ред. Примери са зареждането на уеб страници чрез HTTP/1.1 и HTTP/2, прехвърлянето на файлове и отдалеченото администриране чрез SSH. При тези приложения загубата или разместването на данни без коригиращи механизми може да доведе до неправилно обработване на информацията. Преди да започне обичайният обмен на данни, TCP страните установяват връзка чрез процедура, известна като Three-Way

Handshake, или тристранно ръкостискане. Чрез нея клиентът и сървърът обменят контролни сегменти, синхронизират началните номера на последователност и потвърждават, че комуникацията може да бъде започната. Процедурата включва три основни стъпки:

SYN – клиентът изпраща сегмент със зададен SYN флаг. В него се посочва началният номер на последователност, който клиентът ще използва за изпращаните данни.

SYN-ACK – ако сървърът приема заявката, той отговаря със сегмент, който съдържа SYN и ACK флагове. Сървърът посочва собствен начален номер на последователност и потвърждава получения SYN от клиента.

ACK – клиентът изпраща потвърждение на началния номер на последователност на сървъра. След успешното приключване на обмена връзката е установена и може да започне предаването на данни.

Тази процедура позволява на двете страни да синхронизират необходимата информация за проследяване на потока. Тя не е самото предаване на приложните данни, а предварителен етап за установяване на транспортната връзка. След него TCP продължава да използва номера на последователност и потвърждения, за да управлява обмена. Тристранното ръкостискане има значение и за обработването на закъснели или дублирани сегменти от предишни опити за комуникация. Чрез обмена на актуални параметри страните потвърждават, че могат да участват в новата връзка. Процедурата обаче не осигурява криптиране или удостоверяване на самоличността сама по себе си. Ако приложението изисква защита на съдържанието и проверка на идентичността на отсрещната страна, са необходими допълнителни механизми, например TLS или защитен приложен протокол. При предаване през IP мрежа отделни пакети могат да бъдат загубени, дублирани или доставени в различен ред от този, в който са изпратени. IP не предоставя на транспортния слой гаранция за надеждна доставка. TCP компенсира част от тези ограничения, като номерира байтовете в потока и използва потвърждения от получателя. Потвърждението показва до коя част от потока получателят е приел данните последователно. Ако изпращащата страна не получи очаквано потвърждение в рамките на определен период или установи загуба по друг поддържан механизъм, тя може да изпрати отново липсващите данни. Приемащата страна използва номерата на последователност, за да възстанови правилния ред на потока и да не предава повторно получени данни като ново съдържание на приложението. TCP осигурява поток от байтове, а не гарантира, че всяко изпращане от приложението ще съответства на един отделен сегмент или едно отделно получаване. Операционната система може да разделя или обединява данните при предаването им. Поради тази причина приложните протоколи трябва самостоятелно да определят структурата и границите на своите съобщения. Надеждността на TCP не означава, че предаването винаги е незабавно. При загуба на сегменти повторното им изпращане може да забави получаването на следващите данни от потока. Това е важен компромис: TCP се стреми да предостави пълен и подреден поток, дори когато мрежата не доставя всички сегменти без проблеми. TCP използва два различни, но взаимно допълващи се механизма: контрол на потока и контрол на претоварването. Те имат различни цели и не трябва да се разглеждат като едно и също действие. Контролът на потока предпазва получателя от прекомерно количество входящи данни. Получаващата страна съобщава какъв обем данни може да приеме в дадения момент, като по този начин изпращачът може да съобрази количеството данни, което изпраща без допълнително потвърждение. Това е важно, когато устройствата имат различни изчислителни възможности или когато приложението на получателя обработва данните по-бавно от тяхното постъпване. Контролът на претоварването има за цел да ограничава натоварването върху самата мрежа. Ако се

изпраща повече трафик, отколкото междинните мрежови устройства и връзки могат да обработят, може да се увеличат закъсненията и загубите на пакети. TCP използва алгоритми за контрол на претоварването, чрез които адаптира скоростта на изпращане спрямо наблюдаваното състояние на мрежата. Разликата е съществена: контролът на потока се съобразява с капацитета на приемащата страна, докато контролът на претоварването се стреми да предотврати прекомерно натоварване на мрежовия път. Заедно тези механизми подпомагат стабилната работа на TCP при различни мрежови условия. На фиг. 3 са показани основните етапи на функциониране на TCP.[2]

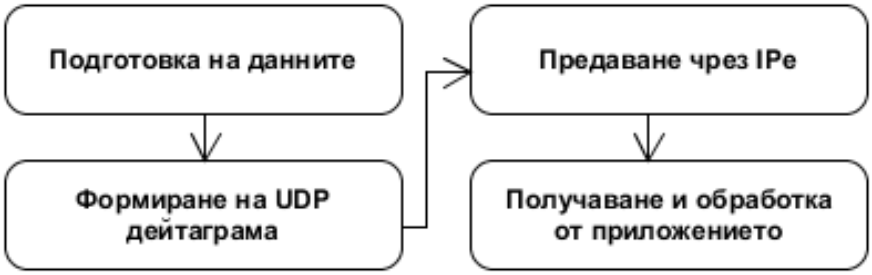


Фиг. 3. Основни етапи на функциониране на TCP

4 Принцип на работа и характеристики протокол UDP

User Datagram Protocol (UDP) е транспортен протокол от архитектурата TCP/IP, който позволява обмен на данни между приложения без предварително установяване на транспортна връзка. За разлика от TCP, UDP не поддържа механизми за потвърждение на получаването, повторно предаване на изгубени дейтаграми или гарантирано подреждане на данните. Изпращачът оформя съобщението в UDP дейтаграма и я предава към IP слоя за пренасяне през мрежата. UDP има сравнително проста структура и малко протоколно натоварване. Заглавната част на UDP е с фиксирана дължина от 8 байта и съдържа четири полета: порт на източника, порт на получателя, дължина и контролна сума. Портовете позволяват на приемащата система да предаде дейтаграмата към съответното приложение. Полето за дължина указва размера на UDP заглавната част и данните, а контролната сума служи за откриване на определени грешки при предаването. Конкретното използване и задължителност на контролната сума зависят от версията на IP и съответните правила на протокола. Тъй като UDP не установява връзка, преди изпращането не е необходим обмен на контролни сегменти, подобен на TCP Three-Way Handshake. Това намалява броя на съобщенията, нужни за започване на комуникацията. Протоколът обаче не може самостоятелно да гарантира, че дейтаграмата ще достигне до получателя, че ще пристигне само веднъж или че ще бъде обработена в реда на изпращане. Ако приложението се нуждае от подобни свойства, то трябва да ги реализира на приложно ниво или да използва друг протокол, който ги предоставя. При UDP данните се изпращат като отделни дейтаграми. Всяка дейтаграма е самостоятелна единица, за разлика от TCP, който представя данните към приложението като поток от байтове. Границите на UDP съобщенията се запазват на транспортно ниво, но това не означава, че мрежата гарантира тяхната доставка. UDP разчита на IP за пренасянето на дейтаграмите между мрежите. По време на комуникацията

дейтаграми могат да бъдат загубени, дублирани или получени в различен ред. UDP не изпраща автоматично повторно изгубените съобщения и не подрежда получените дейтаграми. Освен това протоколът не включва собствен механизъм за контрол на потока или контрол на претоварването. Това не означава, че приложенията върху UDP непременно работят без такива механизми: ако се изискват, те трябва да бъдат реализирани от приложението или от протокол от по-високо ниво. Липсата на вградени механизми за надеждност може да бъде ограничение за приложения, при които всяка част от информацията трябва да бъде получена правилно. В същото време тя може да бъде предимство, когато по-важно е актуалните данни да пристигат навреме, отколкото изгубените данни да бъдат повторно изпращани със закъснение. Например при гласова комуникация кратка загуба на аудио данни може да бъде по-малко смущаваща от продължително забавяне, причинено от повторно предаване. Реалното качество обаче зависи от приложението, мрежовите условия и използваните механизми за обработка на загубите. Основните предимства на UDP са простата структура, малката заглавна част и възможността за изпращане на данни без предварително установяване на връзка. Това го прави подходящ за кратки заявки и отговори, както и за приложения, при които се изпращат чести актуализации и закъснението е важен фактор. Друго свойство е, че UDP позволява изпращането на съобщения до множество получатели чрез механизми на IP като broadcast или multicast, когато мрежата и приложението ги поддържат. Това може да бъде полезно при определени услуги за откриване на устройства, разпространение на информация или групова комуникация. Използването на такива механизми зависи от мрежовата среда и не е гарантирано във всяка интернет връзка. Най-същественото ограничение е липсата на вградени гаранции за доставка, подредба и защита от претоварване. Приложението трябва да прецени дали може да работи при загуба на дейтаграми или дали са необходими допълнителни механизми. Затова UDP не трябва да се определя като универсално по-бърз или по-добър от TCP. Той предоставя по-опростен транспортен механизъм, а пригодността му зависи от задачата. На фиг. 4 са показани основните етапи на функциониране на UDP.[3]



Фиг. 4. Основни етапи на функциониране на UDP

UDP се използва в различни интернет услуги и приложения. Един от примерите е DNS (Domain Name System), който преобразува домейн имена в IP адреси. Обичайните DNS заявки често използват UDP порт 53, тъй като обменът обикновено се състои от кратка заявка и отговор. DNS може да използва и TCP, например при някои по-големи отговори, трансфер на зони и други случаи, определени от протокола. Следователно DNS не е услуга, която използва единствено UDP. Друг пример са приложенията за гласова и видео комуникация в реално време. При такива приложения навременното получаване на текущите аудио- или видео данни често е по-важно от повторното предаване на вече остаряла информация. UDP може да намали транспортните забавяния, но качеството на

комуникацията зависи и от кодека, буферирането, мрежовото закъснение, загубата на пакети и механизмите за адаптация. UDP се използва и в онлайн игрите, при които често се изпращат актуализации за позицията и състоянието на игровите обекти. Ако някоя актуализация бъде изгубена, следваща може бързо да предостави по-нова информация. Това не означава, че всички онлайн игри използват само UDP: изборът зависи от архитектурата на конкретната игра и от изискванията към различните видове данни. Съвременен пример за използване на UDP като основа за по-сложен транспорт е QUIC, който се използва от HTTP/3. QUIC работи върху UDP, но реализира собствени механизми за надеждна доставка, криптографска защита и контрол на претоварването. Това показва, че UDP може да служи като базов транспорт за протоколи, които добавят функции, липсващи в самия UDP.

5 Сравнителен анализ на TCP и UDP

TCP и UDP изпълняват функцията на транспортни протоколи в архитектурата TCP/IP, но предлагат различни възможности за обмен на данни. TCP е ориентиран към връзка и осигурява надежден, подреден поток от байтове. UDP изпраща отделни дейтаграми без предварително установяване на връзка и не предоставя вградени гаранции за доставка и последователност. Поради това изборът между двата протокола трябва да се прави според изискванията на приложението, а не само според броя на функциите, които протоколът поддържа. Основните критерии за сравнение са начинът на установяване на комуникацията, надеждността, запазването на реда на данните, протоколното натоварване, управлението на потока и претоварването, както и типичните приложения. Тези критерии показват как характеристиките на транспортния слой влияят върху поведението на услугите, които използваме в интернет. Таблица 1 обобщава основните разлики между TCP и UDP

Таблица 1. Основни разлики между TCP и UDP

Критерий	TCP	UDP
Установяване на връзка	Установява логическа връзка преди обмена на данни	Не изисква предварително установяване на връзка
Тип на предаването	Поток от байтове	Отделни дейтаграми
Надеждност	Използва потвърждения и повторно предаване при загуба	Не осигурява вградено потвърждение или повторно предаване
Подредба на данните	Предоставя подреден поток към приложението	Не гарантира реда на пристигане на дейтаграмите
Контрол на потока	Поддържа механизъм за контрол на потока	Няма вграден механизъм за контрол на потока
Контрол на претоварването	Поддържа механизми за контрол на претоварването	Самият UDP не предоставя такъв механизъм; приложението или протокол от по-високо ниво може да го реализира
Размер на заглавната част	Минимално 20 байта без опции	8 байта
Протоколно натоварване	По-голямо заради състоянието на връзката и контролните механизми	По-малко, поради по-простата структура
Типични приложения	Уеб комуникации чрез HTTP/1.1 и HTTP/2, SSH, прехвърляне на файлове, електронна поща	DNS заявки, комуникации в реално време, онлайн игри и протоколи, изградени върху UDP

Посочените размери се отнасят до транспортните заглавни части: TCP има минимална заглавна част от 20 байта, която може да бъде по-голяма при наличие на опции, докато UDP заглавната част е 8 байта. Това е една от причините UDP да има по-малко транспортно натоварване, но само по този показател не може да се определи цялостната производителност на дадено приложение. Една от най-съществените разлики между TCP и UDP е начинът, по който се обработва загубата на информация. TCP се стреми да предостави на приложението пълен и подреден поток от данни. При загуба на сегмент протоколът може да го предаде повторно, а получателят възстановява правилната последователност на потока. Това е особено важно при прехвърляне на файлове, зареждане на уеб съдържание и отдалечено управление, където липсващите или разместени данни могат да доведат до неправилно обработване. При UDP всяка дейтаграма се обработва самостоятелно и протоколът не предприема автоматично повторно предаване. Това може да е недостатък, когато всяко съобщение трябва да бъде получено, но може да бъде приемливо при приложения, които обменят чести актуализации. Например при гласова комуникация повторното предаване на вече остарял аудио пакет може да е по-малко полезно от своевременното възпроизвеждане на следващите данни. Тук е важно да се направи разграничение между надеждност и навременност. TCP предоставя надеждност на транспортно ниво, но при загуби повторното предаване може да увеличи закъснението. UDP не гарантира по-ниско закъснение във всички мрежи, но избягва задължителните механизми за установяване на връзка и повторно предаване, присъщи на TCP. Реалното поведение зависи от мрежовите условия и от начина, по който приложението обработва получените данни. TCP поддържа състояние на връзката и използва контролни съобщения, потвърждения и механизми за управление на предаването. Това създава допълнителен протоколен обмен, но осигурява надеждност и адаптиране към възможностите на получателя и състоянието на мрежата. Контролът на потока предотвратява изпращането на повече данни, отколкото получателят може да обработи, а контролът на претоварването ограничава риска от прекомерно натоварване на мрежовия път. UDP има по-малка заглавна част и не изисква установяване на връзка. Това може да намали разходите за обмен при кратки съобщения и приложения, които изпращат чести дейтаграми. Въпреки това по-малкото функции на самия UDP не означават, че цялото приложение непременно ще използва по-малко ресурси или ще работи по-бързо. Ако върху UDP се изграждат собствени потвърждения, повторни предавания, криптиране и контрол на претоварването, тези функции също изискват ресурси и обмен на данни. Затова при оценката на производителността трябва да се разглежда цялата комуникационна система: приложният протокол, размерът на съобщенията, честотата на изпращане, загубите, закъснението и наличната пропускателна способност. Инструментите за анализ на трафика на локална мрежа са разгледани в [1]. TCP и UDP са различни инструменти за различни изисквания, а не универсална класация от „по – бавен“ и „по – бърз“ протокол. Сравнението показва, че TCP и UDP са предназначени за различни комуникационни потребности. TCP е подходящ, когато е необходим надежден и подреден поток от данни, а UDP предоставя по-прост обмен на отделни дейтаграми с по-малко вградени транспортни механизми. Не може да се твърди, че единият протокол е по-добър във всички случаи. При приложения, при които целостта и последователността на данните са водещи, TCP предоставя полезни гаранции. При приложения, чувствителни към закъснение или използващи собствени механизми за управление на обмена, UDP може да бъде по-подходящ. В крайна сметка решението се определя от изискванията към надеждността, времето за реакция, мрежовото натоварване и архитектурата на приложението. Този сравнителен анализ създава основа за следващата

глава, в която ще бъдат разгледани конкретни примери за използване на TCP и UDP в интернет услугите [2, 3].

6 Практическо приложение на TCP и UDP в интернет комуникациите

TCP се използва широко от приложения, при които е важно данните да бъдат предадени надеждно и в правилния ред. Типичен пример са уеб комуникациите чрез HTTP/1.1 и HTTP/2. При тези версии на HTTP транспортният обмен обичайно се осъществява чрез TCP. Протоколът осигурява подреден поток от байтове, върху който HTTP реализира правилата за заявките, отговорите и съдържанието на уеб ресурсите. Когато потребител отвори уеб страница, браузърът обменя съобщения със сървъра. На транспортно ниво TCP управлява връзката, проследява получаването на данните и при необходимост предава повторно изгубени части от потока. Това позволява на приложението да обработва информацията в правилната последователност. При HTTPS към комуникацията се добавя TLS, който осигурява криптографска защита на данните и проверка на сертификата на сървъра според използваната конфигурация. TCP сам по себе си не криптира съдържанието. Друг пример е SSH (Secure Shell), използван за защитен отдалечен достъп и администриране на системи. SSH обичайно използва TCP порт 22. TCP предоставя надежден транспортен канал, а SSH реализира функции като удостоверяване, криптиране и изпълнение на отдалечени команди. Това разграничение показва, че транспортният протокол и приложният протокол имат различни, но взаимно допълващи се роли. TCP се използва и при прехвърляне на файлове и електронна поща. При тези задачи е важно получените данни да съответстват на изпратените. Например SMTP използва TCP за обмен на съобщения между пощенски системи, а различни протоколи за достъп до пощенски кутии също могат да използват TCP. Надеждният транспорт намалява необходимостта приложението да реализира самостоятелно механизми за възстановяване на загубени части от потока. Един от широко разпространените примери за UDP е системата DNS (Domain Name System). DNS преобразува домейн имена, например имена на уеб сайтове, в IP адреси, необходими за установяване на мрежова комуникация. Обичайните DNS заявки често се изпращат чрез UDP порт 53. Тъй като много от тях се състоят от кратка заявка и отговор, UDP позволява обменът да започне без предварително установяване на TCP връзка. DNS обаче не използва само UDP. TCP също е част от DNS спецификациите и се използва в определени случаи, например при трансфер на DNS зони, както и когато условията на протокола налагат това. Затова при описание на DNS е по-точно да се посочи, че UDP е често използван за обичайни заявки, но TCP също има важна роля. UDP се използва и при гласови и видео приложения в реално време. При разговор през интернет приложението изпраща последователност от малки пакети с аудио- или видео данни. Ако пакет пристигне твърде късно, той може да има малка практическа стойност, тъй като възпроизвеждането вече е продължило. В подобни ситуации приложението може да предпочете навременната доставка на следващите данни пред повторното изпращане на вече закъснели данни. Използването на UDP не гарантира само по себе си високо качество на разговор или малко закъснение. Качеството зависи и от пропускателната способност, загубата на пакети, мрежовото закъснение, използвания кодек, буферирането и механизмите за адаптация. Приложенията често включват допълнителни средства за оценка на състоянието на мрежата и за компенсиране на загуби и колебания в закъснението. Онлайн игрите са пример за приложения, при които навременната информация често е от особено значение. Клиентите и сървърът могат да обменят данни за позицията на играчите,

състоянието на обектите и действията в игровия свят. При чести актуализации някои по-стари съобщения могат да загубят значението си, ако междувременно са получени по-нови данни. Затова UDP може да бъде подходящ за определени видове игрови трафик. При UDP обаче разработчиците трябва да отчетат възможността за загуба, дублиране или промяна на реда на дейтаграмите. Ако конкретна информация не бива да се губи, играта може да реализира собствени потвърждения или да използва отделен канал или протокол за нея. Следователно изборът на UDP не премахва нуждата от надеждност изцяло; той позволява на приложението да определи кои данни изискват допълнителни гаранции и кои могат да бъдат изпратени без тях. Този подход е полезен и при други интерактивни системи, които обменят чести актуализации. Във всички случаи изборът на транспорт зависи от характера на данните, допустимото закъснение и поведението, което приложението трябва да поддържа при загуба на пакети. Развитието на интернет протоколите показва, че разграничението между TCP и UDP не трябва да се свежда до твърдението, че TCP се използва за надеждност, а UDP - само за приложения, при които загубата е приемлива. Съвременен пример е HTTP/3, който използва QUIC като транспортен протокол, работещ върху UDP [5, 6]. QUIC реализира функции, които не са част от самия UDP, включително надеждна доставка на потоци, криптографска защита и контрол на претоварването [4, 5]. Така приложението използва UDP за пренасяне на дейтаграмите, докато QUIC добавя необходимите механизми за управление на комуникацията. Тази архитектура позволява различен подход към установяването на защитена комуникация и управлението на множество потоци данни. Примерът с HTTP/3 демонстрира, че изборът на транспортна основа е част от по-широкото проектиране на протоколите. При оценката на дадена технология трябва да се разглеждат функциите на всички съответни слоеве, а не само характеристиките на UDP или TCP поотделно. В таблица 2 е показано сравнение на времето за предаване на данни чрез TCP и UDP, а фиг. 5 резултат от данните.

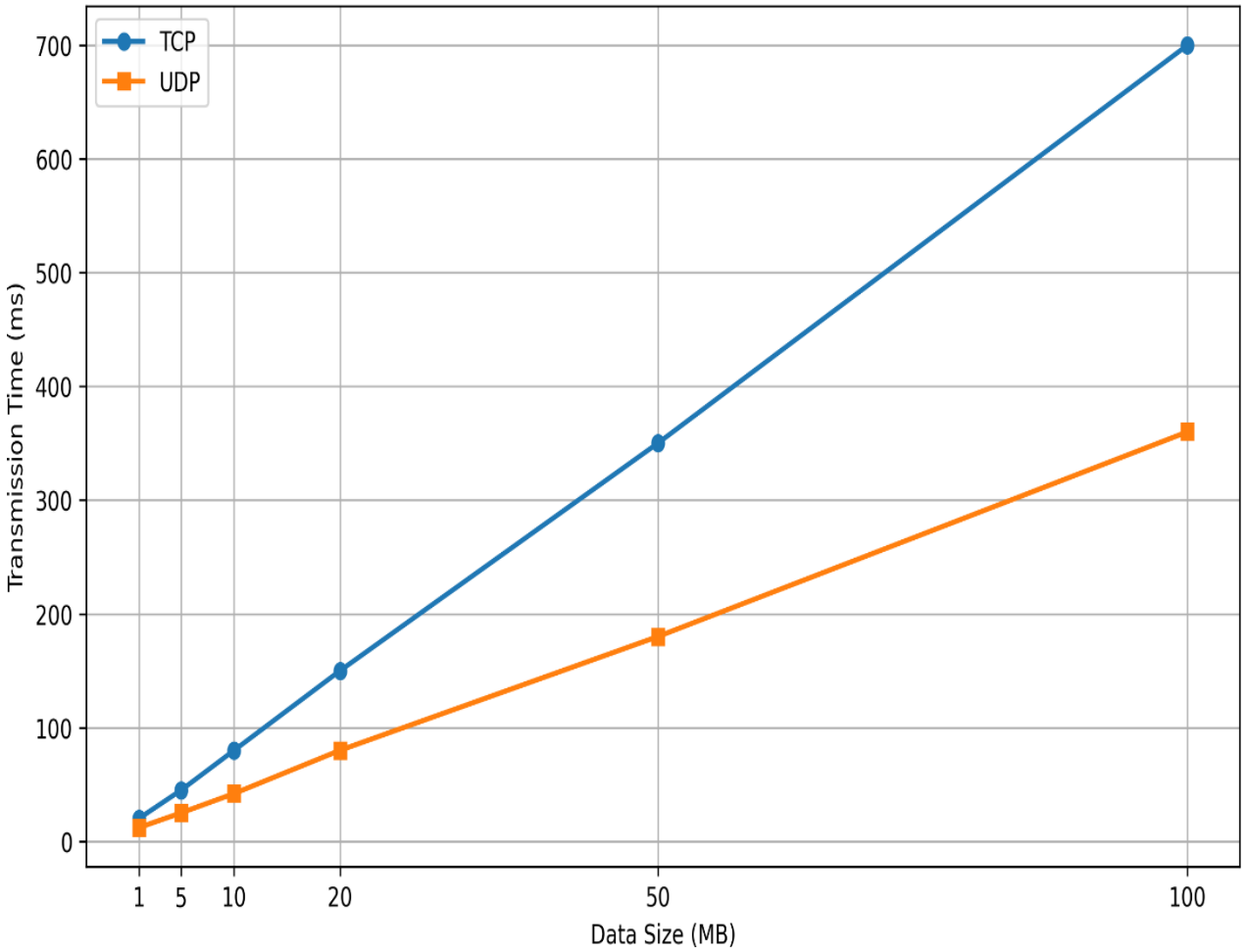
Таблица 2. Сравнение на времето за предаване на данни чрез TCP и UDP

Размер на данните (MB)	TCP (ms)	UDP (ms)
1	20	12
5	45	25
10	80	42
20	150	80
50	350	180
100	700	360

7 Заключение

Транспортните протоколи TCP и UDP имат съществено значение за функционирането на съвременните интернет комуникации. Те осигуряват обмен на данни между приложения, работещи на различни крайни устройства, но използват различни механизми за предаване и обработка на информацията. Разглеждането на техните характеристики показва, че изборът на транспортен протокол трябва да бъде съобразен с изискванията на конкретното приложение. TCP предоставя надежден и подреден поток от байтове чрез механизми за потвърждение, повторно предаване, контрол на потока и контрол на претоварването. Тези свойства го правят подходящ за услуги, при които е важно данните да бъдат получени правилно и в определен ред, като уеб комуникации чрез HTTP/1.1 и HTTP/2, отдалечено администриране чрез SSH и прехвърляне на файлове. UDP предлага по-опростен обмен на отделни дейтаграми, без предварително установяване на транспортна връзка и без вградени

гаранции за доставка и подредба. Този подход е полезен при кратки заявки и отговори, както и при приложения, чувствителни към времето, например някои DNS комуникации, гласови и видео приложения в реално време и определени видове игрови трафик. Когато са необходими допълнителни гаранции, те могат да бъдат реализирани от приложението или от протокол от по-високо ниво. Сравнителният анализ показва, че нито TCP, нито UDP е универсално по-добър във всички ситуации. TCP осигурява полезни механизми за надеждност, но повторното предаване и поддържането на връзка могат да повлияят върху закъснението. UDP има по-малко функции на транспортно ниво, но това не гарантира автоматично по-висока производителност. Реалното поведение зависи от мрежовите условия, вида на данните и изискванията на приложението. Примерът с QUIC и HTTP/3 допълнително показва, че съвременните комуникационни решения могат да комбинират UDP като транспортна основа с допълнителни механизми за надеждност, защита и контрол на претоварването. Това подчертава значението на взаимодействието между протоколите от различните слоеве на TCP/IP архитектурата. В заключение, познаването на принципите на работа, предимствата и ограниченията на TCP и UDP е важно за разбирането на интернет комуникациите и за правилния избор на транспортен механизъм. Изборът следва да се основава на необходимата надеждност, допустимото закъснение, обема на обменяните данни и начина, по който приложението обработва загуби и грешки.



Фиг. 5. Зависимост на времето за предаване от обема на данните при TCP и UDP

ЛИТЕРАТУРА:

[1] Стоянова, В., Талев, Д. Инструменти за анализ на трафика на локална мрежа. International Conference “Advanced Research and Technology for Defence” – ARTDef 2022, 2022, с. 133–141. ISSN 2815-2581.

[2] Eddy, W. (Ed.). Transmission Control Protocol (TCP). RFC 9293, Internet Engineering Task Force, 2022. https://www.rfc-editor.org/rfc/rfc9293

[3] Postel, J. User Datagram Protocol. RFC 768, Internet Engineering Task Force, 1980. https://www.rfc-editor.org/rfc/rfc768

[4] Thomson, M., Turner, S. Using TLS to Secure QUIC. RFC 9001, Internet Engineering Task Force, 2021. https://www.rfc-editor.org/rfc/rfc9001

[5] Iyengar, J., Thomson, M. QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000, Internet Engineering Task Force, 2021. https://www.rfc-editor.org/rfc/rfc9000

[6] Bishop, M. (Ed.). HTTP/3. RFC 9114, Internet Engineering Task Force, 2022. https://www.rfc-editor.org/rfc/rfc9114

APPLICATION OF CHEBYSHEV POLYNOMIALS IN PHOTOVOLTAIC SYSTEMS*

ILIYANA S. IVANOVA, TIHOMIR S. TRIFONOV

ABSTRACT: *Photovoltaic systems account for an increasing share of electricity grids, creating a need for accurate modeling and forecasting methods. Chebyshev polynomials form an orthogonal polynomial basis used to approximate nonlinear relationships and develop various numerical and forecasting models. This review examines the application of Chebyshev polynomials in photovoltaic systems. It covers the modeling of solar cells and meteorological dependencies, MPPT control, feature construction, spatiotemporal models, and Kolmogorov-Arnold networks (KANs). The analysis outlines the main advantages, limitations, and prospects for using the Chebyshev polynomial basis to forecast photovoltaic energy production.*

KEYWORDS: *Chebyshev polynomials, photovoltaic systems, approximation, forecasting, machine learning, photovoltaic power*

DOI: https://doi.org/10.46687/MT26ISI

ПРИЛОЖЕНИЕ НА ПОЛИНОМИТЕ НА ЧЕБИШЕВ ВЪВ ФОТОВОЛТАИЧНИТЕ СИСТЕМИ

ИЛИЯНА С. ИВАНОВА, ТИХОМИР С. ТРИФОНОВ

АБСТРАКТ: *Фотоволтаичните системи заемат все по-голям дял в електроенергийните мрежи. Това налага разработването на подходи за моделиране и прогнозиране с висока точност. Полиномите на Чебишев представляват ортогонален полиномен базис, който намира приложение при апроксимация на нелинейни зависимости и при разработването на различни числени и прогнозни модели. Настоящата обзорна статия проследява приложението на полиномите на Чебишев във фотоволтаичните системи. Разгледани са моделирането на соларни клетки и метеорологични зависимости, MPPT управлението, конструирането на признаци, пространствено-времевите модели и мрежите на Колмогоров–Арнолд (KAN). Анализът очертава основните предимства, ограничения и перспективи за използване на базиса от полиноми на Чебишев при прогнозиране на фотоволтаично производство.*

1 Въведение

Фотоволтаичните системи се характеризират с нелинейни зависимости между електрическите параметри, метеорологичните условия и произведената енергия. Тяхното математическо описание е необходимо при моделиране на соларни клетки, анализ на работните режими, управление и прогнозиране на производството.

За представяне на подобни зависимости се използват различни аналитични, статистически и числени методи. Един от подходите е полиномиалната апроксимация, която позволява сложни зависимости да бъдат описани чрез математически изрази.

Сред тези подходи са и полиномите на Чебишев. Поради ортогоналността и рекурентната си структура те се използват в задачи, свързани с апроксимация и числено моделиране [8]. Във фотоволтаичните системи полиномите на Чебишев се използват за моделиране на електрическите характеристики на соларни клетки [7], за представяне на

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

изменението на слънчевата радиация през денонощието [6] и като основа за моделиране и прогнозиране на фотоволтаичното производство. С развитието на методите за машинно обучение полиномите на Чебишев се използват и като част от по-сложни архитектури, включително невронни мрежи, пространствено-времеви графови модели и мрежи на Колмогоров–Арнолд. Това разширява възможностите за тяхното приложение от класическата полиномиална апроксимация към съвременни методи за анализ и прогнозиране на фотоволтаични системи [4], [10], [12]–[14].

Целта на настоящата статия е да се систематизират основните приложения на полиномите на Чебишев във фотоволтаичните системи и да се проследи развитието им от класическите апроксимационни модели до съвременните подходи за прогнозиране.

2 Математически основи на полиномите на Чебишев

Полиномите на Чебишев са клас ортогонални полиноми, които намират широко приложение в теорията на апроксимациите, числените методи и спектралното моделиране [8].

Полиномите на Чебишев от първи род се дефинират за $x \in [-1, 1]$ чрез зависимостта (1):

$$\mathrm{T_n(x)} = \cos\left(\mathrm{n}\arccos \mathrm{x}\right). \tag{1}$$

Полиномите на Чебишев от първи род със степени от нулева до пета са представени в табл. 1.

Таблица 1. Полиноми на Чебишев до пета степен

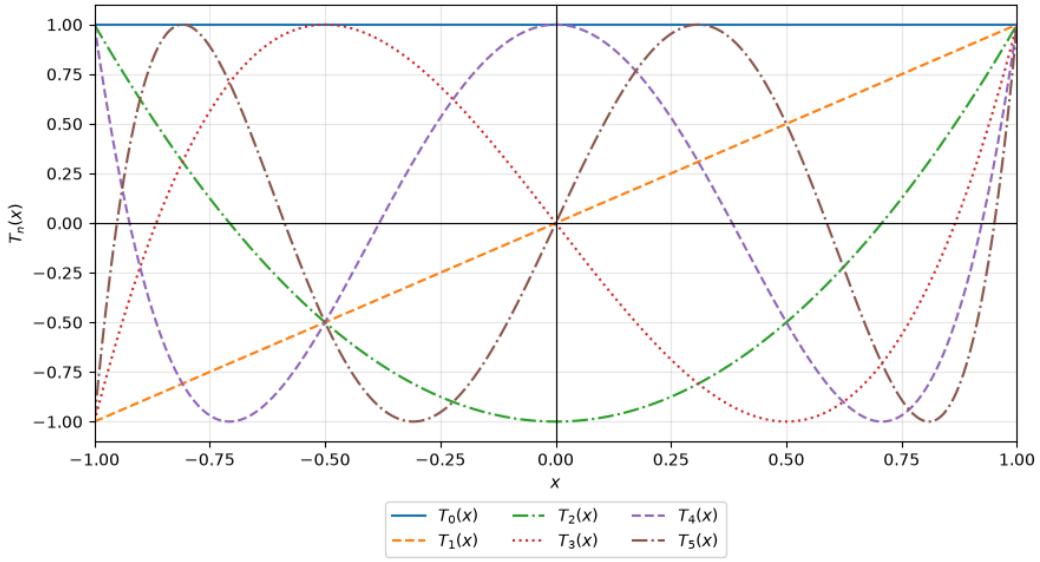
Полином	**Математически вид**
$T_0(x)$	1
$T_1(x)$	x
$T_2(x)$	$2x^2 - 1$
$T_3(x)$	$4x^3 - 3x$
$T_4(x)$	$8x^4 - 8x^2 + 1$
$T_5(x)$	$16x^5 - 20x^3 + 5x$

От таблицата се вижда, че всеки следващ полином се получава чрез рекурентната зависимост, като степента му нараства с единица. Полиномите $\mathrm{T_n(x)}$ са ограничени в интервала $[-1, 1]$, където стойностите им също принадлежат на $[-1, 1]$ [8]. При нарастване на степента се увеличава броят на колебанията на графиката, като всички полиноми от първи род имат стойност 1 при x=1. Тези свойства ги правят подходящи за представяне на функции с променлив характер в разглеждания интервал. Рекурентната зависимост позволява полиномите да се изчисляват последователно, без да е необходимо всеки от тях да се извежда отново поотделно.

На фиг. 1 е показано как се променя формата на графиките при преминаване от по-ниска към по-висока степен.

Полиномите на Чебишев могат да бъдат изчислявани рекурентно съгласно зависимостта (2) [8]:

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x). \tag{2}$$



Фиг. 1. Полиноми на Чебишев от първи род $T_0(x)$–$T_5(x)$ в интервала $[-1, 1]$

В рекурентната зависимост $T_n(x)$е полиномът на Чебишев от степен n, а x е неговият аргумент. Началните полиноми са $T_0(x) = 1$ и $T_1(x) = x$, чрез тях последователно се изчисляват полиномите от по-високи степени.

Ортогоналността на полиномите на Чебишев намалява зависимостта между отделните полиномни членове, характерна за стандартната степенна база [8]. Ортогоналното свойство на полиномите на Чебишев може да бъде представено чрез зависимостта (3):

$$\int_{-1}^{1} \frac{T_m(x)T_n(x)}{\sqrt{1-x^2}}\, dx = \begin{cases} \pi, & m = n = 0, \\ \dfrac{\pi}{2}, & m = n \neq 0, \\ 0, & m \neq n. \end{cases} \tag{3}$$

Тази зависимост показва ортогоналността на полиномите на Чебишев от различни степени върху интервала $[-1, 1]$ спрямо тегловата функция $1/\sqrt{1-x^2}$.

Тъй като стандартната област на дефиниране на полиномите на Чебишев е интервалът $[-1, 1]$, при практическото им приложение входните величини обикновено се преобразуват към този диапазон.

Нормализирането на входна величина x към интервала $[-1, 1]$ може да се извърши чрез зависимостта (4) [8]:

$$\tilde{x} = 2 \cdot \frac{x - x_{min}}{x_{max} - x_{min}} - 1 \tag{4}$$

Тук x е първоначалната стойност, а $x_{\min}$ и $x_{\max}$ са съответно минималната и максималната стойност в данните. Нормализираната стойност $\tilde{x}$ се преобразува в интервала $[-1, 1]$.

3 Приложения на полиномите на Чебишев във фотоволтаичните системи

Полиномите на Чебишев се прилагат при моделирането на характеристиките на соларните клетки [7]. Те се използват и в комбинация с невронни модели при моделиране на фотоволтаични системи [4]. Използването на полиномиални базисни функции позволява да се представи нелинейната зависимост между входните условия и електрическите характеристики на клетката.

Разработен е и шест-параметърен модел на соларна клетка. Той описва електрическите характеристики на клетката чрез шест параметъра, които участват във формирането на зависимостта между изходния ток и напрежението. При част от параметрите се отчита влиянието на температурата. Така моделът може да представи по-точно промените в работата на клетката при различни температурни и експлоатационни условия [7].

Полиномите на Чебишев са използвани за изграждане на аналитичен модел на токово-напреженовата характеристика на силициева соларна клетка. При традиционния еднодиоден модел връзката между тока и напрежението се описва с нелинейно уравнение, в което токът не е изразен непосредствено чрез напрежението. Поради това определянето на работната точка на соларната клетка може да изисква итеративни числени изчисления. В разглеждания подход полиномите на Чебишев се използват за апроксимация на нелинейните членове в уравнението, с което се получава по-удобно за изчисления представяне на токово-напреженовата зависимост [7]. Това улеснява анализа на характеристиката, като същевременно се запазва добра точност на модела.

Тези изследвания показват, че първоначално полиномите на Чебишев намират приложение при описанието на нелинейните електрически характеристики на соларните клетки.

A. Моделиране на метеорологични зависимости

Слънчевата радиация е един от основните фактори, определящи фотоволтаичното производство. Поради това метеорологичните прогнози са важен елемент при изграждането на точни модели за оценка и прогнозиране на фотоволтаичното производство.

Статистически модели са използвани за краткосрочно прогнозиране на метеорологични величини, сред които слънчевата радиация, температурата и скоростта на вятъра. В друго изследване е представено дневното изменение на слънчевата радиация с полином на Чебишев като част от метеорологичен модел за енергийни системи. Този пример показва как полиномите могат да представят характерни изменения на метеорологични величини, свързани с производството на електроенергия [6].

В друг модел ортогонален полином се използва за моделиране на интензивността на валежи, а полином на Чебишев – за моделиране на честотата на природни бедствия [2], [3]. Макар тези изследвания да не разглеждат пряко фотоволтаичното производство, те показват използването на полиномиални методи при анализа на метеорологични и природни процеси.

Прогнозирането на слънчевата радиация се разглежда и в публикации, посветени на статистически методи и машинно обучение. В тях се обобщават различни подходи и се подчертава значението на подходящите входни данни и избора на моделна структура. Тези фактори са важни и при моделирането на фотоволтаичното производство, тъй като точността на прогнозата зависи както от представянето на метеорологичните условия, така и от начина, по който те се свързват с изходната мощност [1], [9].

Разгледаните публикации показват, че метеорологичните зависимости могат да бъдат включени във фотоволтаичните модели по различни начини – чрез статистически прогнози, методи за машинно обучение и полиномиални апроксимации. Полиномите на Чебишев са приложими за представяне на нелинейното изменение на слънчевата радиация и могат да допълнят моделите, използвани за прогнозиране на фотоволтаично производство.

B. Проследяване на точката на максимална мощност

Фотоволтаичната система трябва да работи възможно най-близо до точката на максимална мощност при променящ се интензитет на слънчевата радиация. За тази цел се използват алгоритми за проследяване на точката на максимална мощност (Maximum Power Point Tracking – MPPT).

Разработен е адаптивен невронен контролер, базиран на рекурсивния стъпков метод (*backstepping*), за проследяване на точката на максимална мощност на фотоволтаична система. В предложената архитектура полиномите на Чебишев се използват в невронна структура за апроксимация на нелинейното поведение на системата.

В този случай базисът от полиноми на Чебишев изпълнява различна функция спрямо моделите на соларни клетки. Тук полиномите на Чебишев се използват не само за аналитично описание, а и като елемент от адаптивната система за управление. Това показва възможността полиномите на Чебишев да се използват като функционален базис в алгоритми за автоматично управление и оптимизация на работната точка на фотоволтаичната система [4].

C. Прогнозиране на фотоволтаично производство

a) Конструиране на входни признаци

При моделирането на фотоволтаична мощност полиномите на Чебишев се използват за преобразуване на входните данни и формиране на разширено пространство от признаци. По този начин могат да бъдат представени нелинейни зависимости, които стандартният линеен модел не би могъл да опише директно. Този подход демонстрира приложимостта на полиномите на Чебишев при прогнозиране на фотоволтаично производство. Подобен подход е приложен при едночасово прогнозиране на фотоволтаична мощност: входните данни се разширяват в пространство от полиноми на Чебишев, след което се подбират признаци за прогнозния модел [14].

Общият вид на апроксимация чрез полиноми на Чебишев може да бъде представен чрез зависимостта (5) [8]:

$$\hat{y}(x) = \sum_{k=0}^{n} a_k \, T_k(\tilde{x}) \tag{5}$$

В израза $\hat{y}(x)$ е апроксимираната функция, a_k са коефициентите на апроксимацията, $T_k(\tilde{x})$ е полиномът на Чебишев от степен k, а n е максималната степен на полинома. Аргументът $\tilde{x}$ е нормализиран в интервала $[-1, 1]$.

b) Пространствено-времеви модели

При прогнозиране на множество фотоволтаични системи, разположени на различни географски позиции, освен времевите зависимости могат да бъдат използвани и пространствените връзки между отделните обекти. Съвременните методи в тази област включват различни невронни архитектури и подходи за пространствено-времева обработка на данни [5], [13].

Друг подход е използването на пространствено-времева графова невронна мрежа за прогнозиране на производството на множество фотоволтаични системи. В този модел полиномите на Чебишев се прилагат при параметризирането на спектралните графови операции.

В този случай полиномите на Чебишев не се използват непосредствено за апроксимация на слънчевата радиация или фотоволтаичната мощност, а като математически инструмент във вътрешната структура на графовата невронна мрежа. Това показва развитието на приложението им от класическа числена апроксимация към елемент от съвременните методи за дълбоко обучение [13]. За разлика от класическия подход, при който полиномите изграждат апроксимационния модел на зависимостта между метеорологичните параметри и фотоволтаичното производство, в графовите невронни мрежи те подпомагат обработката на информация, свързана със структурата на графа. Така полиномите на Чебишев намират приложение както в моделирането на физически зависимости, така и в алгоритми за анализ на сложни взаимовръзки.

с) Мрежи на Колмогоров-Арнолд и съвременни прогнозни архитектури

В машинното обучение се развиват и мрежите на Колмогоров-Арнолд (Kolmogorov-Arnold Networks, KAN). За разлика от стандартните невронни мрежи, при които връзките между невроните се характеризират със скаларни тегла, при KAN могат да се използват обучаеми едномерни функции. Тези функции могат да бъдат представени чрез различни математически базиси, включително полиноми на Чебишев [10], [12].

За краткосрочно прогнозиране на фотоволтаична мощност е разработен моделът DSC-Chebyshev KAN-iTransformer [10]. Архитектурата съчетава дълбочинно разделима конволюция (*depthwise separable convolution*), KAN структура с базис от полиноми на Чебишев и iTransformer. Този базис позволява моделиране на сложни нелинейни зависимости между метеорологичните показатели и фотоволтаичната мощност. Комбинацията от тези компоненти подпомага извличането на различни характеристики от времевите данни и представянето на нелинейните зависимости, които влияят върху прогнозата. Така полиномите на Чебишев се използват не само за самостоятелна апроксимация, а и като част от по-сложна архитектура за прогнозиране.

За многостъпково прогнозиране на фотоволтаична мощност се използват многомащабни операции на конволюция и мрежи на Колмогоров-Арнолд с базис от полиноми на Чебишев. Моделът дава точкова прогноза и оценява неопределеността чрез конформно прогнозиране (*conformal prediction*).

Тези разработки показват, че базисът от полиноми на Чебишев може да бъде използван не само за класическа апроксимация, но и като компонент на съвременни прогнозни архитектури за представяне на сложни нелинейни зависимости и оценяване на неопределеността [10, 12, 13].

D. **Предимства и ограничения**

Полиномите на Чебишев притежават свойства, които ги правят приложими при апроксимация и моделиране на зависимости във фотоволтаичните системи. Едновременно с това ефективността им зависи от избора на базис, степените на полиномите и качеството на входните данни. Основните предимства и ограничения са обобщени в табл. 2. От таблицата се вижда, че полиномите на Чебишев предлагат подходяща основа за моделиране на нелинейни зависимости, но приложението им изисква внимателен подбор на входните променливи и степените. Точността на модела трябва да се оценява и върху данни, които не са използвани при обучението.

Таблица 2. Предимства и ограничения на полиномите на Чебишев

Критерий	Предимства	Ограничения
Представяне на зависимости	Комбинации от полиноми на Чебишев могат да апроксимират нелинейни зависимости между слънчевата радиация, температурата и фотоволтаичното производство.	При неподходящ избор на структура моделът може да не представи достатъчно добре сложните зависимости.
Ортогоналност	При подходящо нормализиране ортогоналността на базисните функции може да намали взаимната им корелация и числените затруднения при оценяване на коефициентите в сравнение с обикновената степенна база.	Ортогоналността не премахва напълно числените проблеми и зависи от използвания интервал и начина на нормализация.
Изчисляване	Рекурентната зависимост позволява полиномите да се изчисляват последователно и улеснява включването им в алгоритми за моделиране.	При многомерни модели броят на базисните функции нараства с броя на входните променливи и избраните степени.
Избор на сложност	Степента на полиномите може да се настройва според наличните данни и необходимата точност.	Твърде ниската степен може да доведе до недостатъчна апроксимация, а твърде високата – до прекомерно напасване към обучаващите данни.
Данни и приложимост	Полиномите се използват в класически модели за апроксимация и като базисни функции в някои подходи за машинно обучение.	Липсващи или неточни измервания, несъответствия във времевите данни и неотчетени фактори като засенчване, замърсяване или ограничения на инвертора могат да влошат

Е. Възможности за бъдещи изследвания

Разгледаните публикации показват, че полиномите на Чебишев се използват в различни направления на фотоволтаичните системи – от моделирането на соларни клетки и метеорологични зависимости до управлението и прогнозирането на фотоволтаичната мощност. В някои съвременни разработки те са включени като базисни функции в архитектури за машинно обучение, например в пространствено-времеви графови модели и мрежи на Колмогоров-Арнолд.

Въпреки широкия спектър от приложения, в разгледаната литература по-ограничено е представено използването на полиномите на Чебишев като самостоятелен многомерен модел за прогнозиране на фотоволтаичното производство. Това очертава възможност за бъдещи изследвания, които да оценят точността, устойчивостта и интерпретируемостта на такива модели при различни времеви хоризонти и набори от метеорологични данни.

Полезно би било резултатите да се сравнят с тези на статистически методи и алгоритми за машинно обучение при еднакви входни данни и критерии за оценка.

При разработването на системи за автоматизирано прогнозиране и управление следва да се отчитат и приложимите изисквания за защита на данните и нормативната уредба [11].

4 Заключение

Полиномите на Чебишев са средство за апроксимация с приложение в различни области на фотоволтаичните системи. Разгледаните изследвания показват, че те се използват както за описание на нелинейни физични зависимости, така и като базис в прогнозни модели и архитектури за машинно обучение.

Ортогоналността, рекурентното изчисляване и способността им да представят нелинейни зависимости правят полиномите на Чебишев подходящи за фотоволтаично моделиране. При многомерните модели обаче е необходимо внимателно да се подбират структурата и степените на полиномите.

Многомерната апроксимация с полиноми на Чебишев може да се използва за прогнозиране на фотоволтаичното производство и да допълни съществуващите статистически методи и подходи за машинно обучение.

ЛИТЕРАТУРА:

[1] Bazionis, A., K. P. N. D. Priya, and A. T. T. Karunakaran. “A Taxonomy of Short-Term Solar Power Forecasting: Classifications Focused on Climatic Conditions and Input Data.” IET Renewable Power Generation, 2023, DOI: https://doi.org/10.1049/rpg2.12736.

[2] Dimanova, Donika. “Statistical Modeling and Comparative Analysis of Intense Precipitation in Bulgaria – Application of an Orthogonal Polynomial in the Shumen Region.” 10th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE 2025), 5–7 November 2025. DOI: 10.1109/EEAE65901.2025.11273630.

[3] Dimanova, Donika, and Zdravko Kuzmanov. “Natural Disaster Frequency Model Program with Chebyshev Polynomial.” 2024 9th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), 2024, pp. 1–4. DOI: 10.1109/EEAE60309.2024.10600606.

[4] Govindharaj, Arunprasad, Anitha Mariappan, A. Ambikapathy, Vikas Singh Bhadoria, and Hassan Haes Alhelou. “Real-Time Implementation of Adaptive Neuro Backstepping Controller for Maximum Power Point Tracking in Photovoltaic Systems.” IEEE Access, vol. 9, 2021, pp. 105859–105875. DOI: 10.1109/ACCESS.2021.3099158.

[5] Guo, X. et al. “Image Feature Learning Combined with Attention-Based Spectral Representation for Spatio-Temporal Photovoltaic Power Prediction.” IET Computer Vision, vol. 17, no. 7, 2023, pp. 777–794. DOI: 10.1049/cvi2.12199.

[6] Liu, Y., M. C. Roberts, and R. Sioshansi. “A Vector Autoregression Weather Model for Electricity Supply and Demand Modeling.” Journal of Modern Power Systems and Clean Energy, vol. 6, no. 4, 2018, pp. 763–776. DOI: 10.1007/s40565-017-0365-1.

[7] Lun, S.-X., J.-S. Sang, and T.-T. Guo. “A New Six-Parameter Model Based on Chebyshev Polynomials for Solar Cells.” Mathematical Problems in Engineering, vol. 2015, Article 145258. DOI: 10.1155/2015/145258.

[8] Mason, J. C., and D. C. Handscomb. Chebyshev Polynomials. Chapman & Hall/CRC, 2003. DOI: 10.1201/9781420036114.

[9] Nguyen, Thi Ngoc, and Felix Müsgens. “What Drives the Accuracy of PV Output Forecasts?” 2021. https://doi.org/10.48550/arXiv.2111.02092.

[10] Sha, Mo, Shanbao He, Xing Cheng, and Mengyao Jin. “A Short-Term Photovoltaic Power-Forecasting Model Based on DSC-Chebyshev KAN-iTransformer.” Energies, vol. 19, no. 1, 2026, Article 20. DOI: 10.3390/en19010020.

[11] Simeonova, Iliana. “How GDPR Treats Automated Decision-Making.” Journal Scientific and Applied Research, vol. 28, no. 1, 2025, pp. 164–175. DOI:10.46687/jsar. v28i1.435.

[12] Takara, L. A. et al. “Multi-Scale Convolutional Chebyshev Kolmogorov-Arnold Networks Using Conformal Prediction for Photovoltaic Power Forecasting.” IEEE Access, vol. 14, 2026, pp. 81170–81194. DOI: 10.1109/ACCESS.2026.3694780.

[13] Verdone, Alessio, Simone Scardapane, and Massimo Panella. “Explainable Spatio-Temporal Graph Neural Networks for Multi-Site Photovoltaic Energy Production.” Applied Energy, vol. 353, 2024, Article 122151. DOI: 10.1016/j.apenergy.2023.122151

[14] Yang, Yu, Jia Mao, Richard Nguyen, Annas Tohmeh, and Hen-Geul Yeh. “Feature Construction and Selection for PV Solar Power Modeling.” 2022 IEEE International Symposium on Advanced Control of Industrial Processes (AdCONIP), 2022, pp. 90–95, DOI: https://doi.org/10.48550/arXiv.2202.06226.

ARCHITECTURE AND METHODOLOGY FOR RELIABILITY ASSESSMENT OF REDUNDANT INDUSTRIAL ETHERNET NETWORKS*

DRAGAN S. TONCHEV, TSVETOSLAV S. TSANKOV

ABSTRACT: *A redundant Industrial Ethernet architecture is developed for an automated packaging and dispatch line. The design combines a PROFINET ring, traffic segmentation, controlled supervisory access and centralized diagnostics. A methodology links communication deadlines, recovery coverage and failure consequences. Analytical examples quantify cyclic traffic, monitoring overhead and four-node connectivity under explicit assumptions. A reproducible verification procedure separates IP configuration checks from protocol-specific MRP testing. The approach provides explicit acceptance criteria and identifies the limits of media redundancy.*

KEYWORDS: *industrial Ethernet, PROFINET, reliability, redundancy*

DOI: https://doi.org/10.46687/MT26DST

АРХИТЕКТУРА И МЕТОДИКА ЗА ОЦЕНКА НА НАДЕЖДНОСТТА НА РЕЗЕРВИРАНИ ИНДУСТРИАЛНИ ETHERNET МРЕЖИ

ДРАГАН С. ТОНЧЕВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Разработена е резервирана Industrial Ethernet архитектура за автоматизирана линия за пакетиране и експедиция. Проектът съчетава PROFINET пръстен, сегментация на трафика, контролиран надзорен достъп и централизирана диагностика. Предложена е методика, свързваща времевите изисквания, успешното възстановяване и последствията от отказите. Аналитични примери оценяват цикличния трафик, служебния обмен и свързаността на четири възела при явни допускания. Разработена е възпроизводима процедура за проверка, която разграничава IP конфигурацията от изпитването на MRP. Резултатите определят приложимостта и ограниченията на резервирането на комуникационната среда.*

1 Въведение

В автоматизираната производствена линия комуникацията е част от управляващия контур. Достижимостта на контролер по IP адрес не доказва, че входните данни пристигат навреме, че операторът получава актуално състояние или че процесът запазва допустим режим при отказ. Поради това надеждността на индустриалната мрежа трябва да се оценява спрямо приложната задача, а не единствено чрез работещи портове и номинална скорост.

Разглеждаме линия за пакетиране и експедиция с транспортиране на изделия, групиране, пакетиране и предаване към складов участък. Комуникационната система включва два програмируеми логически контролера (PLC), четири операторски станции с интерфейс човек–машина (HMI), един сървър за надзорно управление и събиране на данни (SCADA) и шест разпределени входно-изходни станции. Избрана е PROFINET архитектура с управляеми индустриални Ethernet комутатори и пръстеновидно резервиране на средата.

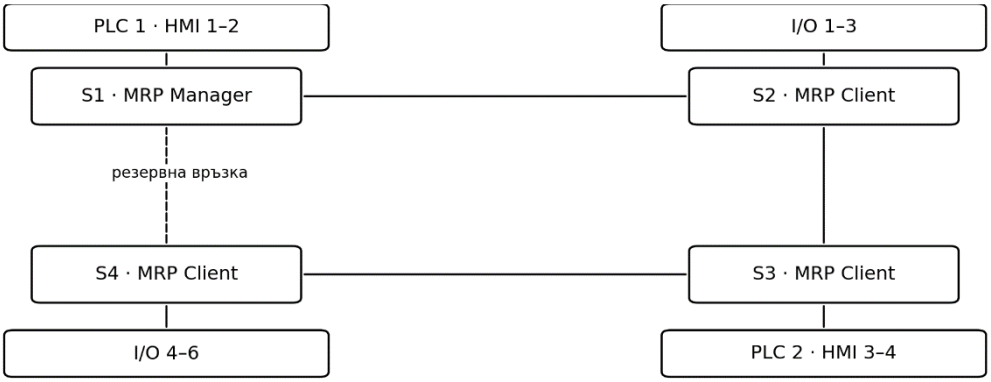
* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Контролерите управляват различни технологични участъци; наличието на два PLC не означава автоматично взаимно резервиране.

Целта е да се разработи архитектура и методика за оценка, които свързват топологията, времевите ограничения, натоварването и последствията от отказите. Приносът на разработката е конкретизирането на тази връзка за зададената система чрез определяне на функционалните комуникационни зависимости, аналитичен модел на пръстена, разчети на трафика и проверими сценарии. Представени са проектни решения и изчислени примери. Експлоатационните параметри следва да се установят на съвместим индустриален стенд.

2 Физическа архитектура и комуникационни зони

Четири комутатора S1–S4 образуват пръстен, а крайните устройства се разпределят по технологични участъци. S1 изпълнява ролята на MRP Manager, останалите възли са MRP Clients. Връзките на пръстена и достъпът на устройствата трябва да се реализират с интерфейси, чиято поддръжка на избрания режим е потвърдена за конкретния модел и фърмуер. Екранът на кабела, заземяването и маршрутите се съгласуват с електромагнитната среда и силовите инсталации.



Фиг. 1. Проектна физическа топология на пръстена и разпределение на крайните устройства по участъци. Общото присъединяване към комутатор не означава принадлежност към една VLAN

MRP предотвратява затворен комуникационен цикъл при нормална работа и възстановява пътя при единично прекъсване. Това е резервиране на преносната среда с възможна комуникационна пауза. То се различава от резервирането на контролери и интерфейси [1, 2]. Приложната допустимост на паузата се определя от наблюдението на цикличните данни и поведението на процеса. Ръководството [1] разглежда MRP реконфигуриране до 200 ms; тази граница не е доказателство за приемливост при конкретен PLC цикъл. Измереният приложен обмен и настройките на устройствата определят действителното прекъсване.

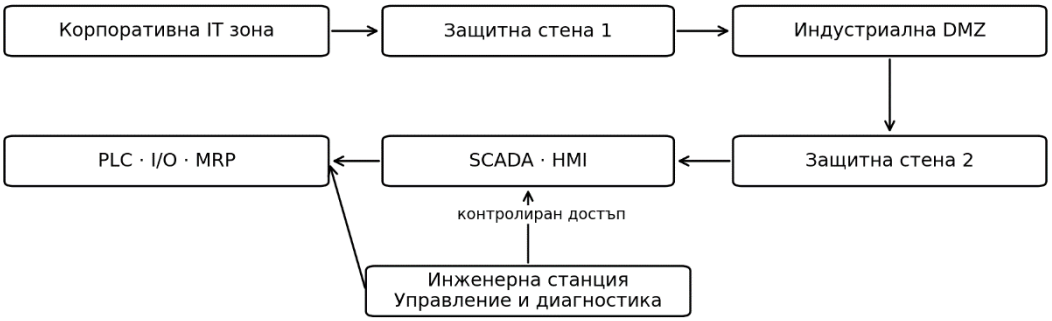
Логическото разделяне следва комуникационните зависимости. PLC и обслужваните от тях I/O станции остават в съвместим полеви сегмент. PROFINET RT обменът не се проектира като обикновен маршрутизиран IP поток между отделни подмрежи. HMI, SCADA и инженерният достъп се организират в отделни функционални зони, като допустимият надзорен IP обмен преминава през контролирани интерфейси.

Съвместимостта на VLAN маркирането и пръстеновите портове се проверява по документацията на оборудването.

Таблица 1. Проектна сегментация и минимални комуникационни зависимости

Зона	Адресна област	Допустим обмен
Полево управление	192.168.100.0/24	Два PLC и шест I/O станции; PROFINET в общ съвместим L2 домейн
Операторско наблюдение	192.168.110.0/24	Четири HMI и SCADA; разрешен приложен достъп към PLC
Инженерно управление	192.168.120.0/24	Конфигуриране и диагностика от определена инженерна станция
Индустриална DMZ	192.168.130.0/24	Посреднически услуги и отчетни данни; без общ достъп до полевата зона

Разпределението на отделни подмрежи отстранява неяснотата при поставяне на всички функционални VLAN в една обща IP мрежа. Идентификаторите на VLAN и разрешените протоколи се фиксират в конфигурационен регистър. VLAN отделя широковещателните домейни, но разрешаването на маршрутизация изисква допълнителни правила за достъп.



Фиг. 2. Комуникационни граници между IT, DMZ и производствената среда

Защитата на границите използва забрана по подразбиране и разрешаване на конкретни услуги. Отдалечената поддръжка се насочва към инженерна станция чрез удостоверен достъп; PLC не се излагат директно към външна мрежа. Журналите и резервните копия на конфигурациите поддържат възстановяването [3]. На фиг. 2 са показани функционални комуникационни зависимости, а не точните физически маршрути на пакетите. Разрешеният межзонов IP обмен се осъществява чрез конфигурирани маршрутизиращи интерфейси и правила за достъп. HMI и SCADA не се разглеждат като транзитни мрежови възли.

Пръстенът не отстранява единичните точки на отказ в крайните кабели, захранването, PLC и SCADA. Два кабела в една обща трасировка могат да бъдат прекъснати от едно събитие. При необходимост от защита срещу такъв отказ се предвиждат физически отделени маршрути и независими захранващи вериги. Резервирането се обосновава за всяка функция отделно.

3 Модел на трафика и времеви бюджет

За всеки информационен поток се задават източник, получател, период, дължина на кадъра, допустима възраст на данните и реакция при пропуск. Разграничаваме цикличния обмен PLC–I/O, надзорния обмен HMI/SCADA и инженерните операции. Критичността се определя от последствията за процеса. Голям брой пакети сам по себе си не е нито доказателство за ефективност, нито показател за надеждност.

Натоварването на дадена посока на връзка се изчислява само от потоците, които преминават през нея. При период T, n еднакви потока и дължина L на Ethernet кадъра, включваща FCS, преамбюлът със SFD и междупакетният интервал добавят общо 20 байтови времена. За скорост C получаваме:

$$B = n \cdot 8(L + 20) / T ; \rho = B / C \quad (1)$$

Илюстративно приемаме шест I/O станции, период 4 ms и кадър 128 B. Ако всички шест потока преминават през една посока на връзка, за нея B = 1,776 Mbit/s. Сборът за симетричен двупосочен обмен е 3,552 Mbit/s. При full-duplex 100 Mbit/s натоварването е 1,776% във всяка посока; сумата на двете посоки не се сравнява с капацитета само на едната. Допусканията са избрани за разчета, а не представени като измерени настройки.

Таблица 2. Разчет на периодичния обмен и сериализацията

Величина	Допускане или изчисление	Резултат
Период и брой потоци	T = 4 ms; n = 6 в една посока	1 500 кадъра/s
Дължина на кадъра	L = 128 B; добавени 20 B	148 байтови времена
Трафик в една посока	6 × 8 × 148 / 0,004	1,776 Mbit/s
Сериализация на кадър	8 × 148 / 100 000 000	11,84 μs
Непрекъсваем нископриоритетен кадър	1 522 B плюс 20 B	123,36 μs
Сериализация и едно блокиране на 3 изхода	3 × (11,84 + 123,36) μs	405,60 μs

Последният ред разглежда опростен път с три изходни порта, непредварително прекъсваемо предаване и строго приоритетно обслужване. На всеки изход може вече да се предава един нископриоритетен кадър. Получените 405,60 μs включват само сериализацията и тази форма на блокиране. Към тях се добавят обработката, разпространението, конкуриращият критичен трафик, PLC цикълът и времето на I/O станцията. Следователно стойността не е обща горна граница на приложното закъснение.

За поток с краен срок D приложният бюджет се записва като сума от времето за формиране на данните, мрежовото закъснение и времето за обработка при получателя. При прекъсване на пръстена се оценява и новият маршрут, който може да има повече комуникационни участъци:

$$T_{source} + T_{network} + T_{sink} \leq D \quad (2)$$

Проектното условие за устойчивост при отказ е $T_{gap} + T_{resume} < W$. T_{gap} е времето от регистрирания отказ до първия възстановен валиден приложен обмен. Tresume е допълнителното време от този момент до устойчивото възстановяване на приложната

функция. Двата интервала не се припокриват. W е максимално допустимото прекъсване за разглежданата технологична функция. Стойностите се определят за всяка критична връзка. Увеличаването на комуникационния timeout трябва да се съгласува с допустимата възраст на данните; то не е самостоятелно решение за надеждност.

4 Оптимизация на надзорния пакетен обмен

Надзорните заявки могат да групират съседни или съвместими променливи, когато приложният протокол го допуска. Това намалява повторените служебни полета и броя на транзакциите. Групирането се прилага към мониторинга, без произволно да променя цикличния PROFINET I/O обмен. Актуалността на алармите и технологичните блокировки се запазва като независимо ограничение.

За m записа с полезна дължина s и постоянна служебна част h разглеждаме модел на една транзакция, преди Ethernet и транспортното капсулиране. При отделни транзакции обемът е m(s + h), а при обща транзакция е ms + h. Коефициентът на полезно съдържание и относителното намаление са:

$$\eta(m) = ms \,/\, (ms + h)\,;\ \delta(m) = 1 - (ms + h) \,/\, [m(s + h)] \qquad (3)$$

Таблица 3. Илюстративно групиране при s = 32 B и h = 64 B

Брой записи m	Отделни транзакции	Обща транзакция	η	Намаление δ
1	96 B	96 B	33,33%	0%
2	192 B	128 B	50,00%	33,33%
4	384 B	192 B	66,67%	50,00%
8	768 B	320 B	80,00%	58,33%

Спестяването от 58,33% за осем записа се отнася до определения модел на транзакцията, а не до измерен общ Ethernet трафик. Реалният ефект зависи от MTU, сегментацията, потвържденията и ограниченията на PLC интерфейса. Ако записите се натрупват последователно през 10 ms, първият може да чака още 70 ms до формиране на групата. При налични едновременно данни това изчакване не възниква. Изборът на m трябва да съобрази свежестта на данните, а не само минималния обем.

Когато текущото натоварване нараства, проектната политика първо ограничава честотата на некритичните заявки и отлага архивните прехвърляния. Приоритетите на цикличния обмен и диагностичните аларми остават фиксирани. За да не се създават колебания, преминаването между режими се извършва по усреднени наблюдения с хистерезис. Праговете и периодът на усредняване подлежат на настройване чрез стендови изпитвания.

5 Аналитична оценка на свързаността и наличността

За да отделим ефекта на топологията от този на оборудването, разглеждаме четири изправни комутатора, независими еднакви връзки и фиксиран интервал на задача без ремонт. Нека q е вероятността една връзка да откаже през този интервал. Критерият е запазване на свързаността между всичките четири комутатора след приключване на реконфигурирането. Крайните устройства, захранването и времевите ограничения първоначално са извън модела.

При линия с три връзки е необходимо всички да останат изправни. В пръстен с четири връзки свързаността се запазва при нула или един отказ. Ако c е условната вероятност при един отказ резервният път да се активира успешно, получаваме:

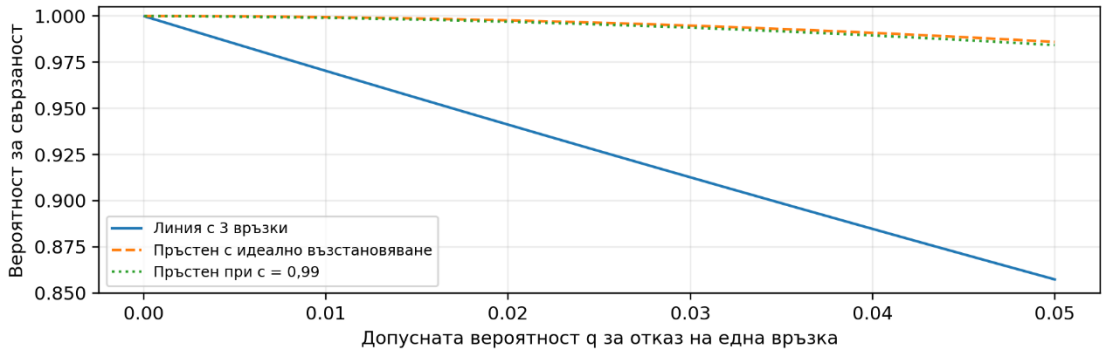
$$R_{line}(q) = (1-q)^3 \quad (4)$$

$$R_{ring}(q,c) = (1-q)^4 + 4cq(1-q)^3 \quad (5)$$

Моделът допуска успешното превключване да се представи с един общ параметър c. При различни портове, режими и места на отказ той трябва да се замени с отделни условни вероятности. При c = 1 оценката е идеализиран топологичен предел. Сравнението е между три връзки в линия и четири в пръстен при еднакъв брой възли, следователно подобрението изисква допълнителна връзка и поддръжка на резервиращия механизъм.

Таблица 4. Изчислена свързаност при явни допускания

q	Линия с 3 връзки	Пръстен с = 1	Пръстен с = 0,99
0,001	0,997003	0,999994	0,999954
0,010	0,970299	0,999408	0,999020
0,050	0,857375	0,985981	0,984267



Фиг. 3. Чувствителност на аналитичната свързаност спрямо q и c

При q = 0,01 пръстенът с c = 0,99 достига 0,999020 срещу 0,970299 за линията. Тези стойности са изчисления при допуснати вероятности. Те не са измерена наличност на реалната линия и не включват общи причини за отказ. Увеличаването на q показва, че резервният път намалява ефекта от единичен отказ, но не премахва риска от множество прекъсвания.

За приложната задача определяме cW като условна вероятност възстановяването при един отказ да е успешно и общата пауза да е под W. Тогава формула (5) се използва с cW вместо c. При липса на отказ приемаме, че приложните времеви изисквания са изпълнени. Тази замяна свързва структурната оценка с технологичния краен срок. Rshared означава вероятността през разглеждания интервал да останат работоспособни четирите комутатора и всички незарезервирани крайни устройства, присъединителни връзки и захранващи елементи, необходими за избраната приложна задача. Параметърът cW се определя при условие, че тези елементи са изправни. Произведението във формула (6) е приложимо при

обоснована независимост между тяхната работоспособност и отказите на пръстеновите връзки:

$$R_{task} = R_{shared} \cdot [(1-q)^4 + 4c_W \cdot q(1-q)^3] \quad (6)$$

За възстановима система се използва различен показател – наличност. Нека U е сумарното работоспособно време, а V е престоят поради отказ. Тогава наблюдаваната наличност е Aobs = U/(U + V). При стационарен модел със средно работоспособно време Tu и средно време за възстановяване Tv наличността е A = Tu/(Tu + Tv). Планираните престои се включват отделно, когато се оценява експлоатационната готовност.

При постоянна интензивност на отказите λ безотказността за интервал t е R(t) = exp(−λt) [4]. Този модел изисква обосновка за стационарност и не описва автоматично износване или обща причина за отказ. При реални наблюдения се представят продължителността, броят на събитията и неопределеността на оценката. Липсата на откази в кратък тест не доказва безкрайно средно време до отказ или зададена годишна наличност.

6 Анализ на отказите и диагностично покритие

Вероятностният модел описва избрани състояния, но не определя всички последствия. Допълваме го с FMEA, при който всяка функция се разглежда чрез вид на отказа, причина, локален ефект, ефект върху процеса и възможност за откриване. Методът е приложим към хардуерни, софтуерни и организационни зависимости [5]. За разглежданата архитектура основните сценарии са обобщени в таблица 5.

Таблица 5. Предварителен качествен анализ на отказите и последствията за комуникационната архитектура

Отказ или отклонение	Последствие за функцията	Откриване и проектна мярка
Една пръстенова връзка	Кратка пауза и промяна на маршрута	MRP събитие и PLC журнал; изпитване на cW
Две пръстенови връзки	Разделяне на пръстена на части	Наблюдение на всички критични двойки; отделени трасета
Комутатор или общо захранване	Загуба на локално присъединени устройства	Портови аларми и захранваща диагностика; независими вериги
Некритичен пакетен burst	Опашки и възможна загуба на актуалност	Броячи за опашки и приложна възраст; QoS и ограничаване
Грешна VLAN или ACL настройка	Блокиран разрешен обмен или нерегламентиран достъп	Положителни и отрицателни тестове; версиониране на настройките
Отказ на SCADA или крайна връзка	Загуба на наблюдение при възможно локално управление	Проверка на местния режим и аларми; резервиране според функцията

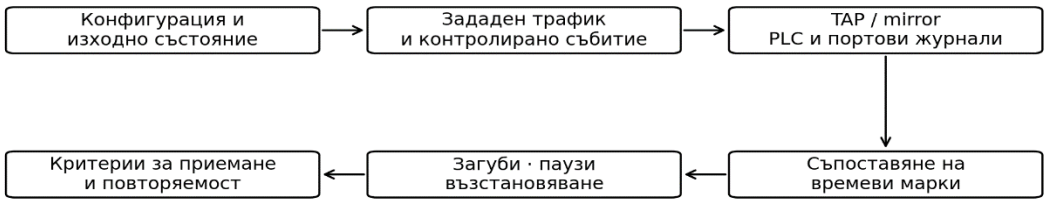
Ако се използва RPN = S · O · D, оценките за тежест S, честота O и затруднение на откриването D се задават по предварително определени скали. RPN е средство за подреждане, а не вероятност за отказ. Високата тежест на последствието се разглежда самостоятелно, защото различни комбинации могат да имат еднакво произведение. Не присвояваме числени оценки без данни или документирана експертна процедура.

Диагностичното покритие се оценява по това дали събитието е открито, локализирано и обработено навреме. Съобщение за възстановен порт не е равнозначно на възстановен

управляващ обмен. Затова портовите събития се съпоставят с пропуски на цикли, качеството на входните данни и поведението на изпълнителните механизми. При некоректни или остарели данни се проверява проектно зададената реакция на PLC.

7 Методика за функционално и времево изпитване

Изпитването се организира в три нива. Първо се проверяват адресиране, VLAN принадлежност, разрешени услуги и забранени маршрути. Второ се изпитват действителните PLC–I/O и HMI/SCADA връзки. Трето се проверява MRP поведението на съвместими устройства с контролирано прекъсване. Общ IP модел в Cisco Packet Tracer може да подпомага първото ниво; той не се приема като измерител на физически PROFINET/MRP характеристики.



Фиг. 4. Последователност за събиране и съпоставяне на доказателствата

За всяка серия се съхраняват модели и фърмуер, роли в пръстена, портови скорости, конфигурации, периоди на обмен и допустими паузи. Предлагаме четири варианта: базова конфигурация, функционална сегментация, сегментация с QoS и допълнително регулиране на надзорните заявки. Разликите се въвеждат последователно, за да се отдели приносът на всяка мярка.

Трафикът се наблюдава чрез TAP или mirror порт, а приложните събития – чрез PLC и SCADA журнали. Времевите марки зависят от захващащото оборудване и използвания часовник [6]. При две точки за измерване на еднопосочно закъснение часовниците се синхронизират и се оценява грешката. При една точка се измерва време заявка–отговор, когато протоколът позволява съпоставяне; то включва и обработката при получателя.

Разликата между два поредни момента на пристигане измерва междупакетен интервал, а не еднопосочно закъснение. За цикличен поток записваме периодите, пропуснатите цикли и възрастта на валидните данни. Загубите се установяват чрез приложни броячи или протоколни номера, със съобразяване на повторенията. Броят на филтрираните пакети в анализатора не се интерпретира като процент на доставка.

Времето на отказа се определя от общо регистрирано събитие, а не от ръчно натискане без времева марка. След него се установява първият валиден приложен обмен и устойчивото възстановяване за предварително определен прозорец. Методиката предвижда изпитване при прекъсване на всяка пръстенова връзка, възстановяване на кабела, отказ на възел, загуба на крайна връзка и два едновременни отказа. Сценариите извън проектния обхват на резервирането служат за установяване на последствията и проверка на зададената реакция на системата.

Натоварването се задава като възпроизводими профили на некритичния трафик, включително кратки bursts, защото средната скорост може да скрива опашки. Връщането

към изходна конфигурация и началното състояние се контролират преди всеки опит. Редът на вариантите се рандомизира или балансира, за да се ограничи влиянието на загряване, кеширане и времеви дрейф.

Единицата на повторение е независимият опит или предварително определен времеви блок. Последователните пакети в един поток не се приемат за независими наблюдения. Представят се брой опити, медиана, високи квантили, максимум и доверителни интервали. При малък брой повторения високите квантили се посочват като несигурни. За сравненията се отчитат размерът на ефекта и зависимостта между наблюденията, без p-стойността да се представя като вероятност хипотезата да е вярна.

Критерият за приемане изисква всички зададени разрешени услуги да работят и забранените връзки да са блокирани. При единично прекъсване на пръстенова връзка приложната пауза трябва да остава под W за всяка критична функция, включена в проектния обхват на резервирането. При два едновременни отказа или загуба на незарезервиран елемент се проверяват откриването на събитието и предварително определената реакция на системата; не се изисква автоматично запазване на всички услуги. При възстановяване на пръстена не трябва да възниква неконтролиран комуникационен цикъл. Успехът на ограничена серия потвърждава поведението в изпитаните условия; дългосрочната надеждност изисква отделно експлоатационно наблюдение.

8 Обсъждане на резултатите и граници на приложимост

Разработката дава три проверими аналитични резултата. При избрания периодичен обмен натоварването е 1,776 Mbit/s в посока. При групиране на осем мониторингови записа определеният транзакционен обем намалява от 768 на 320 B. При четири възела и q = 0,01 изчислената свързаност на пръстена с c = 0,99 е 0,999020. Всеки резултат има собствен набор от допускания и не се пренася автоматично към друг показател.

По-малкият надзорен обем може да освободи ресурси, но не доказва по-висока хардуерна безотказност. Запазената топологична свързаност не доказва спазен краен срок. Ниското средно натоварване не изключва кратък burst и пропуснат управляващ цикъл. Именно съвместното разглеждане на тези ограничения обосновава предложената методика.

При зависими откази, общо захранване или обща кабелна трасировка независимият модел на връзките е недостатъчен. При много кратки допустими паузи трябва да се разгледат други механизми на резервираност или промяна на управляващата архитектура. Изборът следва реалното технологично изискване, а не предположение, че наличието на пръстен гарантира непрекъсваемост.

9 Заключение

Предложената архитектура запазва конкретната производствена структура и я допълва с ясно определени комуникационни зони, контролирани зависимости и диагностика. Методиката свързва резервния път с допустимата приложна пауза чрез cW и отделя структурната надеждност от наличността на възстановимата система. Разчетите показват как натоварването, групирането на мониторингови данни и вероятността за успешно превключване могат да бъдат анализирани количествено.

Практическото потвърждение изисква стенд с поддържан PROFINET/MRP режим и протокол за повторяеми изпитвания. Представената процедура определя какви данни трябва да се събират и кога резервирането е приемливо за процеса. По този начин проектното решение се превръща в проверима инженерна постановка с установени граници на приложимост.

ЛИТЕРАТУРА:

[1] PROFIBUS & PROFINET International. PROFINET Planning Guideline Redundancy. Version 1.00, 07.05.2023, Order No. 8.132. https://www.profibus.com/download/profinet-installation-guidelines

[2] PROFIBUS & PROFINET International. PROFINET Media Redundancy Guideline. Version 1.03, April 2018, Order No. 7.212. https://www.profibus.com/download/profinet-media-redundancy-guideline

[3] Stouffer, K. et al. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3, 2023. DOI: 10.6028/NIST.SP.800-82r3.

[4] NIST/SEMATECH. e-Handbook of Statistical Methods. Section 8.1.6.1 Exponential. https://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm (достъп: 12.10.2026).

[5] IEC 60812:2018. Failure Modes and Effects Analysis (FMEA and FMECA). Edition 3.0. International Electrotechnical Commission, 2018.

[6] Wireshark Foundation. Wireshark User's Guide. Section 7.6 Time Stamps. https://www.wireshark.org/docs/wsug_html_chunked/ChAdvTimestamps.html (достъп: 12.10.2026).

AUTOMATED POSITIONING AND WEATHER PROTECTION OF A PHOTOVOLTAIC PANEL USING SIEMENS LOGO*

SUNAY H. SALIM, TSVETOSLAV S. TSANKOV

ABSTRACT: *A control architecture for stepwise photovoltaic panel positioning using Siemens LOGO! and an EPCC actuator is presented. Position feedback, weather signals and scheduled commands are coordinated through interlocks and defined priorities. A qualitative failure analysis specifies stopping and restart conditions and verification scenarios. Net energy yield is assessed through a comparative procedure including auxiliary consumption. The contribution is a project-specific control and verification framework; mechanical protection and energy gains require experimental validation.*

KEYWORDS: *photovoltaic panel, Siemens LOGO, positioning, weather protection, failure analysis*

DOI: https://doi.org/10.46687/MT26SHS

АВТОМАТИЗИРАНО ПОЗИЦИОНИРАНЕ И КЛИМАТИЧНА ЗАЩИТА НА ФОТОВОЛТАИЧЕН ПАНЕЛ СЪС SIEMENS LOGO

СУНАЙ Х. САЛИМ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Представена е архитектура за стъпково позициониране на фотоволтаичен панел със Siemens LOGO! и задвижване EPCC. Обратната връзка, климатичните сигнали и часовите команди са съгласувани чрез блокировки и определени приоритети. Качествен анализ на отказите задава условия за спиране, повторно пускане и функционална проверка. Предложено е сравнение на нетния енергиен добив с отчитане на собственото потребление. Приносът е съгласуване на управлението и изпитванията за конкретния проект; механичната защита и енергийният ефект изискват експериментално потвърждение.*

1 Въведение

Положението на фотоволтаичния панел влияе върху условията за приемане на слънчевото излъчване. Подвижната конструкция позволява промяна на ориентацията, но въвежда задвижване, датчици и допълнителни механични натоварвания. Управлението трябва да съчетае работното позициониране с реакция при неблагоприятни климатични условия.

Разглежданият проект използва стъпково едноосно позициониране в четири работни положения вместо непрекъснато следене. Siemens LOGO! изпълнява логиката, а електрически цилиндър EPCC премества рамката. Климатичните сигнали прекъсват нормалната програма и активират проектна защитна позиция [1].

Целта на доклада е да съгласува функционалната архитектура, приоритетите между режимите, реакциите при отказ и методиката за оценка на системата. Разработката доразвива проекта [1] с условия за преход между състоянията и критерии за проверка. Резултатът е проектно и програмно решение; енергийният добив и устойчивостта на конструкцията се оценяват отделно.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

2 Компоненти и обратна връзка

Системата включва основа, шарнирна рамка, панел, линейно задвижване, позиционни и климатични датчици. За сигналите за дъжд, вятър и градушка се задават източник, активно ниво и валидност. Сигналът за градушка изисква конкретен датчик или външен източник; наличието на дъжд не доказва градушка.



Фиг. 1. Функционална архитектура с обратна връзка за положението

LOGO! предоставя логически, времеви и часови функции, които могат да се комбинират в графична програма [2]. Необходимият брой входове се определя след отчитане на климатичните сигнали, четирите работни положения, защитния краен изключвател и органите за ръчно управление. При недостиг на входове се използва подходящо разширение. Фигура 1 показва информационните връзки; независимата защитна верига за аварийно спиране не е показана.

ЕРСС е електромеханично линейно задвижване, което преобразува въртенето на двигателя в линейно движение [3]. Изходите на LOGO! следва да подават команди към съвместим моторен контролер или управляващ интерфейс. Те не заместват силовото управление на двигателя. Изборът на мотор, контролер и монтажни елементи трябва да съответства на конкретната конфигурация.

3 Работни режими и приоритети

Часовата програма задава цел P1, P2, P3 или P4; съответният датчик потвърждава достигането ѝ. При настройване се съгласуват часовите граници, ходът на цилиндъра и ъгълът на панела. Системата следва предварителен график. След дневния период се връща към началното положение.

Климатичната заявка се формира от активните сигнали за дъжд, силен вятър или градушка. В проекта е избрана вертикална защитна позиция [1], като ефективността ѝ при различни климатични въздействия подлежи на експериментална проверка. Ориентацията се оценява за конкретната рамка, закрепване и посока на натоварването; една позиция не се приема автоматично за подходяща при всички опасности. При едновременни сигнали се задава предварително съгласувана реакция.

След отпадане на всички климатични заявки и при валидни входове се задейства времезакъснение за възстановяване на нормалния режим. В разглеждания проект е предвидена примерна продължителност от 10 min [1]. Повторна опасност нулира таймера.

След изтичането му се определя актуалната часова цел, вместо да се продължава прекъсната команда, която вече може да е остаряла.

Таблица 1. Режими и управляващи реакции

Режим	Условие	Реакция
Автоматично позициониране	Няма климатична опасност	Движение към зададеното P1–P4
Защитно позициониране	Климатична заявка; движение е разрешено	Движение към защитната позиция
Изчакване	Всички опасности са отпаднали; входовете са валидни	Задържане до изтичане на таймера
Ръчно управление	Ръчен режим без климатична заявка	Движение по операторска команда
Спиране при отказ	Блокировка или недостигната позиция	Спиране, запомнен отказ и сигнализация

Приоритетите се определят в следния ред: аварийно спиране и блокировки на задвижването; допустимо защитно позициониране; ръчна команда; часово позициониране. Климатичната заявка отменя нормалния режим, но не разрешава движение при активна авария, несъвместима обратна връзка или забранена посока. Аварийното състояние се запомня до отстраняване на причината и отделно потвърждение за повторно пускане.

4 Логика за движение и блокировки

Управлението допуска движение само в една посока. При смяна на посоката първо се прекратява текущата команда и се спазват условията за превключване на моторния контролер. Крайните изключватели блокират съответната посока и при ръчно управление. Програмното спиране се разглежда отделно от функцията за аварийно спиране, за която се предвижда подходяща независима защитна верига според оценката на риска.

Целта се сравнява с обратната връзка; при вече достигнато положение движение не се подава. При нова цел таймерът за движение се стартира от началото на прехода, но остава активно общо ограничение за непрекъснатото задвижване. Ако положението не бъде достигнато навреме, командата се прекратява и се запомня отказ. Времевите граници се настройват по реалния ход, скорост и натоварване. Смяната на режима не трябва да позволява безкрайно движение чрез постоянно рестартиране на таймерите.

Ръчният режим отменя часовата програма, но запазва климатичния приоритет и блокировките. След авария потвърждението за нулиране не е команда за движение; необходимо е отделно разрешение за пускане. Обслужването се извършва по процедура с ограничен достъп до движещите се части и определени условия за повторно включване.

При липса на позиционен сигнал се различават движение между положенията и неизвестна позиция след включване. Първото се допуска само в рамките на започнат и ограничен по време преход; второто изисква определена процедура за установяване на положението. Несъвместими сигнали водят до спиране. След прекъсване на захранването не се възстановява безусловно предишната команда. Поведението на рамката без захранване се проверява механично, включително необходимостта от задържане на товара.

5 Анализ на отказите и последствията

Анализът свързва елементите, отказите, последствията, откриването и реакциите (таблица 2). Не се задават недоказани вероятности. Отчитат се и скрити откази: двоичен вход не позволява непременно да се отличи повреден климатичен датчик от реална липса на опасност. Диагностиката се съгласува с избрания датчик.

Таблица 2. Откази и проектни реакции

Отказ	Последствие и откриване	Проектна реакция
Климатичен вход остава неактивен	Възможна пропусната опасност; проверка с контролен сигнал	Тест на датчика; реакция при невалиден вход
Несъвместими позиционни сигнали	Положението е неоднозначно; логическа проверка	Спиране и запомняне на отказа
Задвижването не достига целта	Блокиране или претоварване; таймер и сигнал от контролера	Прекратяване на командата; проверка преди ново пускане
Краен изключвател не сработва	Риск от надхвърляне на хода; отделно стендово изпитване	Независимо ограничаване на хода според механичния проект
Прекъсване на захранването	Невъзможен защитен преход; проверка на задържането	Оценка на механичното задържане и необходим резервен ресурс

За климатично събитие се проследяват последователно наличието на валиден сигнал, разрешението за движение, работата на задвижването и потвърждението за защитна позиция. Успешната команда без позиционно потвърждение не е успешна защита. При отказ системата спира и сигнализира, но конструкцията може да остане изложена на натоварване. Ето защо програмната реакция и остатъчният механичен риск се оценяват поотделно.

6 Методика за функционална проверка

Проверката обхваща входните комбинации и преходите между режимите. LOGO! Soft Comfort позволява симулиране на входове и наблюдение на изходите и таймерите [2]. Таблица 3 задава очакваното поведение. Изпитват се и граничните моменти: опасност непосредствено преди края на изчакването, смяна на часовата цел по време на движение и отказ при защитен преход.

Всеки тест съдържа начална позиция, входна последователност с времена, очаквани и действителни изходи. Измерват се реакцията и преходът, проверяват се спирането при целта и взаимното изключване на посоките. След симулацията се провеждат стендови проверки на задвижването, рамката и датчиците.

7 Методика за оценка на енергийния ефект

Сравнението използва едновременно наблюдавани подвижен и неподвижен панел с близки електрически характеристики, еднакви условия на засенчване и съпоставими преобразуватели. Задават се ориентацията на неподвижния панел, графикът на подвижния, интервалът на запис и периодът на наблюдение. Отчитат се излъчването, температурата на модулите, произведената енергия, престоят в защитен режим и броят на преместванията. Различни метеорологични дни не се сравняват директно без подходящо съгласуване на условията.

Нетната енергия се определя като $E_{нет} = EPV - E_{спом}$, където $E_{спом}$ включва задвижването, контролера, датчиците и загубите в тяхното захранване за целия период, включително изчакването. Същият принцип се прилага към референтната система. Ефектът е $G = (E_{нет,подв} - E_{нет,стат}) / E_{нет,стат} \times 100\%$, при $E_{нет,стат} > 0$ и еднакви граници на измерване. Ако спомагателното потребление вече е включено в измерената отдадена енергия, то не се изважда повторно.

Таблица 3. Функционални сценарии за проверка

Входно условие	Очакван резултат
Нова часова цел при безопасни условия	Движение до целевия датчик и спиране
Опасност по време на движение	Отмяна на часовата цел; защитен преход само при разрешено движение
Климатичният сигнал отпада	Изчакване след отпадане на всички заявки
Опасността се връща преди края на таймера	Отмяна на възстановяването
Противоположни команди	Не се активират едновременно двете посоки
Целта не е достигната навреме	Спиране и аварийна сигнализация
Краен изключвател при ръчен режим	Движението в съответната посока се блокира
Опасност при активен отказ	Няма движение; отказът запазва приоритет
Включване с неизвестна позиция	Без автоматично продължаване на предишната команда
Несъвместими позиционни сигнали	Спиране и запомняне на отказ
Нулиране след отстранен отказ	Без самостоятелно стартиране на движение

8 Резултат от разработката и ограничения

Разработката свързва четирите работни положения и защитната позиция с приоритети, блокировки, условия за повторно пускане и проверими реакции при отказ. Анализът показва къде липсваща диагностика или механична зависимост може да попречи на защитния преход. Приносът е тази съгласувана организация на проекта и изпитванията, а не доказан процент на енергиен прираст или количествена надеждност.

Климатичната защита се оценява чрез времето за позициониране, допустимите натоварвания и задържането при отпаднало захранване. Изпитват се конкретните закрепвания и задвижване. Без експлоатационни данни не се задават интензивности на отказ или вероятности за успешна защита. Енергийните, програмните и механичните проверки не се заменят взаимно.

9 Заключение

Системата съчетава стъпково позициониране с климатична реакция. Доработката свързва приоритетите, отказите и повторното пускане с проверими сценарии. Оценката на нетния добив включва потреблението на управлението и задвижването. Следващият етап е прототип с документирани функционални, енергийни и механични изпитвания.

ЛИТЕРАТУРА:

[1] Салим, С. Х. Автоматизирана система за управление на соларен панел в зависимост от климатичните условия. Дипломна работа, Шуменски университет „Епископ Константин Преславски“, 2026.

[2] Siemens AG. LOGO! System Manual. Edition 07/2022, A5E33039675-AK. https://cache.industry.siemens.com/dl/files/041/109741041/att_924628/v1/logo_system_manual_en-US_en-US.pdf

[3] Festo. Electric Cylinder EPCC. Technical Catalogue, 2025/09. https://www.festo.com/media/catalog/203025_documentation.pdf

EXPERIMENTAL STUDY OF THE RESPONSE TIME AND PERFORMANCE OF A WEB-BASED INFORMATION SYSTEM UNDER CONCURRENT REQUESTS*

YOVKO M. HRISTOV, DESISLAV M. HRISTOV

ABSTRACT: *This paper presents an experimental evaluation of response time and throughput for the web-based information system "Doktorant". The tests were conducted against a remotely accessible test environment using k6 and varying numbers of virtual users. The scenario includes authentication, dashboard access, opening the doctoral-student list, searching for a test profile, and requesting the second list page. The measured indicators include average HTTP response time, the 95th percentile, throughput, and failed requests. When the load increases from 20 to 100 virtual users, average HTTP response time rises from 147.08 ms to 419.47 ms, while throughput increases from approximately 24.00 to 89.52 requests per second. No failed HTTP requests were recorded in the reported two-minute runs. The results indicate increasing response latency under higher concurrent load and provide a basis for further application profiling and optimization.*

KEYWORDS: *web application, performance, response time, load testing, k6, PHP, MariaDB*

DOI: https://doi.org/10.46687/MT26YMD

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ НА ВРЕМЕТО ЗА РЕАКЦИЯ И ПРОИЗВОДИТЕЛНОСТТА НА WEB БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ПРИ ЕДНОВРЕМЕННИ ЗАЯВКИ

ЙОВКО М. ХРИСТОВ, ДЕСИСЛАВ М. ХРИСТОВ

АБСТРАКТ: *В доклада е представено експериментално изследване на времето за реакция и производителността на WEB базираната информационна система „Докторант". Изследването е проведено върху отдалечено достъпна тестова среда чрез инструмента k6, като натоварването е генерирано с различен брой виртуални потребители. Тестовият сценарий включва удостоверяване на потребителя, зареждане на табло, отваряне на списък с докторанти, търсене на тестов профил и зареждане на втора страница от списъка. Оценени са средното време за HTTP отговор, 95-ият процентил (p95), пропускателната способност и броят на неуспешните заявки. При увеличаване на натоварването от 20 до 100 виртуални потребители средното време за отговор нараства от 147,08 ms до 419,47 ms, докато пропускателната способност се увеличава от приблизително 24,00 до 89,52 заявки в секунда. В проведените двуминутни тестове не са отчетени неуспешни HTTP заявки. Резултатите показват нарастване на времето за реакция при високо конкурентно натоварване и дават основа за последващо оптимизиране и по-задълбочено профилиране на приложението.*

1 Въведение

WEB базираните информационни системи осигуряват достъп до функционалности и данни чрез стандартен браузър и обикновено обслужват множество потребители чрез обща приложна и сървърна инфраструктура. При такъв модел времето за реакция зависи не само от алгоритмите на приложението и операциите в базата данни, но и от уеб сървъра, PHP средата, мрежовата свързаност и наличните системни ресурси. Поради това

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН"

функционалната коректност сама по себе си не е достатъчна за оценка на качеството на една система; необходимо е да се изследва и поведението ѝ при конкурентни заявки.

Обект на изследване е WEB базираната информационна система „Докторант“, разработена като прототип за подпомагане на процесите по управление на информацията за докторанти. Предмет на изследването са времето за HTTP отговор и пропускателната способност на системата при различен брой виртуални потребители.

Целта на изследването е експериментално да се оцени изменението на времето за реакция и броя обслужени HTTP заявки в секунда при постепенно увеличаване на натоварването. За постигането ѝ са поставени следните задачи: да се дефинира повторяем тестов сценарий; да се изпълнят тестове с различен брой виртуални потребители; да се измерят основни показатели за производителност; да се сравнят резултатите; и да се формулират изводи относно поведението на системата и ограниченията на експеримента.

Изследването е ограничено до отдалечено достъпната тестова инсталация. Поради това измереното време за HTTP отговор включва мрежовото взаимодействие между генератора на натоварване и сървъра, както и обработката на заявката от сървърната инфраструктура. То не трябва да се тълкува като чисто време за изпълнение на PHP код или SQL заявка.

2 Теоретични основи и измервани показатели

a. Натоварващо тестване

Натоварващото тестване оценява поведението на софтуерна система при зададено ниво на активност. Натоварването може да се моделира чрез виртуални потребители, честота на заявките, продължителност на теста и последователност от действия. При WEB приложенията виртуалният потребител изпълнява сценарий, който може да включва множество HTTP заявки, паузи и проверки на получените отговори. Следователно броят на виртуалните потребители не е равнозначен на броя заявки, изпратени едновременно във всеки момент. [1], [6]

b. Време за отговор

Времето за HTTP отговор измерва интервала от изпращането на заявката от клиента до получаването на отговора. Средната стойност дава обща представа за времето за обслужване на заявките, но невинаги отразява достатъчно ясно наличието на по-бавни отговори. Медианата представя централната стойност на разпределението, а 95-ият процентил (p95) показва времето, в рамките на което са приключили 95% от измерените заявки. Останалите 5% са с по-дълго време за отговор. Поради това p95 допълва средната стойност и позволява по-пълна оценка на поведението на системата при натоварване. [2]

c. Пропускателна способност и грешки

Пропускателната способност в настоящото изследване се представя чрез броя HTTP заявки, обработени за секунда (requests per second, req/s). Тя се разглежда съвместно с времето за отговор: увеличаването на броя заявки в секунда не е непременно признак за линейно мащабиране, ако времето за отговор расте значително. Делът на неуспешните HTTP заявки и резултатите от функционалните проверки се използват като показатели за надеждността на изпълнението на тестовия сценарий.

Използваните показатели се интерпретират съвместно. Ниското ниво на грешки показва, че заявките са обработени успешно в рамките на проверките, но не означава автоматично, че времето за реакция е постоянно или че системата има неограничен капацитет. [1], [2]

3 Изследвана система и тестова среда

„Докторант“ е WEB базирана информационна система, предназначена за управление на информация, свързана с докторантското обучение. В разработения прототип са реализирани функционалности за управление на докторанти и потребители, контрол на достъпа и други административни операции. Приложението използва PHP, уеб сървър Apache и релационна база данни MariaDB. Документацията на използваните технологии е представена в [3–5]. В тестовата среда системата е достъпна през HTTPS.

За натоварващите тестове е използван отделен компютър с Windows, от който се стартира k6 чрез PowerShell. Сървърната среда е виртуална машина с Ubuntu, Apache, PHP-FPM 8.3 и MariaDB 10.11.14. Тези версии са отчетени от диагностичните изходи на сървъра. Измерванията са извършени срещу отдалечената инсталация, а не върху локална среда.

В базата данни са създадени 500 синтетични тестови профила, предназначени за проверка на списъка, търсенето и пагинацията. Тестовите записи използват различими идентификатори и не представляват реални докторанти. Това позволява изпълнение на повтаряеми операции върху набор от данни с известен размер. Резултатите не следва автоматично да се екстраполират към значително по-големи бази данни или към реално производствено натоварване.

Генериране на натоварването

Натоварването е генерирано с k6 чрез сценарий с фиксиран брой виртуални потребители и зададена продължителност. Всяка итерация включва зареждане на страницата за вход, извличане на CSRF токен, удостоверяване, зареждане на таблото, отваряне на списъка с докторанти, търсене на предварително определен тестов профил и зареждане на втората страница. Между някои действия има паузи, така че тестът моделира последователност от потребителски операции, а не непрекъснато изпращане само на една заявка.

Скриптът проверява HTTP статусите, наличието на CSRF токен, пренасочването след удостоверяване, зареждането на основните страници и наличието на търсения тестов профил. По този начин резултатите от производителността се съпоставят с изпълнението на функционалните проверки. [1], [6]

4 Методика на експеримента

При основните сравнения са използвани тестове с продължителност две минути и различен брой виртуални потребители. Този подход позволява сравнение на поведението при нарастващо натоварване в относително еднакъв времеви прозорец. В наличните резултати има и по-ранни кратки пилотни тестове, както и тест с 100 VU за пет минути. Те се запазват като допълнителни наблюдения, но не се смесват без уточнение с двуминутните тестове.

За част от ранните нива има повече от едно измерване или по-кратки пробни изпълнения. В основната графика са използвани представителните двуминутни резултати, когато такива са налични. Тестът с 1 VU е кратък и не е напълно съпоставим с двуминутните изпълнения, затова не е включен в основната графика за натоварването. [1], [6]

Ограничения на методиката

Измерванията са проведени от отдалечен клиент, поради което резултатите включват влияние на мрежовия път и състоянието на клиентската и сървърната инфраструктура. Не

е използван непрекъснат запис на CPU, RAM, swap и дискова активност през целия период; налично е наблюдение на пикови стойности чрез top. Следователно системните показатели се използват като контекст, а не като пълна времева серия. Не са измервани отделно времето за SQL операции и времето за изпълнение на PHP код.

Единична неуспешна HTTP заявка е отчетена в петминутния тест с 100 VU. В повторния двуминутен тест със 100 VU не са отчетени неуспешни заявки. Това различие се отбелязва в анализа, без да се прави неподкрепено заключение за причината на единичния неуспех.

Таблица 1

Параметър	Описание
Инструмент	k6
Генератор на натоварване	Windows клиент, стартиране чрез PowerShell
Сървърна среда	Ubuntu VM; Apache; PHP-FPM 8.3; MariaDB 10.11.14
Данни	500 синтетични тестови профила
Основен сценарий	Вход, табло, списък, търсене, втора страница
Основна продължителност	2 минути за основните сравнителни тестове
Нива на натоварване	5, 10, 20, 30, 50 и 100 VU
Показатели	Средно време, медиана, p95, req/s, неуспешни заявки и checks

5 Резултати от експерименталното изследване

Таблица 2 представя основните двуминутни измервания. За 5 VU е използван тестът с продължителност две минути; за 10, 20, 30, 50 и 100 VU са използвани отчетените резултати от съответните двуминутни изпълнения.

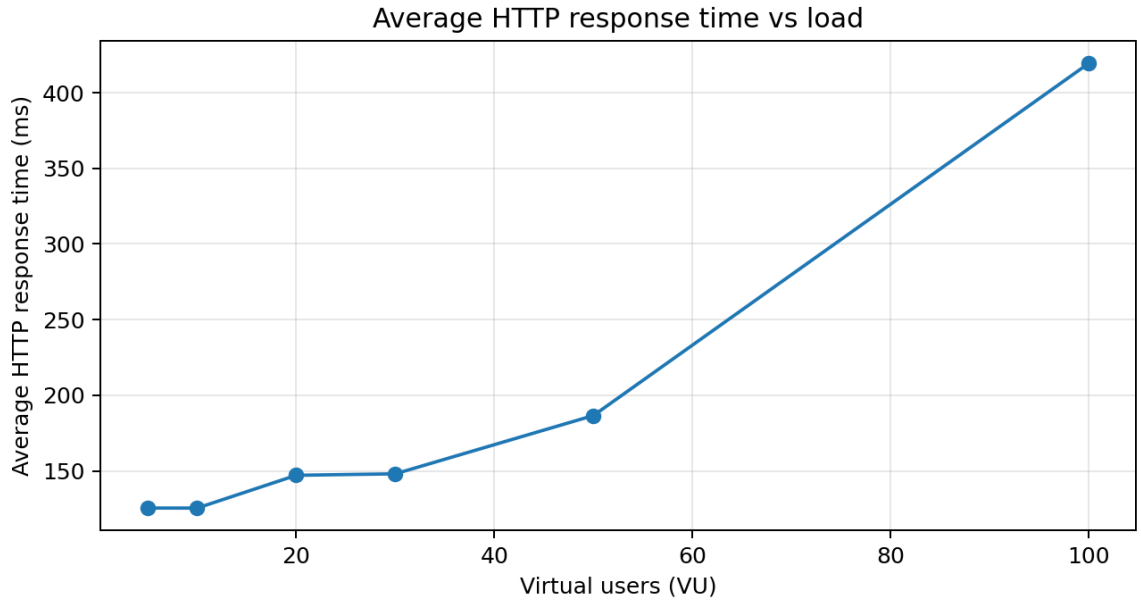
Таблица 2

Виртуални потребители (VU)	**Средно HTTP време (ms)**	**p95 (ms)**	**HTTP заявки/s**	**Неуспешни заявки**
5	125.44	215.16	6.27	0
10	125.41	217.74	12.51	0
20	147.08	265.24	24.00	0
30	148.06	262.74	36.29	0
50	186.60	367.91	57.59	0
100	419.47	894.62	89.52	0

Забележка: За 5 VU двуминутният тест е изпълнен за 2 минути и 130 итерации; за останалите нива стойностите са взети от отчетите, предоставени за съответните тестове. Нулевият брой неуспешни заявки се отнася до тези двуминутни изпълнения.

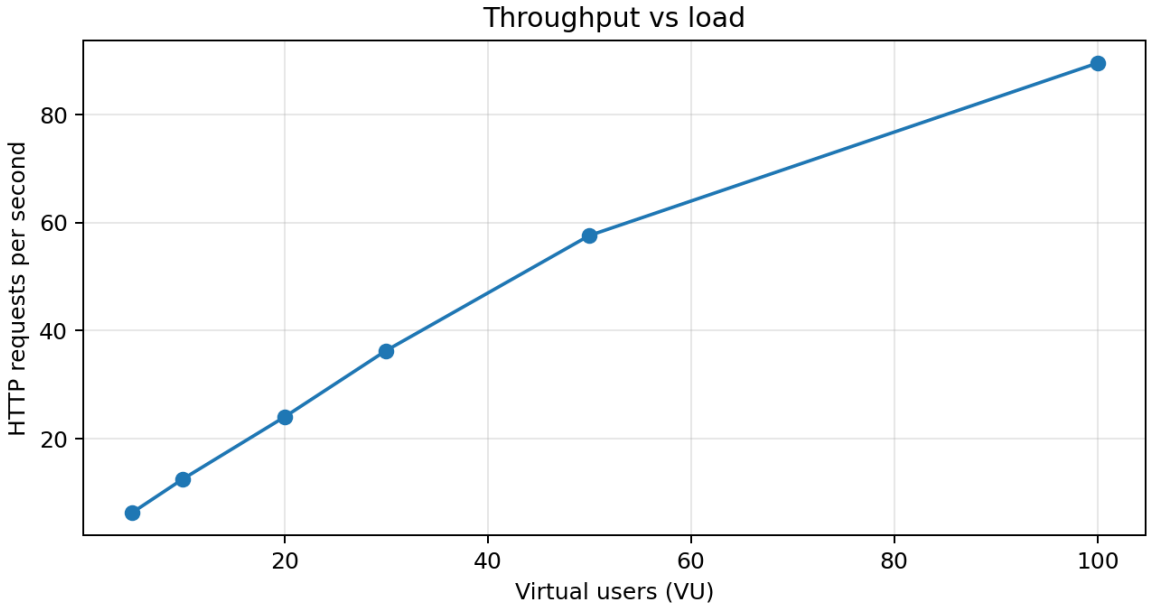
a. Средно време за отговор

При 20 и 30 VU средното време за отговор е близко – съответно 147,08 ms и 148,06 ms. При 50 VU то се увеличава до 186,60 ms, а при 100 VU достига 419,47 ms. Наблюдава се отчетливо нарастване на латентността при най-високото изследвано натоварване. Резултатите не показват линейна зависимост между броя виртуални потребители и времето за отговор.



Фигура 1. Средно време за HTTP отговор при различен брой виртуални потребители.

b. Пропускателна способност



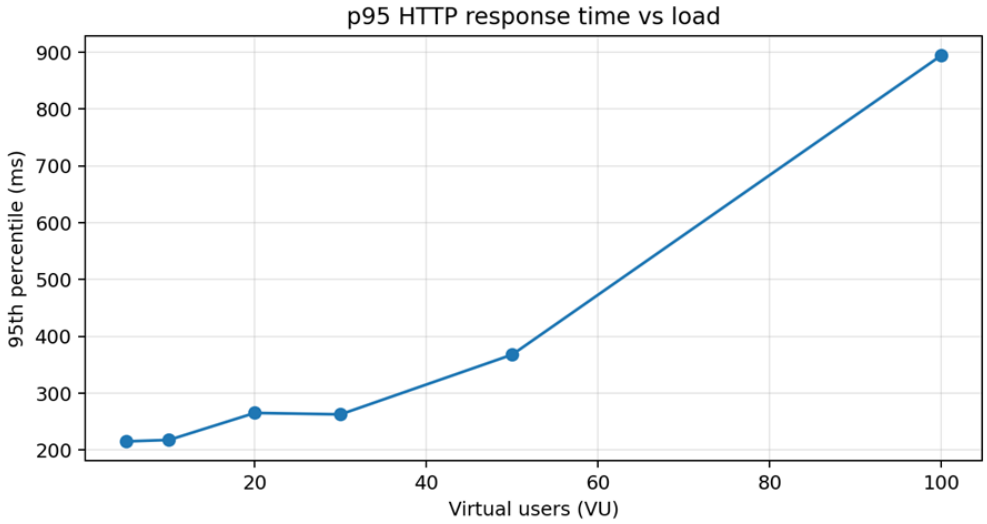
Фигура 2. Пропускателна способност при различен брой виртуални потребители.

Пропускателната способност нараства от приблизително 24,00 заявки/s при 20 VU до 89,52 заявки/s при 100 VU. Увеличението не е пропорционално на удвояването на виртуалните потребители между 50 и 100 VU: броят заявки в секунда нараства от 57,59 до 89,52, докато средното време за отговор се увеличава повече от два пъти. Това е признак за намаляваща ефективност на допълнителното натоварване.

c. Време за отговор на 95% от HTTP заявките

За оценка на времето за отговор при по-бавните HTTP заявки е използван показателят 95-ият процентил (p95). Той показва времето, в рамките на което са приключили 95% от измерените заявки, докато останалите 5% са с по-дълго време за отговор. [2]

При натоварване от 20 виртуални потребители стойността на p95 е 265,24 ms, а при 100 виртуални потребители достига 894,62 ms. Това показва значително нарастване на времето за отговор при по-високо натоварване и означава, че при 100 виртуални потребители 95% от заявките са получили отговор за не повече от приблизително 0,895 секунди.



Фигура 3. Време за отговор на 95% от HTTP заявките при различен брой едновременни потребители.

Както се вижда от фигура 3, увеличаването на броя виртуални потребители е съпроводено с отчетливо повишаване на p95. Резултатът допълва анализа на средното време за отговор, като показва, че при по-високо натоварване се увеличава времето за обслужване на по-бавните заявки. Следователно оценката на производителността не трябва да се основава единствено на средните стойности, а да отчита и разпределението на времената за отговор.

d. Резултати за отделните операции.

Таблица 3

Натоварване	Операция	Средно време (ms)	p95 (ms)	Максимум (ms)
20 VU	Списък	165.40	268.67	519.68
20 VU	Търсене	168.11	282.40	555.38
20 VU	Втора страница	177.94	271.95	468.52
50 VU	Списък	192.03	310.95	740.90
50 VU	Търсене	205.21	346.48	1344.11
50 VU	Втора страница	213.69	386.35	964.80
100 VU	Списък	452.28	845.42	1587.27
100 VU	Търсене	412.41	795.61	1770.92
100 VU	Втора страница	434.73	867.36	2341.63

При 20 VU разликите между трите измервани операции са малки. При 100 VU средните времена за всички операции са над 400 ms, като най-високо средно време е измерено при списъка с докторанти. Тези стойности характеризират HTTP операциите като част от сценария и включват мрежовото взаимодействие, а не само времето за изпълнение на заявката към базата данни.

6 Анализ и обсъждане

Основната тенденция е нарастване на времето за реакция с увеличаването на броя виртуални потребители. При 20–30 VU средните времена остават близки, докато при 50 VU се наблюдава умерено увеличение, а при 100 VU – значително повишение. Същевременно пропускателната способност продължава да нараства, но не пропорционално на натоварването. Това предполага, че допълнителните конкурентни заявки увеличават времето за обслужване и/или чакане.

Наблюдението на сървъра чрез top по време на теста със 100 VU показва периодични пикове в натоварването. В моментната снимка процесите PHP-FPM използват значителен дял от CPU, а свободният CPU е отчетен като 0%. Наличната RAM в същия момент е приблизително 357 MiB, а около 563,5 MiB swap са използвани. По време на наблюдението високите стойности се появяват през интервали от няколко секунди и са последвани от периоди с по-ниско натоварване. Това е съвместимо със сценарий, при който множество виртуални потребители изпълняват последователни заявки с паузи между действията.

Тези наблюдения насочват към PHP обработката и наличните ресурси като области, които заслужават допълнително профилиране. Те обаче не доказват, че PHP е единственото ограничение. За да се определи конкретната причина, биха били необходими непрекъснати измервания на CPU, RAM, swap, дискова активност, Apache/PHP-FPM опашки и време за изпълнение на SQL заявките.

При двуминутните тестове с 5, 10, 20, 30, 50 и 100 VU всички функционални проверки са успешни и не са отчетени неуспешни HTTP заявки. Това показва, че приложението е изпълнило проверяваните операции успешно в рамките на тези тестове. При отделния петминутен тест със 100 VU е имало една неуспешна HTTP заявка и една неуспешна проверка; при повторния двуминутен тест със 100 VU такива не са отчетени. Наличните данни не позволяват да се определи еднозначно причината за единичния неуспех.

Ограничение на изследването е, че сценарият включва удостоверяване при всяка итерация, както и няколко различни страници и паузи. Следователно отчетените req/s и времена описват целия сценарий, а не изолирана операция. Освен това базата данни съдържа 500 синтетични профила; резултатите не са директно обобщими за бази с десетки хиляди записи, различни заявки или различна сървърна конфигурация.

7 Заключение

В доклада е проведено експериментално изследване на времето за реакция и пропускателната способност на WEB базираната информационна система „Докторант“ при различен брой виртуални потребители. Използван е k6 за генериране на конкурентно натоварване, като тестовият сценарий включва удостоверяване, зареждане на табло, списък с докторанти, търсене и пагинация.

Резултатите показват, че при 20 VU средното HTTP време е 147,08 ms, а при 100 VU достига 419,47 ms. За същите нива пропускателната способност нараства от 24,00 до 89,52 заявки/s, но увеличението е съпроводено със значително нарастване на p95 – от 265,24 до 894,62 ms. Следователно системата обработва повече заявки при по-високо натоварване, но с по-голямо закъснение.

В основните двуминутни тестове не са отчетени неуспешни HTTP заявки и всички функционални проверки са преминали успешно. Наблюдението на сървърните ресурси при 100 VU показва периодични пикове на процесорно натоварване и ограничен резерв от свободна памет. Тези данни дават основание да се препоръча последващо профилиране на PHP-FPM и SQL операциите, както и непрекъснато събиране на системни метрики при бъдещи тестове.

Целта на изследването е постигната в рамките на зададените условия: получени са измерими резултати за времето за реакция, p95 и пропускателната способност при няколко нива на конкурентно натоварване. Като бъдеща работа се предвиждат тестове с по-голям набор от данни, отделни сценарии за конкретни операции и по-подробно събиране на сървърни показатели, които да позволят локализиране на причините за забавяне.

ЛИТЕРАТУРА:

[1] Grafana Labs. k6 documentation: https://grafana.com/docs/k6/latest/ (дата на достъп: 12.10.2026).

[2] Grafana Labs. k6 metrics reference: https://grafana.com/docs/k6/latest/using-k6/metrics/ (дата на достъп: 12.10.2026).

[3] Apache Software Foundation. Apache HTTP Server Documentation: https://httpd.apache.org/docs/ (дата на достъп: 12.10.2026).

[4] PHP Group. PHP Manual: https://www.php.net/manual/en/ (дата на достъп: 12.10.2026).

[5] MariaDB Foundation. MariaDB Server Documentation: https://mariadb.com/kb/en/ (дата на достъп: 12.10.2026).

[6] Grafana Labs. k6 scenarios and virtual users: https://grafana.com/docs/k6/latest/using-k6/scenarios/ (дата на достъп: 12.10.2026).

COMPARATIVE DESIGN OF AN AUTOMATED LINE FOR RECYCLING ALUMINIUM CANS*

DIYAN V. MARKOV, TSVETOSLAV S. TSANKOV

ABSTRACT: *Three design configurations for recycling aluminium cans are compared through process structure, material flow and automation requirements. The selected route is extended with buffer management, inter-module transfer conditions, failure responses and verification scenarios. A conditional batch calculation is distinguished from the capacity of a pipeline with overlapping operations. Parametric scenarios illustrate the influence of metal recovery and operating availability without claiming measured performance. Technical and economic evaluation uses consistent product quality and system boundaries. The contribution is a project-specific framework connecting process selection, control logic and measurable validation criteria.*

KEYWORDS: *aluminium recycling, automated line, material flow, buffer management, capacity, failure analysis*

DOI: https://doi.org/10.46687/MT26DVM

СРАВНИТЕЛНО ПРОЕКТИРАНЕ НА АВТОМАТИЗИРАНА ЛИНИЯ ЗА РЕЦИКЛИРАНЕ НА АЛУМИНИЕВИ КЕНОВЕ

ДИЯН В. МАРКОВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Сравнени са три проектни конфигурации за рециклиране на алуминиеви кенове чрез технологичната структура, материалния поток и изискванията към автоматизацията. Предпочетеният вариант е доразвит с управление на буферите, условия за предаване между модулите, реакции при отказ и изпитвателни сценарии. Разграничени са условният партиден разчет и капацитетът при припокриващи се операции. Параметрични сценарии показват влиянието на извличането и работната наличност, без да се заявява измерена производителност. Техническата и икономическата оценка използват еднакво качество на продукцията и граници на системата. Приносът е съгласуване на технологичния избор, управляващата логика и критериите за проверка в конкретния проект.*

1 Въведение

Алуминиевите опаковки представляват вторична суровина, която може да се включи отново в производствения цикъл след събиране, сортиране, подготовка и претопяване. Рециклирането изисква контрол върху примесите и технологичните загуби, тъй като количеството приет скрап не е равно на количеството получен метал [2].

При проектиране на автоматизирана линия основната задача е да се свържат отделните операции в съгласуван материален поток. Раздробяването, отстраняването на покрития и топенето имат различни времена и условия на работа. Недостатъчният капацитет на една операция може да ограничи цялата линия независимо от производителността на останалите модули.

Целта е да се сравнят трите конфигурации от [1] и да се доразвие предпочетеният вариант чрез материален разчет, правила за транспорт и буфериране, реакции при отказ и методика за оценка. Анализът е проектен. Изчислените сценарии показват зависимости

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие MATTEX 2026 – ФТН“

между параметрите; ефективността на подготовката, качеството на метала и действителният капацитет изискват измервания.

2 Функционална структура на линията

Входната суровина е пресован скрап от алуминиеви кенове. Проектната последователност включва подаване на балите, грубо дробене, подготовка на повърхността, отделяне на неалуминиеви компоненти, фино дробене, топене и формоване. Конвейерите свързват технологичните единици, а междинните буфери ограничават зависимостта между операции с различна продължителност.



Фиг. 1. Обобщена последователност на материалния поток

Отстраняването на органични покрития е част от подготовката на скрапа за претопяване и се разглежда в технологичните описания на рециклирането [3]. Изборът на конкретно оборудване зависи от състава на суровината, необходимото качество и условията за отвеждане на образуваните газове или отпадъчни потоци. В настоящия модел тази операция се описва функционално, без да се задават непотвърдени режими на обработка.

Управлението съгласува готовността на подаващия и приемния модул. Нов материал не се подава при блокировка на дробилката или запълнен следващ буфер. Транспортът към топенето се разрешава след потвърждение на подготовката и готовност за приемане. Предаването се потвърждава от датчици и технологични сигнали, вместо да се приема за успешно само по изминало време.

3 Приемане и проследимост на суровината

Входният поток се организира по партиди с идентификатор, доставчик, маса и резултат от приемния контрол. Дялът на алуминия се задава на определена масова основа, а влагата и примесите се отчитат отделно. При несъответствие партидата се задържа за проверка. Разпределянето на суровината по качество намалява неопределеността на разчетите и позволява загубите да се съпоставят с конкретна доставка.

Проследимостта продължава през буферите и крайния продукт. При смесване се записват участващите партиди и маси; без такъв запис не може еднозначно да се отнесе крайният добив към един доставчик. Отделените примеси и остатъци също се измерват и обозначават. Организацията на обратния поток включва приемане, подготовка, реализация на получения метал и управление на остатъчните потоци.

4 Сравнение на технологичните варианти

Първият вариант използва термично отстраняване на покритията след грубо раздробяване. Вторият включва химическа обработка и оптично сортиране. Третият

разширява механичната подготовка и броя на операциите по почистване [1]. Различията създават отделни изисквания към междинното съхранение, обслужването и управлението на отпадъчните потоци.

Таблица 1. Структурно сравнение на трите проектни варианта

Критерий	Вариант 1	Вариант 2	Вариант 3
Отстраняване на покрития	Термична обработка	Химическа обработка	Многоетапна обработка
Механична подготовка	Грубо и фино дробене	Дробене между основните операции	Допълнителен етап на дробене
Сортиране	Отделяне на примеси	Оптично сортиране	Оптично сортиране
Специфичен контрол	Топлинен режим и газоотвеждане	Вани, изплакване и отпадъчни води	Повече междинни преходи
Проектна сложност	По-кратка последователност	Допълнителни обработващи модули	Най-разгърната последователност

Структурното сравнение не доказва по-висока чистота или по-ниски разходи. За това са необходими измервания на остатъчните покрития, определяне на химичния състав и оценка на металните загуби и енергийните разходи. Първият вариант е предпочетен за детайлно разглеждане поради по-кратката последователност; това е проектен приоритет, а не доказана оптималност. Химическата и многоетапната обработка остават алтернативи, чиито режими и приложимост трябва да се потвърдят за конкретния скрап.

Изборът преминава през две проверки. Първо се установява дали вариантът изпълнява изискванията към качеството, оборудването и спомагателните системи. Едва след това допустимите варианти се сравняват по капацитет, разход на ресурси, ремонтопригодност и общи разходи. По-кратката линия не компенсира неприемливо качество. За оптичното сортиране се определят класовете на материалите и критериите за разграничаване; самото му наличие не доказва съответствие на крайния химичен състав.

5 Управление на конвейерите и междинните буфери

Всяка технологична единица се описва със състояния „готовност“, „работа“, „задържане“ и „отказ“. Локалният контролер управлява устройството, а координацията определя разрешението за предаване на материал. За връзката между два модула се обменят готовност за приемане, наличие на материал, заявка за предаване, потвърждение и отказ. Неполучено потвърждение в зададения интервал прекратява подаването и изисква проверка на действителното положение на материала.

Горният и долният праг на буфера са различни, за да не възниква често включване и изключване около една стойност. Капацитетът се определя по маса и допустима геометрия на складирания материал. Изменението е $dB/dt = q_{вх} - q_{изх}$, където B е запасът, а потоците са в съпоставими единици. За прекъсване на подаването с продължителност Δt ориентировъчният запас е $B_{необх} = q_{изх} \cdot \Delta t$. Този разчет предполага постоянен поток и се уточнява чрез реалните колебания.

Таблица 2. Условия за координация на материалния поток

Условие	Управляваща реакция	Проверка
Приемният модул е готов	Разрешение за предаване при наличен материал	Потвърдено приемане
Буферът достигне горен праг	Спиране на предходното подаване	Няма препълване
Буферът спадне под долен праг	Заявка за попълване	Съгласувано възобновяване
Приемен модул е в отказ	Блокиране на подаването към него	Задържане в допустим буфер
Загубена комуникация	Отнемане на разрешението за ново предаване	Няма работа по остарял сигнал

Буферът компенсира кратки прекъсвания, но не отстранява траен недостиг на капацитет. Ако предходният модул постоянно подава повече от следващия, запасът нараства до горния праг и подаването трябва да се ограничи. При спиране на линия последователността се съгласува с технологичните модули: прекратяването на транспорта не означава автоматично изключване на охлаждане, вентилация или други спомагателни функции. Условията се определят от конкретното оборудване.

6 Материален баланс и идеален капацитет

За входна бала в [1] са приети 711 kg и алуминиев дял 75%. Съдържащият се алуминий е 533,25 kg преди подготовката и топенето. Останалите 177,75 kg са неалуминиевата част според това допускане. Стойността 75% е входен параметър на проекта; за реална доставка тя се установява чрез представително определяне на състава.

$$m_{Al} = m_{in} \cdot x_{Al} = 711 \cdot 0{,}75 = 533{,}25\,kg$$

В материалния баланс се разграничават входният алуминиев дял и извличането η. В следващата формула mout означава масата на извлечения алуминий в крайния продукт. Тя е произведение на входната маса, алуминиевия дял и η. Общата маса на получена сплав може да е различна и се определя с отчитане на състава и добавките. Без измерено η не може да се заяви действителен добив.

$$m_{out} = m_{in} \cdot x_{Al} \cdot \eta$$

Балансът на алуминия включва всички входящи потоци, включително добавките, ако съдържат алуминий. Общото входящо количество се съпоставя с алуминия в крайния продукт, отделените остатъци и изменението на запасите. Масата на шлаката не се приема изцяло за загубен метал. Пълният материален баланс включва и помощните вещества, газовите и течните потоци; той не се свежда до разлика между скрапа и готовия продукт. Началните и крайните запаси трябва да бъдат съпоставими за избрания интервал.

В дипломната работа за първия вариант е посочено циклово време 988 s, получено като сбор от 870 s машинно време и 118 s спомагателно време [1]. Този разчет обаче не е съгласуван с циклограмата, в която времената на петте технологични операции са 240, 150, 250, 182 и 200 s – общо 1022 s, без допълнителните движения. Поради това стойността 988 s се използва тук единствено като условен разчетен сценарий. При последователни цикли без паузи тя дава приблизително 3,64 бали/h и алуминиев поток преди загубите около 1943 kg/h. Тези стойности не представляват потвърден капацитет на линията; окончателната оценка изисква съгласуване на времената и определяне на допустимото припокриване на операциите.

$$n_b = 3600 / 988 \approx 3{,}64 \text{ партиди}/h$$

Таблица 3. Разчетни показатели при приетите входни условия

Показател	Стойност	Статус
Маса на входна бала	711 kg	Проектно допускане
Дял на алуминия	75%	Проектно допускане
Алуминий преди загубите	533,25 kg/бала	Материален разчет
Прието време за условния последователен цикъл	988 s	Условна стойност от [1]
Идеален брой партиди	3,64/h	Условен разчет при цикъл 988 s
Алуминиев поток преди загубите	1,94 t/h	Условен разчет при цикъл 988 s, без паузи и технологични загуби

Това е условен разчет при последователна обработка. Необходима е циклограма с началото, продължителността и заетостта на всяка операция. Времето от входа до изхода на една бала и интервалът между две завършени бали са различни показатели. При припокриване на операциите сумата на времената не определя директно установената производителност.

7 Капацитет и чувствителност на разчета

За звено i номиналният капацитет е qi = mi / ti, където mi е обработваната маса, а ti – цикловото време. При паралелни еднакви единици капацитетите могат да се сумират само ако подаването и обслужването позволяват едновременна работа. Всички qi се привеждат към една материална основа. Сравняването на kg входен скрап/h с kg готов метал/h без преобразуване би дало погрешно ограничаващо звено.

При съгласувани потоци номиналният капацитет на линията се ограничава от звеното с най-нисък капацитет, определен на съпоставима материална основа. Реалната производителност зависи и от буферите, общите ресурси, престоите и скоростта на работа. Дипломната работа съдържа циклограми и времена на операциите, но те не са съгласувани с обобщените разчети [1]. Затова на този етап не може надеждно да се определи ограничаващото звено. Необходимо е да се уточнят обработваната маса за всяка операция, заетостта на оборудването и възможностите за едновременна работа. Технологичното време, транспортното време и изчакването се отчитат отделно.

За условния последователен сценарий с прието цикълово време 988 s алуминиевият поток преди технологичните загуби е Q_0 = 1943,02 kg/h. Тази стойност е изчислителна основа за анализа на чувствителността, а не потвърдена производителност на линията. Ако η е извличането, а A – делът на плановото време, през което се работи с тази проектна скорост, средният поток е $Q = Q_0 \cdot \eta \cdot A$. Моделът не включва отделно намаляване на скоростта. Когато Q е измерено за целия период и вече съдържа престоите, A не се прилага повторно. Таблица 4 използва избрани параметри само за демонстрация на чувствителността.

Таблица 4. Илюстративни сценарии при условно циклово време 988 s

Извличане η	Дял на работа A	Среден поток Q
0,90	0,80	1 399 kg/h
0,90	0,90	1 574 kg/h
0,95	0,80	1 477 kg/h
0,95	0,90	1 661 kg/h

Сценариите не са резултати от изпитване и не задават типични стойности за алуминиев скрап. При фиксирани останали параметри относителното изменение на η или A води до същото относително изменение на Q. По-високото извличане трябва да се оценява съвместно с необходимите ресурси и качеството. То не е автоматично икономически изгодно, ако допълнителните разходи превишават стойността на получената продукция.

8 Анализ на отказите и възстановяване

Отказите се разглеждат чрез причината, местното последствие и отражението върху следващите модули. Приоритет имат събитията, които могат да доведат до неконтролирано подаване, смесване на непроверена суровина или загуба на потвърждение за технологична готовност. Без експертно оценяване и експлоатационни данни не се присвояват числени вероятности или оценки за риск. Таблица 5 задава проектни реакции и доказателствата за тях.

Таблица 5. Откази и реакции на линията

Отказ	Последствие	Предвидена реакция
Заклинване на конвейер	Задържане и натрупване на материал	Спиране на подаването; проверка на остатъчния товар
Невалиден сигнал за буфер	Риск от препълване или работа без материал	Блокиране на ново предаване; проверка на датчика
Отказ на дробилния модул	Неподготвен материал не може да продължи	Задържане на входа и контрол на следващите запаси
Непотвърдена подготовка	Неопределено качество на партидата	Отделяне за проверка преди следващия етап
Загубена готовност на приемния модул	Прекъсване на предаването	Отнемане на разрешението; технологично съгласувано спиране

Критичен сценарий е подадена заявка за транспорт при липса на реална готовност. Проследяват се валидността на сигнала, разрешението, действителното движение и потвърждението за приемане. Така се различават отказ на датчик, комуникация, задвижване и приемна машина. Повторното пускане изисква проверка на наличния материал и актуални сигнали; нулирането на аларма не е самостоятелна команда за старт. Защитните функции се определят отделно от обичайната координация.

9 Критерии за техническа и икономическа оценка

Вариантите се оценяват при еднаква суровина, качество на продукта, планов фонд време и граници на системата. Капиталовите разходи включват машини, транспорт, буфери, управление и спомагателни инсталации. Експлоатационните обхващат енергия,

консумативи, поддръжка, труд и обработка на остатъците. По-подробната конфигурация може да бъде оправдана, ако изпълнява изискване, което по-краткият вариант не постига.

Годишният обем е Мгод = Qпрод · Нпл, при реализуем продуктов поток Qпрод в t/h и Нпл в h/год. Алуминиевият поток Q от таблица 4 се преобразува към продукт според състава и добавките; той не се приема автоматично за маса на продаваемата сплав. Ако Qпрод включва прекъсванията, фондът не се намалява повторно за тях. Цената на скрапа се прилага към закупената маса. Реализуемите остатъци се отчитат отделно от отпадъците с разход за обработка.

За всяка операция специфичното енергийно потребление е ei = Ei / Мпрод, при едни и същи период и граници на измерване. Отчитат се дробене, подготовка, топене, транспорт и спомагателни системи. Електричеството и горивата се записват отделно; при общ енергиен показател се задава основата за преобразуване. Разходите за подготвителните операции се включват дори когато се извършват извън площадката. Такива граници са съществени и в екологичната оценка [3].

Опростеният годишен паричен ефект е разликата между приходите и текущите парични разходи. Прост срок на откупуване T = I / CF се изчислява само при положителен годишен ефект CF, с изрично посочени допускания; той не отчита промяната на паричните потоци във времето. Тук I е началната инвестиция, а CF – приетият постоянен нетен годишен паричен поток; T се получава в години. В настоящия проект липсват потвърдени цени и разходи, затова не се заявява числен срок. Чувствителността се проверява към η, A, цените на суровината и продукта, енергията и обслужването.

10 Методика за проверка на проектното решение

Проверката има три части. Модел на последователността изпитва сигналите, буферите и режимите. Стендовата проверка установява времената и поведението на конкретните устройства. Технологичните опити определят подготовката, металния добив, качеството и ресурсите. Триизмерна симулация на транспорта може да подпомогне първата част, но не валидира самостоятелно химическата обработка или топенето.

Таблица 6. Сценарии и критерии за проверка

Сценарий	Критерий
Нормален поток	Всяко предаване е потвърдено и проследимо
Запълнен буфер	Подаването се прекратява преди препълване
Отказ на приемна машина	Няма нов материал към недостъпния модул
Прекъсната комуникация	Разрешението не остава активно по остарели данни
Възстановяване след отказ	Пускане само след проверка на товара и готовността
Технологичен опит	Измерени състав, извличане, остатъци и енергия

За всеки опит се записват конфигурацията, началните запаси, масата и съставът на суровината, входните събития, времената и действителните реакции. Капацитетът се измерва след отделно обозначен начален период и при известни запаси в края. Изчакванията се разграничават от престоите по отказ. Повторенията трябва да обхванат повече от една партида, за да се види влиянието на входните колебания. Критериите за качество и приемане се определят преди изпитването.

11 Заключение

Трите конфигурации са сравнени по подготовката и организацията на потока. За предпочетения вариант са съгласувани материалният баланс, буферите, предаването между модулите и реакциите при отказ. Разчетът с 988 s е използван като условен сценарий поради несъответствието между обобщеното циклово време и времената в циклограмата на дипломната работа. Окончателната оценка на капацитета изисква съгласуване на технологичните и спомагателните времена, определяне на капацитетите на отделните звена и допустимото припокриване на операциите. Параметричните сценарии показват влиянието на извличането и престоя, а методиката задава измеримите данни за окончателен технически и икономически избор.

ЛИТЕРАТУРА:

[1] Марков, Д. В. Проектиране на автоматизирана линия за рециклиране на алуминиеви кенове. Дипломна работа, Шуменски университет „Епископ Константин Преславски“, 2026.

[2] European Aluminium. Recycling. https://european-aluminium.eu/projets/recycling/ (достъп: 12.10.2026).

[3] European Aluminium. Environmental Profile Report 2018. February 2018. https://european-aluminium.eu/wp-content/uploads/2023/01/European-Aluminium_Environmental-Profile-Report-2018_full-version.pdf

PROTOTYPE ARCHITECTURAL MODEL USING A POSITIONAL ALTERNATION CODING MODEL AND VARIABLE LENGTH METACODE*

VALENTIN T. ATANASOV

ABSTRACT: *The coding model considered in this publication is dynamic with intrinsic decodable logic, symmetric, based on a monotonically increasing code length function with a constant unit step. The architecture of the proposed model assumes a conditionally independent prototype of a certain program implementation, which in general makes it applicable in a number of areas.*

KEYWORDS: *compression, decompression, architecture model, monotonic coding scheme*

DOI: https://doi.org/10.46687/MT26VTA

АРХИТЕКТУРЕН МОДЕЛ НА ПРОТОТИП, ИЗПОЛЗВАЩ МОДЕЛ НА КОДИРАНЕ С ПОЗИЦИОННО РЕДУВАНЕ И ПРОМЕНЛИВА ДЪЛЖИНА НА МЕТА КОДА

ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *Разглежданият в настоящата публикация модел за кодиране е динамичен с вътрешно присъща декодируема логика, симетричен, основан на монотонно нарастваща функция на кодовата дължина с постоянна единична стъпка. Архитектурата на предлагания моделът, предполага условно независим прототип от определена програмна реализация, което в общия случай го правим приложим в редица области.*

1 Въведение

Статистически изследвания обобщават информация за общия обем на създадените, обработените и използвани данни в световен мащаб, прогнозно достигащи до 394 зетабайта през 2028 година, сравнявайки ги със 149 зетабайта през 2024 година [1].

Подложен на изследване на IoT трафик в неиндустриална мрежа сочи, че действителният размер на IoT пакети се изменя значително, при това е налице зависимост от протокола и устройството. Но успоредно с тези обстоятелства се отчита, че има ясен дял от малки пакети (50÷400 байта) при трафика в сензорни мрежи или подобни крайни устройства [2].

Подобен клас IoT устройства са склонни да обменят малки количества данни в пакети, от които преобладаващата част са с размер под 250 байта. Този размер е установен чрез анализ на трафика при физически устройства, обстоятелство показващо ясна тенденция към малки размери на пакети при IoT обмен [3]. При друго изследване, проучващо енергийното поведение на IoT устройства, при различни настройки, включващи и обем на обменяните данни, се установява, че енергията за предаване на данните нараства с размера на предадения пакет данни [6],

Един от основните въпроси при обработката на такъв тип данни насочва проблемния анализ към натоварването при операционализацията в обработката на малки IoT JSON

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

данни и влиянието на фактори като натоварване и човешка намеса. Същностната характеристика на въведеното понятие „*операционализация*“ се опира на психофизични характеристики като когнитивен товар на човека в процеса на семантичното възприятие и разбиране на такъв тип данни. Това е ключово характеризиране на качеството „*човекочетими*“. И в допълнение на статистическата информация е установеното доминиране на IoT JSON формата при мрежовия обмен в разглежданите сензорни мрежи.

Тези въпроси определят основната задача при разработката, насочена към синтеза на архитектура на модел за компресия, ориентирана към малки по обем текстови *човекочетими* телеметрични данни, представени в JSON формат и използвани при IoT приложенията.

Преди да се пристъпи към архитектурното моделиране следва да се разгледат основните характеристики на методите за компресия, определящи ключови области от показатели. Тези показатели могат да бъдат обобщени и изведени като:

- *Степен на компресия;*
- *Наличие на загуба;*
- *Време на компресиране;*
- *Време на декомпресиране;*
- *Обратимост;*
- *Хибридност;*
- *Области на приложимост;*
- *Основаване на споделено познание;*
- *Използване на ресурси;*
- *Баланс между размер и качество*.

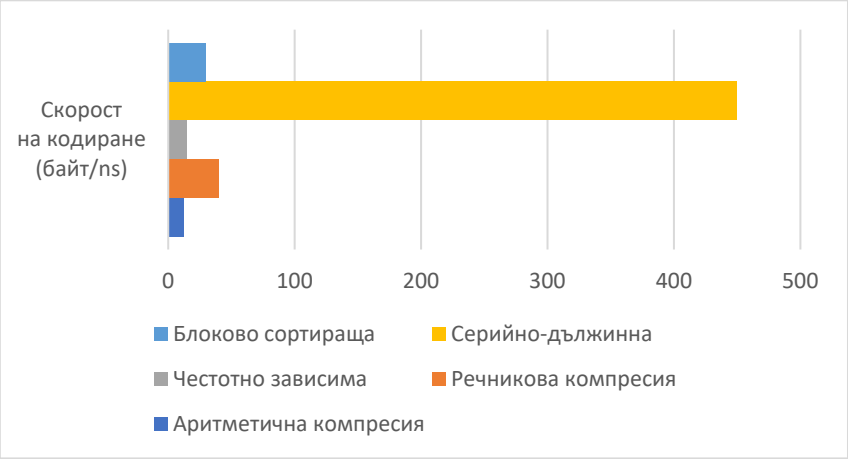
Представените по-горе показатели очертават областта от тях, която има съществено значение за разглеждания в настоящото изследване архитектурен модел на компресия. Важен аспект при използването и избора на метод за компресия на данни без загуба е влиянието на даден алгоритъм за компресия върху системата, в която физически се реализира изпраният процес на компресиране.

Архитектурата на модела следва да отчита възможните влияния на редица фактори върху процеса на компресия/декомпресия. За разбирането на такова влияние е направено обобщение, представящо влиянието на известни методи за компресия върху определени системни фактори, изложени в таблица 1 и фигури 1, 2 и 3 [4][5].

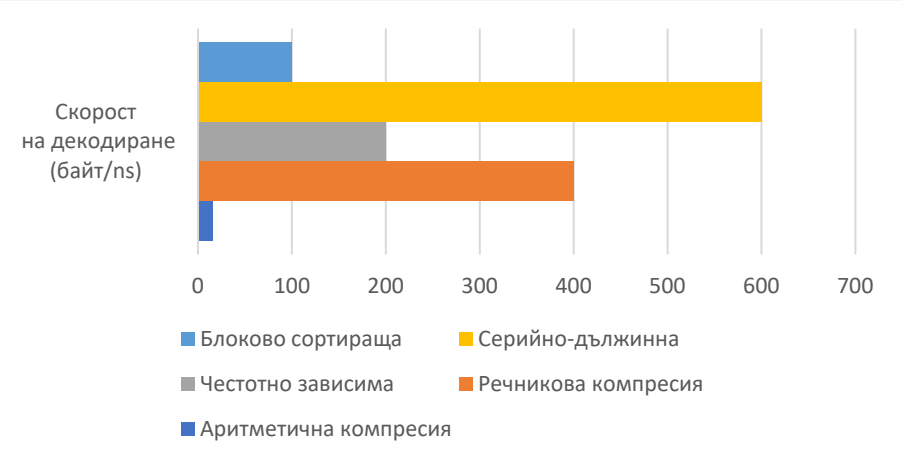
Таблица 1. Зависимост на методите за компресия от системни фактори

Компресия	Процесорно натоварване	Зависимост от апаратната част	Зависимост от програмната част
Честотно зависима	*Умерено към ниско*	*Много ниска*	*Средна*
Речникова	*Асиметрично (Високо при кодиране / Ниско при декодиране)*	*Висока (Критична към паметта)*	*Висока*
Серийно-дължинна	*Нищожно (Минимално)*	*Нулева*	*Минимална*
Аритметична	*Изключително високо*	*Средна към висока*	*Изключително висока*
Блоково сортираща (BWT)	*Симетрично умерено*	*Висока*	*Висока*

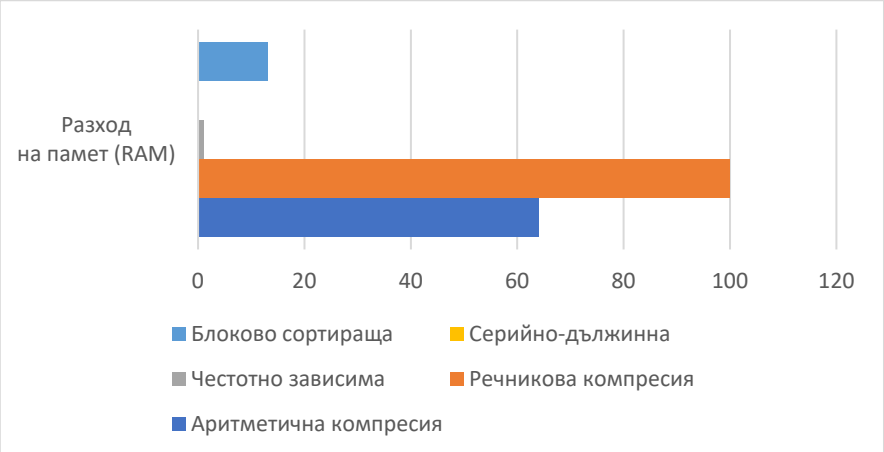
От показаните диаграми на фигури 1, 2 и 3, представящи емпирични резултати, недвусмислено могат да се потвърдят направените в горната таблица 1 заключения.



Фиг. 1. Влияние на основни методи за компресия върху фактор *скорост на кодиране*



Фиг. 2. Влияние на основни методи за компресия върху фактор *скорост на декодиране*

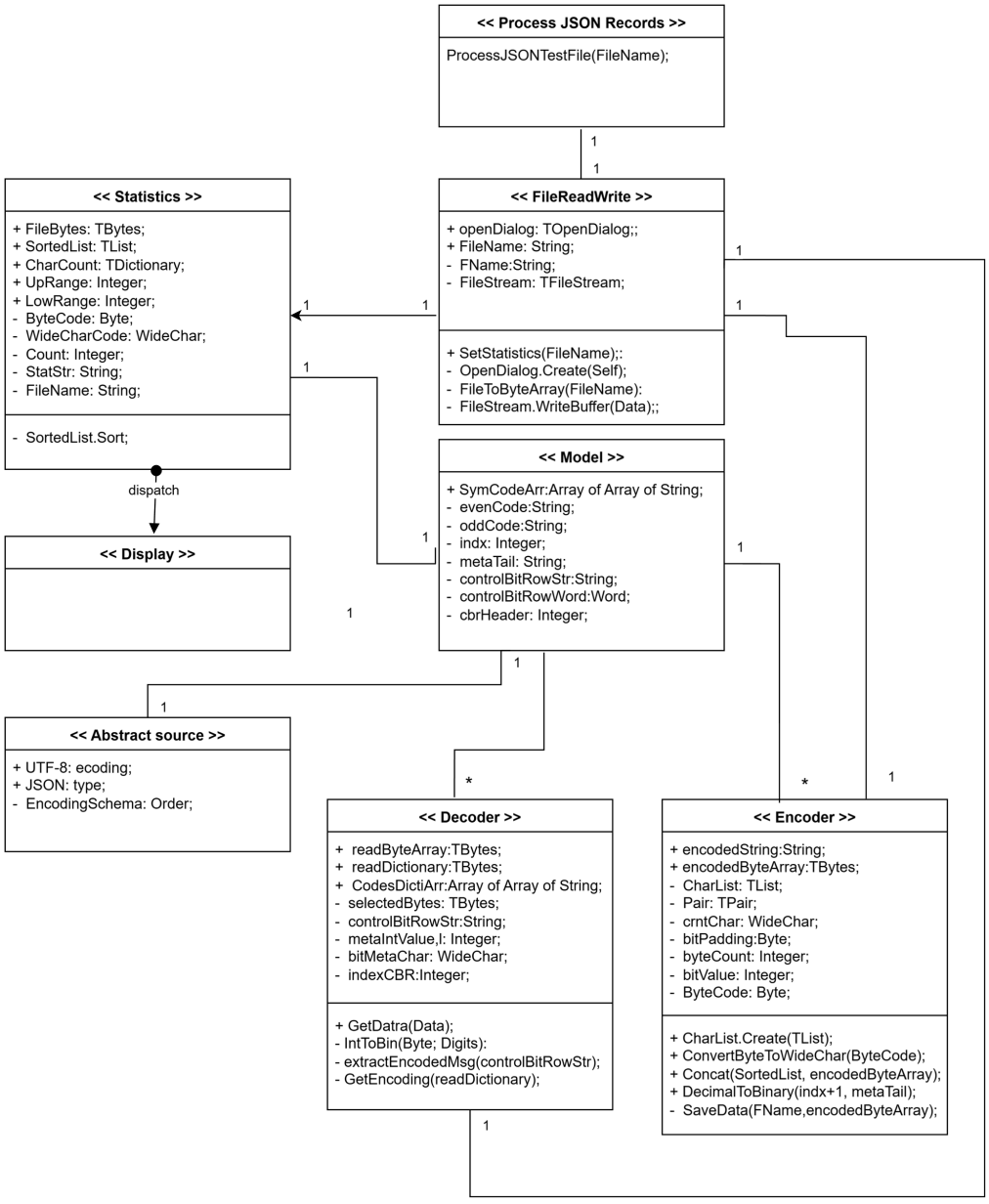


Фиг. 3. Влияние на основни методи за компресия върху фактор *обем заета оперативна памет*

2 Архитектура на прототипа, използващ модел на кодиране с позиционно редуване и променлива дължина на мета кода

Моделирането на прототип, използващ модел на кодиране с позиционно редуване и променлива дължина на мета кода, преминава през изграждането на статична структура, представяща взаимовръзките на основните логически блокове на този прототип.

Такава статична структура се описва от архитектурно построение, представящо основните ù програмни елементи - полета, типове данни, в това число и дефинираните методи за обработка. Предлаганата архитектура на модел за компресия е етап от разработването на прототип, използващ кодиране с позиционно редуване и променлива дължина на мета кода (Фиг. 4).



Фиг. 4. Архитектура на прототип, използващ модел на кодиране с позиционно редуване и променлива дължина на мета кода

Разглежданата архитектура на гореспоменатия прототип отразява известни програмни постановки и характеристики, които определят използването на силно типизиран език за програмиране. Това обстоятелство намира своето обяснение в наложеното изискване за допустимост на експериментите с разработвания прототип, използващ модел на кодиране с позиционно редуване и променлива дължина на мета кода, в известни операционни системи, в чиято функционалност е файловата обработка, тъй като предмет на модела са именно файлови единици. И в допълнение следва архитектурата да способства провеждането на експерименти с прототипа, постигащи целта за натрупване на емпирични данни, необходими за последващата статистическа обработка.

Опирайки се горните постановки следва да се отбележи, че архитектурата се описва от характеристиките на нейното предназначение. В този смисъл не се налага нейната пълна независимост от средствата за реализация. И тъй като прототипът трябва да обработва по същество файлове, архитектурата следва да съдържа имплицитно изискване към средата, тоест тя трябва да предоставя устойчив механизъм за обработка на файлове.

3 Заключение

Разглежданата архитектура на прототипа ще способства за постигане на основната цел на планираното експериментално изследване, целящо проверка на ефективността от използването на модела за кодиране с позиционно редуване и променлива дължина на мета кода, реализиран от програмен прототип. За постигането на тази цел се формират показатели, по които ще бъдат изследвани и съпоставимо анализирани представения прототип и три независими алгоритъма за компресия.

Съществена част от планирания експеримент с разработвания прототип е провеждането на 1000 наблюдения, за които експерименталните резултати да бъдат вътрешно консистентни и обобщените им показатели да формират напълно достоверна, методически издържана и изчерпателна оценка, основана върху анализа на тези експериментални резултати.

ЛИТЕРАТУРА:

[1] Martinez, B., Montón, M., Vilajosana, I., Prades, J. D., Modeling Power Consumption for IoT devices, "The Power of Models: Modeling Power Consumption for IoT Devices," in IEEE Sensors Journal, vol. 15, no. 10, 2015, pp. 5777-5789, doi: 10.1109/JSEN.2015.2445094.

[2] Skowron, M., Janicki, A., Mazurczyk, W., Traffic Fingerprinting Attacks on Internet of Things Using Machine Learning, Volume 4, 2019, doi: 10.1109/ACCESS.2020.2969015.

[3] Wang, M., Shi, S., Zhang, X., Han, S., Qian, Ch, LOIS: Low-cost Packet Header Protection for IoT Devices, IoTDI '23: Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation, 2023, pp:354 - 366, doi.org/10.1145/3576842.3582380.

[4] Mahoney, M., Large Text Compression Benchmark, 2026, (https://mattmahoney.net/dc/text.html), (Посетен на 25.06.2026).

[5] Language Modeling is Compression, 2024, (https://github.com/google-deepmind/language_modeling_is_compression), (Посетен на 25.06.2026).

[6] Baena, E., Yang, H., Koutsonikolas, D., Haqu, I., A Comprehensive Survey on Smart Home IoT Fingerprinting: From Detection to Prevention and Practical Deployment, 2025, (https://arxiv.org/html/2510.09700v1), (Посетен на 06.05.2026).

SEGMENTATION AND INTEGRATION OF IP SYSTEMS IN A PRODUCTION NETWORK*

AYKUT A. REMZIEV, TSVETOSLAV S. TSANKOV

ABSTRACT: *The paper presents a segmented architecture integrating office and production systems, IP telephony, video surveillance and access control. Seven logical segments and an industrial demilitarized zone define the communication boundaries. Service-specific traffic policies are combined with a verification procedure for permitted communication, isolation, concurrent load and link failure. Application response time, packet loss, link utilization and service recovery time provide measurable evaluation criteria. The contribution is a project-specific framework connecting network zones, access rules and acceptance tests. Quantitative validation requires subsequent testing.*

KEYWORDS: *IT/OT integration, VLAN, industrial DMZ, traffic management, network verification*

DOI: https://doi.org/10.46687/MT26AAR

СЕГМЕНТИРАНЕ И ИНТЕГРАЦИЯ НА IP СИСТЕМИ В МРЕЖА НА ПРОИЗВОДСТВЕН ОБЕКТ

АЙКУТ А. РЕМЗИЕВ, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Представена е сегментирана архитектура за интегриране на офисни и производствени системи, IP телефония, видеонаблюдение и контрол на достъпа. Седем логически сегмента и индустриална демилитаризирана зона определят комуникационните граници. Политиките за трафика са свързани с методика за проверка на разрешения обмен, изолацията, едновременното натоварване и отказите на връзки. Определени са показатели за приложен отговор, загуба на пакети, използване на връзките и възстановяване на услугите. Приносът е съгласуване на зоните, правилата за достъп и приемателните изпитвания в конкретния проект. Количествената оценка изисква последващи измервания.*

1 Въведение

Обединяването на компютърни и IP-базирани системи в производствен обект създава обща комуникационна среда за административни задачи, управление на оборудване и наблюдение. Изискванията към отделните услуги обаче се различават. Офисните приложения допускат променливо натоварване, докато производствените системи зависят от непрекъснатостта на обмена между контролери, операторски панели и надзорни станции.

Когато всички устройства принадлежат към една мрежова зона, отказ или неправомерен достъп в административния сегмент може да засегне производството. Затова архитектурата трябва да определя кои системи могат да комуникират, през какви контролни точки преминава обменът и как се проверява работата на ограниченията. NIST разглежда сегментацията и контролираните връзки като средства за защита на оперативните технологии при съобразяване с техните специфични изисквания [3].

Целта на доклада е да представи проект на сегментирана производствена мрежа и методика за проверка на интегрираните IP услуги. Разработката конкретизира инженерния

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

модел в [1] чрез адресен план, комуникационни граници, политика за трафика и изпитвателни сценарии. За всяка услуга се свързват три проектни решения: допустимият маршрут, условията за обслужване и доказателството за правилна работа.

2 Изходни данни и проектни изисквания

Проектният обект включва три производствени халета и административна сграда с обща площ приблизително 12 000 m². Входните данни са подбрани за модел на средно предприятие със 150 служители. Предвидени са 25 работни станции, 5 IP телефона, 10 IP камери, 2 безжични точки за достъп, 3 сървъра и 5 програмируеми логически контролера [1]. Тези количества определят мащаба на проекта и не представляват резултат от натоварващо изпитване.

Основните изисквания са логическо отделяне на производството, поддържане на IP услуги в обща физическа инфраструктура, ограничен административен достъп и възможност за разширяване. За магистралната свързаност е заложен капацитет 10 Gbit/s, а изискването за наличност е минимум 99,9%. Това са целеви параметри, чието постигане трябва да се установи с отделни измервания.

3 Сегментация и адресен план

Мрежата е организирана йерархично чрез ядро, разпределителен слой и слой за достъп. Изграждането на информационна мрежа с Network Notepad е разгледано в [2]. VLAN сегментацията обособява устройствата по функционално предназначение. Частните адресни диапазони са избрани според RFC 1918 [4], като всяка зона използва самостоятелна подмрежа. Таблица 1 представя проектното разпределение.

Таблица 1. Логически сегменти на производствената мрежа

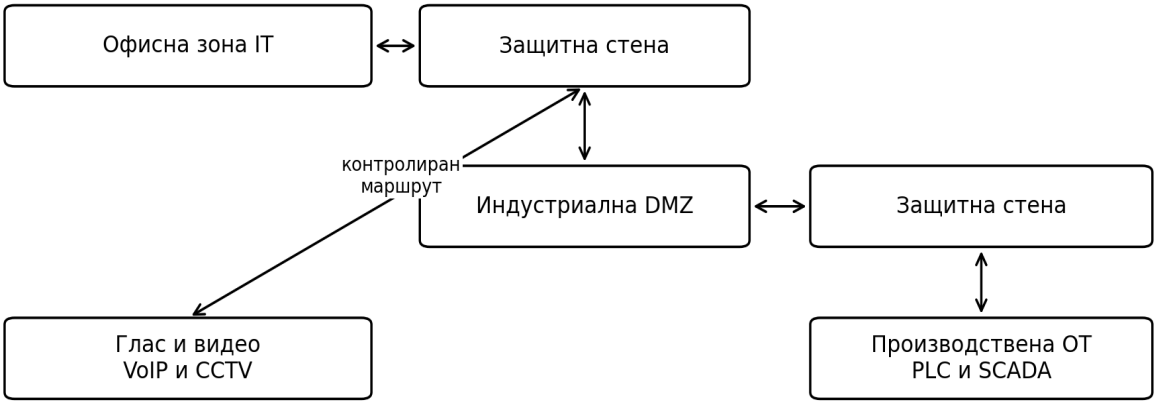
Зона	VLAN	Подмрежа	Устройства
Офисна IT	10	192.168.10.0/24	Работни станции и принтери
Производствена OT	20	10.20.0.0/24	PLC, HMI и SCADA
Индустриална DMZ	30	172.16.30.0/24	Посреднически и архивни услуги
IP телефония	40	192.168.40.0/24	IP телефони и IP-PBX
Физическа сигурност	50	10.50.0.0/24	Камери, видеорекордер и контрол на достъпа
Гостенски достъп	99	192.168.99.0/24	Гостенски безжични устройства
Управление	100	192.168.100.0/24	Мрежово оборудване

VLAN отделя широковещателните домейни, но сам по себе си не определя пълната политика за сигурност. Междусегментният обмен се разрешава само чрез зададени правила на защитните стени и списъци за контрол на достъпа. Управленските интерфейси се достъпват от определена административна станция във VLAN 100. Гостенската зона получава само предвидените външни услуги; достъпът към останалите вътрешни зони се забранява и при наличие на маршрут.

4 Интеграция на IT и OT системите

Индустриалната демилитаризирана зона (IDMZ) служи като посредник между административната и производствената среда. Вместо свободен двупосочен достъп до PLC

и SCADA се разрешават конкретни услуги през контролирани интерфейси. Фигура 1 показва функционалните граници; тя не заменя подробната физическа топология.



Фиг. 1. Функционално разделяне на IT и OT средата

В IDMZ се предвиждат отчетна услуга и посредник за контролиран технически достъп. Производствени данни се подават към отчетната услуга чрез определена надзорна станция в OT зоната; офисните клиенти четат отчетите от IDMZ, без непосредствена сесия към PLC. Техническият достъп преминава през удостоверен посредник и се разрешава за конкретен получател и период. За всяка връзка се записват източник, получател, посока на установяване на сесията, протокол, порт и основание за разрешаване. Отговорите по разрешени сесии се разграничават от правото да се започва нова връзка в обратната посока.

IP телефонията и видеонаблюдението използват отделни логически зони. Гласовият трафик зависи от закъснението и неговото изменение, докато видеопотоците създават продължително натоварване [5]. В настоящия вариант контролът на достъпа се включва във VLAN 50, преименуван на зона за системи за физическа сигурност. Контролерите комуникират само със съответния сървър, а камерите – с видеорекордера. Тъй като VLAN не ограничава автоматично обмена в една подмрежа, разделянето между тези устройства изисква изолация на портове или поддържан еквивалентен механизъм. Ако оборудването не го осигурява, контролът на достъпа се отделя в допълнителен VLAN.

5 Управление на трафика и мрежовите ресурси

Изборът на управляеми комутатори се обвързва с необходимите функции: VLAN, контрол на достъпа, обслужване по класове, статистика на портовете и огледално копиране на трафика за диагностика. Маркирането на пакети се приема само от определени доверени устройства или се задава на входа на мрежата. Така приоритетът не зависи единствено от маркировка, поставена от произволен клиент.

Проектната политика отделя цикличния обмен PLC–HMI/SCADA от архивиране, прехвърляне на файлове и видео. За производствения обмен се задава допустим срок според технологичния процес, а за гласовия трафик – отделен клас на обслужване. Видеопотоците и архивните задачи се ограничават така, че да не изчерпват ресурса на общата връзка. Редът и ресурсите на опашките се определят след оценка на натоварването; общото означение „OT трафик“ не е достатъчно, за да получат всички производствени пакети най-висок приоритет.

Капацитетът се оценява за всяка обща връзка по сумата от едновременно преминаващите потоци, служебния обмен и резерва за краткотрайни пикове. Особено внимание изискват връзките към видеорекордера и IDMZ. Магистрала 10 Gbit/s не премахва ограниченията на по-бавен порт, защитна стена или сървър. При отпадане на основен път оценката се повтаря за резервния, който може да поеме трафика на повече сегменти.

6 Методика за функционална и количествена проверка

Проверката се организира в три етапа: конфигурационна проверка, изпитване на разрешения и забранения обмен и измерване при натоварване и отказ. Успешен ICMP отговор потвърждава достижимост, но не доказва работата на приложната услуга. За всеки сценарий се изпълнява действителна заявка или поток и резултатът се съпоставя с правилата и журналите на устройствата. Забранена връзка се проверява към действително работеща услуга, за да не бъде объркан отказът на защитната стена с неработещ получател.

Таблица 2. Сценарии и критерии за функционална оценка

Сценарий	Очаквано поведение	Критерий
Офисна станция към отчетна услуга в DMZ	Разрешен приложен обмен	Достъп само до зададената услуга
Офисна станция директно към PLC	Забранена връзка	Отказ и запис в защитната стена
Гостенски клиент към вътрешни зони	Забранена връзка	Няма вътрешен достъп
Камера към видеорекордер	Разрешен видеопоток	Запис и възпроизвеждане
Административна станция във VLAN 100 към оборудване	Разрешен управленски достъп	Удостоверена сесия; отказ от други зони
Отпадане на основна връзка	Преминаване към резервен път	Измерено прекъсване и възстановяване
Контролер за достъп към сървъра	Разрешен обмен на събития	Получено събитие; отказ към несвързани устройства
ОТ обмен при едновременни видео и офисни потоци	Продължава приложният обмен	Време на отговор и загуби спрямо предварително зададени граници

Конфигурационната проверка може да се подпомогне с Cisco Packet Tracer за адресиране, VLAN и поддържаните правила за достъп. Поведението на производствените протоколи и реалните времена се изпитват в отделен стенд с представителни устройства и приложения. Wireshark се използва за наблюдение през огледален порт или подходяща точка за прихващане. Посочват се местоположението и посоката на наблюдение, тъй като един запис не обхваща непременно целия обмен, а претоварването на огледалния порт може да доведе до липсващи пакети в самия запис.

Количествената проверка сравнява обичайно натоварване, едновременна работа на услугите и отпаднала основна връзка. При сравнение на политики за обслужване се запазват

конфигурацията, броят на потоците, размерите на заявките и продължителността на опитите. Режимите се повтарят, а резултатите се представят по услуги.

Времето на приложен отговор е разликата между изпращане на заявката и получаване на съответния отговор в една точка на наблюдение. Отчитат се медианата и 95-ият персентил. Показателят включва обработката в получателя. Еднопосочното мрежово закъснение изисква наблюдение в двата края със синхронизирани часовници; интервалът между последователно пристигнали пакети не е измерване на това закъснение.

Делът на загубите се оценява като $L = (N_{изп} - N_{пол}) / N_{изп} \times 100\%$, където броячите се отнасят до един и същ поток и интервал, а $N_{изп} > 0$. За UDP са необходими последователни номера или съпоставими броячи в двата края; TCP повторенията се отчитат отделно. Средната скорост за наблюдавана посока се изчислява като $R = 8B / \Delta t$, където B е броят на отчетените байтове, а Δt е интервалът в секунди. Използването на връзката е $U = R / C \times 100\%$, при еднакви единици за R и капацитета C и изрично посочено ниво на отчитане на байтовете.

Времето за възстановяване се измерва от предизвикания отказ до устойчивото възобновяване на услугата, определено предварително чрез последователни успешни приложни цикли за зададен период. При камерите се проверява записът, при телефонията – активният разговор, а при ОТ – валидните данни в допустимия срок. Отделните услуги могат да имат различни времена при един мрежов отказ.

За възпроизводимост се записват версиите и конфигурациите, приложните протоколи, точките на наблюдение, броят и параметрите на потоците, продължителността и повторенията. Допустимите граници се задават преди опитите според изискванията на процеса и използваните приложения. Целевата наличност 99,9% се оценява за определена услуга и период чрез $A = (T_{набл} - T_{прек}) / T_{набл} \times 100\%$; правилата за отчитане на планираните прекъсвания се посочват изрично.

7 Обсъждане и ограничения

Резултатът е проектен модел, който свързва седем мрежови зони с правила за достъп, обслужване на трафика и приложни проверки. Изолацията между IT и OT се оценява чрез забранените сесии, а интеграцията – чрез разрешената отчетна услуга в IDMZ. Това позволява открита грешка да се отнесе към адресиране, правило за достъп, недостиг на ресурс или отказ на приложение.

Методиката разглежда поотделно достижимостта, качеството на обмена и наличността. По-бърз приложен отговор не доказва по-висока дългосрочна надеждност; успешното превключване при един отказ не доказва изпълнение на годишна наличност. Резервирането на връзки не отстранява общ отказ на захранване, единствена защитна стена или приложен сървър. Преди внедряване се проверяват тези общи зависимости и ограниченията на конкретното оборудване. Докладът не представя проведено натоварващо изпитване, а проект и възпроизводим план за неговата оценка.

8 Заключение

Разработената архитектура интегрира офисни, производствени и IP услуги чрез функционални VLAN зони и индустриална демилитаризирана зона. Доработката свързва адресния план с разрешените приложни потоци, управлението на общите ресурси и критериите за проверка при натоварване и отказ. Така проектът дава конкретна основа за приемателни изпитвания. Изпълнението на целевите показатели за капацитет, време на отговор и наличност следва да се установи с измервания в представителна среда.

ЛИТЕРАТУРА:

[1] Ремзиев, А. А. Интегриране на компютърни и IP-базирани системи в мрежова среда на производствен обект. Дипломна работа, Шуменски университет „Епископ Константин Преславски“, 2026.

[2] Казаков Ст. Изграждане на информационна мрежа с Network Notepad. MATTEX 2024, сборник доклади, т. 2, Шумен, 2024, с. 94–102. ISSN 1314-3921.

[3] Stouffer, K. et al. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3, 2023. DOI: 10.6028/NIST.SP.800-82r3.

[4] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E. Address Allocation for Private Internets. RFC 1918, 1996. DOI: 10.17487/RFC1918.

[5] Kurose, J. F., Ross, K. W. Computer Networking: A Top-Down Approach. 8th ed., Pearson, 2021.

COMPARATIVE ANALYSIS BETWEEN WI-FI 7 AND OLDER GENERATION SYSTEMS*

NIKOLET G. LYULEDZHIEVA, PETKO M. NALBANTOV

ABSTRACT: *In the context of rapid digitalization, growing data exchange, and the intensive integration of artificial intelligence technologies, cloud services, and high-resolution streaming, the requirements for wireless networks are increasing exponentially. The Wi-Fi 7 standard (IEEE 802.11be) emerges as a technological response to modern challenges regarding ultra-high speed, minimal latency, and reliability in crowded environments. This paper examines the architectural and functional differences between Wi-Fi 7 and previous generations (Wi-Fi 6/6E and Wi-Fi 5), focusing on key innovations such as 320 MHz channels, 4096-QAM modulation, and Multi-Link Operation (MLO). A comprehensive analysis of physical (PHY) and medium access control (MAC) layers, network security, and enterprise deployment scenarios is presented.*

KEYWORDS: *wireless networks, Wi-Fi 7, IEEE 802.11be, latency, throughput, MLO, 4096-QAM, spectral efficiency*

DOI: https://doi.org/10.46687/MT26NGL

СРАВНИТЕЛЕН АНАЛИЗ МЕЖДУ Wi-Fi 7 И СИСТЕМИТЕ ОТ ПО-СТАРО ПОКОЛЕНИЕ

НИКОЛЕТ Г. ЛЮЛЕДЖИЕВА, ПЕТКО М. НАЛБАНТОВ

АБСТРАКТ: *В условията на бързо дигитализиране, нарастващ обмен на данни и интензивно навлизане на технологии с изкуствен интелект, облачни услуги и поточно видео с висока разделителна способност, изискванията към безжичните мрежи нарастват лавинообразно. Стандартът Wi-Fi 7 (IEEE 802.11be) се явява технологичен отговор на съвременните предизвикателства за свръхвисока скорост, минимално латентно време и надеждност в натоварена среда. В рамките на настоящия доклад се разглеждат архитектурните и функционални разлики между Wi-Fi 7 и предходните поколения (Wi-Fi 6/6E и Wi-Fi 5), като се акцентира върху ключови иновации като 320 MHz канали, 4096-QAM модулация и мултилинк операциите (MLO). Направена е задълбочена съпоставка на физическия (PHY) и медийния (MAC) слоеве, изследвана е сигурността и са анализирани практическите аспекти при внедряване в корпоративни и индустриални среди.*

1 Увод и историческа еволюция на безжичните мрежи

Еволюцията на безжичните локални мрежи (WLAN) през последните десетилетия следва непрекъснат стремеж към увеличаване на пропускателната способност, намаляване на закъсненията (латентността) и оптимизиране на радиочестотния спектър. Ако през първите години на безжичните технологии (стандартите 802.11a/b/g) основният фокус е бил върху мобилността и базовото свързване в рамките на офиса или дома, то съвременните предизвикателства включват поддръжката на стотици свързани устройства едновременно, виртуална и разширена реалност (VR/AR), 4K/8K видео стрийминг, автоматизирани производствени линии и критични бизнес приложения в реално време.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Факт е, че в съвременните телекомуникационни взаимоотношения безжичната мрежа функционира в изключително напрегнат радиочестотен дискурс – едновременно се изисква висока плътност на покритието, гарантиран ресурс за всяко устройство и устойчивост срещу външни смущения. В отговор на пазарните нужди и научния напредък, Институтът на инженерите по електротехника и електроника (IEEE) разработи стандарта IEEE 802.11be, придобил гражданственост като Wi-Fi 7. Официалният старт на процедурите по сертифициране от страна на Wi-Fi Alliance в началото на 2024 г. беляза навлизането в нова ера на безжичните комуникации, в която мрежовата инфраструктура се превръща в гръбнак на дигиталната трансформация.

Проследяването на историческото развитие показва ясна генерационна приемственост. При Wi-Fi 4 (802.11n) за първи път бе въведена технологията MIMO (Multiple-Input Multiple-Output), която позволи използването на няколко антени за засилване на сигнала. Wi-Fi 5 (802.11ac) ограничи фокуса си основно върху 5 GHz лента, предлагайки по-широки канали (до 160 MHz) и 256-QAM модулация. На следващия етап Wi-Fi 6 и 6E (802.11ax) направиха значителна крачка към подобряване на ефективността при висока плътност на клиентите чрез OFDMA (Orthogonal Frequency-Division Multiple Access) и отварянето на новата 6 GHz честотна лента. Независимо от тези постижения обаче, бързият растеж на трафика и появата на приложения с изисквания за латентност под 5 милисекунди бързо разкриха технологичните тавани на предходните поколения.

Фиксирането върху фундаментални технологични подобрения – неколкократно по-широки канали, по-плътни модулационни схеми и способност за паралелно предаване по няколко честотни ленти наведнъж – рефлектира директно върху потребителското изживяване и стабилността на системите. Поради това анализът на Wi-Fi 7 в сравнение с неговите предшественици не е просто сравнение на максимални скорости, а задълбочен изглед към архитектурните промени в комуникационните протоколи.

2 Архитектурни и функционални различия между поколенията

Като хронотоп (пространство и време), еволюцията на Wi-Fi стандартите бележи преход от базови, монолитни честотни ленти към сложни многопоточни, многодиапазонни и динамично адаптиращи се мрежови архитектури. Исторически погледнато, всяко ново поколение надгражда предшествениците си за сметка на по-ефективно използване на радиоспектъра и по-интелигентно управление на достъпа до средата.

При Wi-Fi 5 (802.11ac) архитектурата бе фокусирана изключително върху увеличаването на единичната скорост (peak throughput) в 5 GHz спектър. Въпреки въвеждането на Downlink MU-MIMO, мрежата страдаше от висока латентност при голям брой едновременно предаващи потребители, тъй като клиентските устройства трябваше да чакат своя ред за пълен достъп до канала. С появата на Wi-Fi 6/6E (802.11ax) фокусът се измести от единичната скорост към общата мрежова ефективност (High Efficiency - HE). Чрез въвеждането на OFDMA каналът бе разделен на по-малки ресурси (Resource Units - RUs), което позволи на рутера да комуникира с множество устройства в рамките на един и същ времеви интервал. Допълнително, Wi-Fi 6E разшири спектъра с добавянето на 6 GHz лента (от 5.925 GHz до 7.125 GHz), осигурявайки допълнителен чист спектър от 1200 MHz.

Стандартът Wi-Fi 7 (802.11be), обозначаван като Extremely High Throughput (EHT), стъпва върху постиженията на Wi-Fi 6E, но прави съществен качествен скок. Той интегрира едновременно трите честотни ленти (2.4 GHz, 5 GHz и 6 GHz) в единен, гъвкав преносен ресурс чрез технологията Multi-Link Operation (MLO). Освен това Wi-Fi 7 удвоява

пространствените потоци, разширява максималната ширина на каналите до 320 MHz и увеличава модулацията до 4096-QAM.

За по-голяма прегледност в Таблица 1 са обобщени основните технически параметри и архитектурни разлики между последните три поколения Wi-Fi стандарти.

Таблица 1. Детайлно сравнение на техническите параметри на Wi-Fi 5, Wi-Fi 6/6E и Wi-Fi 7

Технологичен параметър	**Wi-Fi 5 (802.11ac)**	**Wi-Fi 6 / 6E (802.11ax)**	**Wi-Fi 7 (802.11be)**
Поддържани честотни ленти	5 GHz (2.4 GHz с 802.11n)	2.4 GHz, 5 GHz, 6 GHz (само при 6E)	2.4 GHz, 5 GHz и 6 GHz (интегрирани)
Максимална ширина на канал	20, 40, 80, 160 MHz	20, 40, 80, 160 MHz	До 320 MHz (в 6 GHz спектър)
Амплитудна модулация (QAM)	256-QAM (8 bits/symbol)	1024-QAM (10 bits/symbol)	4096-QAM (12 bits/symbol)
Максимална теоретична скорост	до 6.9 Gbps (практически ~3.5)	до 9.6 Gbps	до 46.1 Gbps
Технология за мултиплексиране	OFDM	OFDMA (за DL и UL)	Advanced OFDMA с Multi-RU
Мулти-потребителски MIMO	DL MU-MIMO (до 4 клиенти)	DL/UL MU-MIMO (до 8 клиенти)	DL/UL MU-MIMO (до 16 потока)
Мултилинк комуникация (MLO)	Не се поддържа	Не се поддържа	Поддържа се (STR и eMLSR)
Пробиване на канали (Puncturing)	Частично / Негъвкаво	Ограничено	Static & Dynamic Channel Puncturing
Средна латентност	30 - 100 ms	10 - 30 ms	< 5 ms (при MLO)

Подробният анализ на данните от таблицата показва, че преходът от Wi-Fi 6 към Wi-Fi 7 носи почти петкратно увеличение на теоретичната пропускателна способност (от 9.6 Gbps на 46.1 Gbps). Това се дължи на синергичния ефект от удвояването на ширината на канала (320 MHz), повишаването на ефективността на кодиране чрез 4096-QAM (носещо 20% увеличение на плътността на данните спрямо 1024-QAM) и удвояването на пространствените потоци от 8 на 16. Важно е обаче да се отбележи, че най-съществения напредък при Wi-Fi 7 не се изразява само в суровата пикова скорост, а във възможността за поддържане на изключително ниска латентност и висока надеждност в реални, натоварени среди.

3 Дълбочинен анализ на иновативните технологии при Wi-Fi 7

За постигането на декларираните характеристики в стандарта IEEE 802.11be са внедрени поредица от ключови технологични иновации на физическия (PHY) и медийния (MAC) слоеве:

3.1. Мултилинк операция (Multi-Link Operation - MLO):

В предходните поколения безжични мрежи, дори когато рутерът поддържаше няколко честотни ленти (напр. 2.4 GHz и 5 GHz), клиентското устройство можеше да се свърже и да

предава данни само през една конкретна лента в даден момент. Превключването между лентите изискваше процедура по презакачване, която предизвикваше прекъсване на трафика и закъснение. MLO фундаментално променя този парадигмален модел. Чрез MLO една точки за достъп (AP) и едно клиентско устройство могат да изградят едновременно няколко радиовръзки (Links) в различни ленти (2.4 GHz, 5 GHz и 6 GHz).

Съществуват два основни режима на работа при MLO: STR (Simultaneous Transmit and Receive) и NSTR (Non-Simultaneous Transmit and Receive / Enhanced Multi-Link Single Radio – eMLSR). При STR режим устройството разполага с независими радиовериги и може едновременно да изпраща данни по 5 GHz лента и да получава данни по 6 GHz лента. Това напълно премахва проблема с блокирането на канала и осигурява пренебрежимо малка латентност (под 5 ms). При eMLSR режим устройството слуша по няколко канала едновременно, но предава по този, който в момента е свободен, с което се спестява енергия и хардуерна сложност.

3.2. Удвоена ширина на канала (320 MHz ultra-wide channels):

Wi-Fi 7 въвежда поддръжка за 320 MHz широки канали в 6 GHz спектър. Това представлява точно удвояване спрямо максималните 160 MHz канали при Wi-Fi 6/6E. Предаването по 320 MHz канал позволява пренос на огромни обеми от данни за изключително кратко време. Поради голямата ширина на спектъра обаче нараства и рискът от припокриване със смущения от съседни мрежи, което наложи създаването на нов механизъм за управление на спектъра – т.нар. Channel Puncturing.

3.3. Усъвършенствано пробиване на канали (Dynamic Channel Puncturing):

При по-старите поколения (Wi-Fi 5 и Wi-Fi 6), ако част от 160 MHz канал (например 20 MHz поддиапазон) бе заета от смущение или друг потребител, целият 160 MHz канал трябваше да бъде изоставен или свиваше ширината си наполовина (до 80 MHz). Wi-Fi 7 въвежда изключително гъвкава система за пробиване на канали. При наличие на смущение в определена честотна лента, рутерът „блокира“ или „пробива“ само засегнатия 20 или 40 MHz участък, докато останалата част от 320 MHz канал продължава да се използва за трансфер на данни без драстичен спад в общата скорост.

3.4. Модулационна схема 4096-QAM (12-bit QAM):

Модулацията определя колко бита информация могат да бъдат кодирани в един радиосигнал (символ). Докато Wi-Fi 6 използваше 1024-QAM (кодираща 10 бита на символ), Wi-Fi 7 преминава към 4096-QAM, където всеки символ пренася 12 бита информация. Това носи директно 20% увеличение на пропускателната способност при същата ширина на канала. За постигането на устойчива 4096-QAM връзка обаче се изисква високо съотношение сигнал/шум (SNR), поради което тази модулация се прилага най-ефективно при близки разстояния и чист радиоефир.

3.5. Multi-RU и подобрен OFDMA:

При Wi-Fi 6 на едно устройство можеше да се разпределя само един ресурс за предаване (Resource Unit - RU) в даден рамков интервал. При Wi-Fi 7 се въвежда технологията Multi-RU, която позволява на един клиент да се разпределят няколко ресурса (комбинация от RUs с различна ширина), оптимизирайки допълнително спектралната ефективност.

4 Мрежова сигурност, криптографски протоколи и защита на данните

С увеличаването на скоростта и навлизането на безжичните мрежи в критични промишлени и корпоративни процеси, въпросът за сигурността на данните придобива

първостепенно значение. Всяко следващо поколение Wi-Fi стандарти не само подобрява радиопараметрите, но и затяга изискванията към автентикацията и криптирането.

Таблица 2. Влияние на новите технологични решения в Wi-Fi 7 върху ключовите мрежови показатели

Иновативно технологично решение	Засегнат мрежов параметър	Механизъм на въздействие	Очакван практически ефект
Multi-Link Operation (MLO)	Латентност и надеждност	Едновременно предаване по 2.4/5/6 GHz ленти	Забавяне < 5 ms, премахване на прекъсванията
320 MHz широк канал	Максимална скорост (Throughput)	Удвояване на спектралната ширина в 6 GHz	Пренос на данни с над 40 Gbps
4096-QAM модулация	Плътност на данните	Кодиране на 12 бита в символ (спрямо 10)	+20% по-висока скорост при добър SNR
Dynamic Channel Puncturing	Устойчивост на смущения	Изолиране само на зашумените 20/40 MHz части	Запазване на голяма част от канала при интерференция
Multi-RU (Resource Units)	Спектрална ефективност	Гъвкаво комбиниране на RU за един клиент	По-добро оползотворяване на празната честота
16x16 MU-MIMO	Капацитет на мрежата	Удвояване на пространствените потоци (от 8 на 16)	Едновременно обслужване на повече клиенти

При по-старите мрежи (Wi-Fi 4 и първите години на Wi-Fi 5) масово се използваше защитният протокол WPA2 (Wi-Fi Protected Access 2), разчитащ на криптиране AES-CCMP. През последните години обаче бяха открити фундаментални уязвимости в WPA2, най-известната от които бе атаката KRACK (Key Reinstallation Attacks), базирана на манипулация на четиристепенното ръкостискане (4-way handshake).

При Wi-Fi 6/6E бе въведена задължителната поддръжка на стандарта WPA3. WPA3 замени остарелия метод PSK (Pre-Shared Key) с по-сигурния протокол SAE (Simultaneous Authentication of Equals), базиран на нулев опит за разкриване на паролата (zero-knowledge proof) и устойчив на атаки чрез речник (dictionary attacks). Освен това за корпоративните мрежи (WPA3-Enterprise) бе въведено 192-битово криптографско ниво.

При Wi-Fi 7 рамката за сигурност е доразвита спрямо новите мултилинк архитектури. Задължителната за Wi-Fi 7 сертификация поддръжка на WPA3 е надградена, за да поддържа независима и паралелна автентикация на отделните линкове при MLO координирането. Това предотвратява атаки от типа „man-in-the-middle“ при превключване между 5 GHz и 6 GHz ленти. В допълнение, задължителното прилагане на Protected Management Frames (PMF) при Wi-Fi 7 гарантира, че управляващите пакети (деаутентикация, деасоциация) не могат да бъдат фалшифицирани от злонамерени актьори с цел предизвикване на откази от обслужване (DoS).

5 Практическо приложение, сфера на внедряване и икономическа ефективност

Сравнителният анализ между Wi-Fi 7 и предходните поколения разкрива фундаментална промяна в таргетираните сценарии на употреба. Докато Wi-Fi 5 бе проектиран за битови потребители и базови офиси, а Wi-Fi 6 за среди с висока плътност (стадиони, летища, аудитории), то Wi-Fi 7 навлиза директно в сфери, доминирани досега от кабелните Ethernet връзки и частните 5G мрежи.

5.1. Индустриална автоматизация и роботика (Industry 4.0):

В съвременните умни фабрики автономните мобилни роботи (AGV/AMR) и роботизираните ръце изискват закъснение на комуникацията под 5 ms и нулев процент загуба на пакети. Досега това се постигаше само с физически кабели или скъпи частни 5G мрежи. Wi-Fi 7 със своя MLO режим осигурява необходимата детерминистична латентност и дублиране на връзката през няколко честоти, правейки възможно пълното безжично управление на фабричните халета.

5.2. Виртуална, разширена и смесена реалност (VR/AR/MR):

Приложенията за потапяща реалност (Immersive Media) изискват едновременно огромна пропускателна способност (над 1-2 Gbps за некадрирано видео с висока разделителна способност) и минимално време за реакция (за предотвратяване на "motion sickness" при потребителя). Wi-Fi 7 осигурява точно тази синергия от параметри, позволявайки безжични VR очила от последно поколение да функционират без забавяне.

5.3. Здравеопазване и телемедицина:

Дистанционните хирургични операции и преносът на обемни медицински изображения (ядерно-гнитен резонанс, скенери) в реално време изискват абсолютна гаранция за непрекъсваемост на връзката. Чрез комбинирането на 6 GHz чист спектър и MLO дублиране, Wi-Fi 7 предоставя сигурна среда за критично медицинско оборудване.

Таблица 3. Сравнителен анализ на приложимостта на Wi-Fi поколенията по сектори

Сектор / Сценарий	Wi-Fi 5 (802.11ac)	Wi-Fi 6 / 6E (802.11ax)	Wi-Fi 7 (802.11be)
Домашни потребители	Отлично за 1080p видео	Отлично за 4K стрийминг и умни домове	За състезателен гейминг и 8K VR
Корпоративни офиси	Умерено (проблеми при много потребители)	Много добро (OFDMA поддържа висока плътност)	Заместител на кабелния Ethernet
Индустрия 4.0 / Роботика	Неприложимо (висока латентност)	Частично приложимо (за некритични данни)	Напълно приложимо (замества 5G/Ethernet)
Медицина / Телемедицина	Ограничено	Добро за мониторинг	За хирургия в реално време
Публични зони (стадиони)	Слаб капацитет	Висок капацитет	Ултра капацитет с MLO координация

6 Предизвикателства пред внедряването на Wi-Fi 7

Въпреки безспорните си технологични предимства, масовото навлизане на Wi-Fi 7 е съпроводено от редица инженерни, регулаторни и икономически предизвикателства, които трябва да бъдат взети под внимание при планирането на нови мрежи:

6.1. Регулаторни ограничения в 6 GHz спектър:

Докато в САЩ (FCC) бе освободен целият 1200 MHz спектър в 6 GHz лента (от 5.925 до 7.125 GHz), в Европа (CEPT и Европейската комисия) за нелицензирано ползване засега е одобрена само долната част на спектъра (5.925 - 6.425 GHz, т.нар. 500 MHz). Това ограничава броя на достъпните непрепокриващи се 320 MHz канали в Европа до едва един или два, което създава предизвикателства при планирането на големи корпоративни мрежи с множество точки за достъп.

6.2. Изисквания към опорната мрежа (Backhaul infrastructure):

Тъй като една точка за достъп Wi-Fi 7 може практически да предава данни със скорост над 10-20 Gbps, стандартните 1 Gbps или 2.5 Gbps Ethernet суичове се превръщат в тесно място (bottleneck). Внедряването на Wi-Fi 7 изисква цялостна подмяна на корпоративната комутационна мрежа с Multi-Gigabit суичове (10 GbE, 25 GbE) и осигуряване на по-висока захранваща мощност по мрежата (PoE++ / 802.3bt).

6.3. Изчислителна сложност и консумация на енергия:

Поддръжката на 4096-QAM, MLO с няколко активни радиовериги и 16 пространствени потока изисква значително по-мощни процесори в точките за достъп и крайната периферия. Това води до увеличено отделяне на топлина и по-висока консумация на енергия, което е предизвикателство за мобилните устройства с батерийно захранване.

7 Заключение и бъдещи перспективи

Процесите на технологично обновяване и въвеждане на нови поколения безжични стандарти винаги са съпътствани от логиката на пазарното търсене и необходимостта от преодоляване на съществуващите физически ограничения. Настоящият сравнителен анализ между Wi-Fi 7 и системите от по-старо поколение показва, че стандартът IEEE 802.11be не представлява просто очередно еволюционно увеличение на скоростта, а качествен архитектурен скок в безжичните комуникации.

Внедряването на ключови иновации като Multi-Link Operation (MLO), 320 MHz канали, 4096-QAM модулация и Dynamic Channel Puncturing трансформира Wi-Fi от среда за най-добро усилие (best-effort) в детерминистична комуникационна платформа с ултраниска латентност под 5 ms и висока надеждност.

В съвременната дигитална реалност, където изкуственият интелект, облачните изчисления, роботиката и потапящите технологии изискват абсолютна надеждност на свързването, Wi-Fi 7 се утвърждава като ключов стандарт за критичните инфраструктури на бъдещето. Поетапната интеграция на Wi-Fi 7 с частните 5G/6G мрежи ще оформи единна, хибридна безжична екосистема, способна да отговори на най-високите технологични предизвикателства на XXI век.

ЛИТЕРАТУРА:

[1] IEEE 802.11be, 2024. Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Extremely High Throughput (EHT). IEEE Standards Association.

[2] Wi-Fi Alliance, 2024. Wi-Fi CERTIFIED 7™ Technology Overview and Specifications. Technical White Paper.

[3] GOUGH, C., 2023. Wireless Networks and Next-Generation Connectivity Standards. London: TechPress.

[4] KHOROV, E., LEVITSKY, I., ASTERIADIS, A., 2023. A Survey on IEEE 802.11be Extremely High Throughput (Wi-Fi 7). IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 412-441.

[5] LOPEZ, A., GARCIA, M., 2024. Multi-Link Operation Performance Analysis in Wi-Fi 7 Enterprise Networks. Journal of Network and Computer Applications, vol. 215, 103682.

[6] MIL-STD-810H, 2019. Environmental Engineering Considerations and Laboratory Tests. US Department of Defense.

[7] NAIK, G., LIU, J., PARK, S., 2022. Coexistence and Spectrum Sharing in the 6 GHz Band: Wi-Fi 6E, Wi-Fi 7, and 5G NR-U. IEEE Access, vol. 10, pp. 32540-32555.

[8] YU, H., et al., 2024. A novel measurement strategy for wireless spectrum efficiency and performance optimization. Fire Safety Journal, vol. 145, 104118.

[9] ZANG, Y., CHEN, X., 2023. Next Generation Wi-Fi 7 Architecture, PHY/MAC Enhancements and Applications. Springer Wireless Communications Series.

APPLICATION OF EDGE AI (ARTIFICIAL INTELLIGENCE IN EDGE DEVICES) IN MODERN COMPUTER SYSTEMS*

PETKO M. NALBANTOV, NIKOLET G. LYULEDZHIEVA, GEORGI P. ILIEV

ABSTRACT: *In the era of rapid digitalization and the exponential growth of sensor and multimedia data generated by IoT devices, the traditional centralized Cloud Computing model exposes significant structural and physical limitations. This paper investigates the Edge AI paradigm (Artificial Intelligence in edge devices) as a modern technological solution designed to minimize latency, reduce bandwidth congestion, and preserve data privacy. A detailed architectural comparison between centralized cloud processing and decentralized edge inferencing is presented. Hardware architectures optimized for edge inferencing (NPU, TPU, FPGA, TinyML) alongside model compression techniques (quantization, pruning, knowledge distillation) are critically evaluated. Practical implementations across Industry 4.0, autonomous vehicles, smart cities, IoMT, and AIoT environments are discussed together with engineering deployment challenges.*

KEYWORDS: *computer systems, Edge AI, edge computing, NPU, TinyML, quantization, low latency, Industry 4.0*

DOI: https://doi.org/10.46687/MT26PMN

ПРИЛОЖЕНИЕ НА EDGE AI (ИЗКУСТВЕН ИНТЕЛЕКТ В КРАЙНИ/ПЕРИФЕРНИ УСТРОЙСТВА) В СЪВРЕМЕННИТЕ КОМПЮТЪРНИ СИСТЕМИ

ПЕТКО М. НАЛБАНТОВ, НИКОЛЕТ Г. ЛЮЛЕДЖИЕВА, ГЕОРГИ П. ИЛИЕВ

АБСТРАКТ: *В условията на стремителна дигитализация и генериране на експоненциално нарастващи обеми от данни от сензори, камери и смарт устройства, традиционният модел за централизирана обработка в облачни сървъри (Cloud Computing) разкрива съществени физически и инфраструктурни ограничения. В настоящия доклад се разглежда парадигмата Edge AI (Изкуствен интелект в крайни/периферни устройства) като съвременен технологичен отговор за преодоляване на високата латентност, мрежовите тесни места и проблемите с поверителността на данните. Направена е детайлна архитектурна съпоставка между централизираната и периферната обработка. Анализирани са хардуерните платформи за изчисления в периферията (NPU, TPU, FPGA, TinyML) и софтуерните техники за компресия на невронни мрежи (квантуване, прунинг, дестилация на знания). Подробно са разгледани ключови практически приложения в Индустрия 4.0, автономните превозни средства, интелигентните градове, телемедицината и AIoT средите, както и инженерните предизвикателства пред внедряването на Edge AI.*

1 Увод и парадигмален преход към периферни изчисления (Edge AI)

През последното десетилетие компютърните системи и технологии отбелязаха невиждан възход, воден от развитието на изкуствения интелект (AI), машинното обучение (ML) и концепцията за Интернет на нещата (IoT). В първоначалния етап от развитието на тези технологии доминираше моделът на централизираните облачни изчисления (Cloud Computing). При него огромни масиви от сурови данни, събирани от милиарди крайни

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

устройства (камери, индустриални сензори, медицински апарати, умни телефони), се изпращат през интернет мрежата до отдалечени дейта центрове, където мощен хардуерен масив извършва обработката и връща отговора обратно към периферията.

Въпреки че облачните среди предоставят практически неограничен изчислителен ресурс и памет, техният монополен статус бе сериозно разклатен от навлизането на приложения в реално време (Real-Time Applications). Забавянето при пренос на данните през мрежата (RTT - Round Trip Time), потенциалните прекъсвания на интернет връзката, критичните изисквания към сигурността на личните данни и огромната консумация на мрежов лентов ресурс (bandwidth) показаха, че облакът не може да задоволи изискванията на фундаментални сфери като автономното шофиране, фабричната автоматизация и хирургическата телемедицина.

Така възниква парадигмата Edge AI – концепция, при която алгоритмите за машинно обучение и невронните мрежи се изпълняват директно върху крайните или периферните устройства (Edge Devices), разположени в непосредствена близост до източника на данни. При Edge AI изчислителният процес (инференцията – inferencing) се премества от отдалечените сървъри върху самия микроконтролер, процесор или специализиран ускорител на устройството. В резултат на това данните се анализират мигновено на място, а към облака се предават единствено агрегирани метаданни или критични събития. Преходът от Cloud AI към Edge AI бележи нов етап в развитието на компютърните архитектури, при който децентрализацията на изчисленията осигурява автономност, ниска латентност и повишена сигурност.

2 Архитектурни и функционални различия между Cloud AI и Edge AI

За да се разбере същността на Edge AI, е необходимо да се направи детайлен архитектурен паралел между традиционната облачна обработка и периферните изчисления. Двата подхода не са взаимноизключващи се, а по-скоро комплементарни, но се различават фундаментално по отношение на топологията, латентността, разпределените ресурси и протоколите за сигурност.

При Cloud AI изчислителната тежест е концентрирана в суперкомпютри или сървърни клъстери с хиляди високопроизводителни графични ускорители (GPU) и тензорни модули (TPU). Тази архитектура е изключително подходяща за фазата на **обучение на модела (Model Training)**, която изисква обработка на огромни масиви от данни и терафлопи изчислителна мощ. Тя обаче е нерационална за непрекъсната фаза на **изпълнение (Model Inferencing)** в условия на ограничена свързаност.

При Edge AI изчисленията се извършват върху топология от "умни" крайни възли – от микроконтролери с консумация под 1 миливат до усъвършенствани периферни сървъри (Edge Servers/Gateways). Моделът предварително се обучава в облака, след което се оптимизира, олекотява и зарежда върху периферното устройство, където изпълнява задачи по класификация, детекция и прогнозиране в реално време.

В Таблица 1 са синтезирани основните технически и функционални разлики между Cloud AI и Edge AI средите.

Анализът на съпоставителните данни показва, че преминаването към Edge AI трансформира структурата на мрежовия трафик и изчислителното забавяне. Вместо да се разчита на централизирана инфраструктура, изчислителната мощ е разпределена в периферията, което премахва зависимостите от физическото разстояние до дейта центъра и подобрява надеждността на цялата система.

Таблица 1. Сравнителен анализ между Cloud AI и Edge AI архитектурите

Архитектурен параметър	Cloud AI (Облачен изкуствен интелект)	Edge AI (Периферен изкуствен интелект)
Локация на изчисленията	Централизирани дейта центрове / Облак	Крайни устройства / Сензори / Edge Gateways
Средна латентност (Закъснение)	Висока (50 ms - 2000 ms) поради мрежата	Ултраниска (< 1 ms - 10 ms) локална обработка
Зависимост от мрежата	Задължителна постоянен интернет връзка	Възможност за пълна автономност (Offline)
Консумация на мрежова лента	Изключително висока (непрекъснат видеопоток)	Минимална (изпращат се само резултати)
Поверителност и сигурност	Риск при пренос на чувствителни данни	Максимална (данните не напускат устройството)
Изчислителен ресурс	Практически неограничен (Supercomputers / GPU)	Ограничен (NPU, TPU, TinyML, FPGA)
Консумация на енергия	Стотици киловати в дейта центъра	Миливати до десетки ватове (на батерия)
Основно предназначение	Обучение на тежки AI модели и Big Data	Изпълнение на оптимизирани модели (Inferencing)

3 Хардуерни архитектури и софтуерни рамки за Edge AI

Реализацията на изкуствен интелект върху крайни устройства изисква специализиран баланс между изчислителна производителност, енергийна консумация, отделяне на топлина и физически размер. Традиционните микропроцесори с общо предназначение (CPU) са неефективни при паралелните матрични операции, характерни за дълбоките невронни мрежи (DNN). Поради това индустрията разработи специализирани хардуерни и софтуерни решения:

3.1. Специализирани хардуерни ускорители за Edge AI:

• **NPU (Neural Processing Unit):** Специализирани силициеви ядра, проектирани за хардуерно ускорение на векторани и матрични операции (умножение и акумулиране - MAC операции). NPU осигуряват десетки ТОПС (Trillion Operations Per Second) при консумация от едва няколко вата и са масово интегрирани в съвременните мобилни чипове (SoC) и индустриални компютри.

• **Edge TPU (Tensor Processing Unit):** Разработени от компании като Google ASIC ускорители, специализирани за бързо изпълнение на Tensorflow Lite модели върху периферни устройства с ниска консумация.

• **FPGA (Field-Programmable Gate Array):** Програмируеми вентилни матрици, които позволяват хардуерна преконфигурация на архитектурата в зависимост от конкретната невронна мрежа. Те предлагат най-ниска латентност и висока гъвкавост, подходящи за индустриални среди.

• **TinyML и Микроконтролери (MCU):** Концепцията TinyML позволява изпълнение на ултралеки машини за състоянието и невронни мрежи върху стандартни 32-битови микроконтролери (напр. ARM Cortex-M) с операционна памет под 256 KB и консумация в миливатовия диапазон.

3.2. Софтуерни методи за компресия и оптимизация на AI модели:

За да може сложна невронна мрежа, обучавана върху хиляди гигабайти, да бъде внедрена в микроконтролер с ограничена памет, се прилагат следните софтуерни оптимизационни техники:

• **Квантуване (Quantization):** Редуциране на точността на теглата на невронната мрежа от 32-битови плаващи числа (FP32) към 8-битови цели числа (INT8). Това намалява размера на модела над 4 пъти и ускорява изчисленията без съществена загуба на точност.

• **Прунинг / Обрязване (Pruning):** Премахване на излишните тегла и неврони в мрежата, които имат нисък принос към крайния резултат, за да се намали бройката на нужните изчислителни операции.

• **Дестилация на знания (Knowledge Distillation):** Обучение на по-малка и лека мрежа ("ученик") да възпроизвежда поведението на голяма и сложна мрежа ("учител").

Таблица 2. Сравнение на хардуерните платформи за Edge AI изчисления

Хардуерна платформа	Типична консумация	Изчислителна мощ (TOPS)	Гъвкавост	Типично приложение
Edge CPU (ARM/RISC-V)	1W - 5W	< 0.5 TOPS	Изключително висока	Базов контрол, обработка на текстови данни
Edge GPU (напр. Nvidia Jetson)	10W - 60W	20 - 275 TOPS	Висока	Автономни автомобили, сложен Computer Vision
NPU (Neural Processing Unit)	1W - 10W	10 - 50 TOPS	Средна (само за NN)	Смартфони, смарт камери, Edge Gateways
FPGA (Field Programmable)	5W - 20W	Зависи от дизайна	Хардуерно гъвкава	Индустриална роботика, аерокосмически системи
TinyML Microcontroller (MCU)	< 10 mW	< 0.01 TOPS	Ниска	Носими медицински сензори, вибрационни анализи

4 Практически приложения на Edge AI в специалността КСТ

Технологията Edge AI намира широк спектър от практически приложения в съвременните компютърни системи, индустриалната автоматизация и ежедневието:

4.1. Индустрия 4.0 и Интелигентно производство (Smart Manufacturing):

В модерните цифровизирани фабрики Edge AI се прилага за предсказуема поддръжка (Predictive Maintenance). Сензори за вибрации, акустика и температура, оборудвани с TinyML микроконтролери, анализират непрекъснато работата на роторни машини. При откриване на микроаномалии в честотния спектър устройството алармира за предстояща дефектация седмици преди тя да се случи, предотвратявайки милионни щети.

Допълнително, камери с NPU ускорители извършват автоматизиран оптичен контрол на качеството (Computer Vision) на поточната линия със скорост от стотици детайли в минута.

4.2. Автономни превозни средства и безпилотни летателни апарати (Дронове):

При автономните автомобили (Self-Driving Cars) всяка секунда забавяне може да бъде фатална. Автомобил, движещ се със 100 км/ч, изминава близо 28 метра за една секунда. Изпращането на видеопоток от камерите и лидарите до облака за анализ на препятствията е напълно недопустимо. Edge AI бордовите компютри (като Nvidia DRIVE) обработват терабайти данни в секунда локално в автомобила, вземайки спирачни и кормилни решения с закъснение под 2 милисекунди.

4.3. Интелигентни градове и видеонаблюдение (Smart Cities & Edge Vision):

Традиционните системи за градско наблюдение изискват огромна мрежова честотна лента за предаване на видеопотоци до централно полицейско управление. Съвременните "умни" камери с вграден Edge AI анализират картината директно на обектива – разпознават регистрационни номера, броят преминаващи пешеходци и откриват пътнотранспортни произшествия или изоставени предмети. Към централния сървър се изпращат единствено кратки текстови нотификации и координати, спестявайки над 99% от мрежовия трафик.

4.4. Интернет на медицинските неща (IoMT - Internet of Medical Things):

Персонални преносими медицински устройства (ЕКГ холтери, инсулинови помпи) използват Edge AI за анализ на биометричните показатели на пациента в реално време. При откриване на опасни аритмии или спадове в захарта устройството подава незабавен сигнал към пациента и болницата, без да зависи от това дали телефонът има клетъчен обхват.

Таблица 3. Приложение на Edge AI по сектори и постигнати ефекти

Сектор на приложение	Използвана Edge AI технология	Традиционен проблем	Постигнат ефект с Edge AI
Индустрия 4.0	TinyML сензори за вибрации	Неочаквани аварии на машини	Предотвратяване на престои, локален анализ
Автономни коли	Edge GPU / Multi-NPU масиви	Висока латентност на облака	Реакция под 2 ms, безопасно шофиране
Smart Cities	Smart Cameras с YOLO/Computer Vision	Претоварване на мрежата от видео	99% редукция на трафика, спазване на GDPR
Телемедицина (IoMT)	Микроконтролери за ЕКГ анализ	Липса на обхват при криза	Непрекъснат автономен офлайн мониторинг
Умни домове (AIoT)	Локално разпознаване на реч	Изпращане на глас в облака (privacy)	Защита на личните данни, мигновен отговор

5 Поверителност, сигурност и киберзащита при Edge AI

Един от най-силните аргументи в полза на Edge AI е значителното подобряване на поверителността и сигурността на данните. В ерата на строги регулаторни рамки като GDPR в Европейския съюз, изпращането и съхраняването на чувствителни видеопотоци, гласови

записи и медицински досиета в централизирани облаци крие огромни правни и киберрискове.

При Edge AI суровите лични данни се обработват изцяло в оперативната памет на локалното устройство и незабавно се изтриват. Към външни системи се съобщава само абстрактен резултат (напр. "открит е пешеходец на кръстовището" вместо предаване на видеото на пешеходеца). Това радикално намалява повърхността за атака (Attack Surface).

От друга страна, самата Edge AI инфраструктура поставя нови предизвикателства пред инженерните екипи по киберсигурност:

• **Физическа уязвимост на крайните устройства:** Тъй като Edge устройствата са монтирани на обществени места или във фабрики, злонамерени лица могат да получат физически достъп до тях и да се опитат да извлекат теглата на AI модела чрез инженерни методи (Side-Channel Attacks).

• **Атаки срещу AI модела (Adversarial Attacks):** Чрез фина модификация на входящия сигнал (напр. лепене на специален стикер върху пътен знак) нападателят може да подведе периферния AI модел да направи грешна класификация.

За справяне с тези заплахи съвременните КСТ архитектури интегрират хардуерни модули за сигурност (Secure Enclaves / TPM) и криптиране на теглата на моделите в флаш паметта на устройството.

6 Инженерни предизвикателства и пречки пред масовото внедряване

Въпреки изключителните предимства, масовото навлизане на Edge AI среща няколко съществени технически и организационни бариери:

6.1. Ограничения на ресурсите и термичен мениджмънт:

Периферните устройства често работят в пасивно охлаждани кутии при екстремни външни температури (напр. на стълбове за улично осветление или в двигателни отсеци). Поддържането на висока изчислителна мощност без прегряване изисква прецизно управление на честотата и захранващото напрежение на NPU ускорителите.

6.2. Управление и актуализация на моделите (MLOps at the Edge):

Обновяването на софтуера и AI моделите върху флот от десетки хиляди разпределени периферни устройства е изключително комплексна задача. Необходими са сигурни протоколи за обновяване по въздуха (OTA - Over The Air) и възможност за връщане към предишна версия при възникване на грешка.

6.3. Дрифт на данните (Data & Concept Drift):

С течение на времето условията на околната среда около периферното устройство се променят (напр. промяна в осветеността, сезонни промени), което води до спад в точността на предварително обучения модел. За преодоляването на този проблем се разработват техники за **Федеративно обучение (Federated Learning)**, при които устройствата обновяват модела си локално и обменят само подобренията с облака без споделяне на сурови данни.

7 Заключение и бъдещи перспективи

Настоящият доклад показва, че Edge AI (Изкуственият интелект в крайните и периферните устройства) не е просто временна архитектурна тенденция, а фундаментална промяна в начина, по който компютърните системи обработват информация.

Чрез изместване на изчислителния център от далечните облачни дейта центрове към самото място на възникване на данните, Edge AI постига ултраниска латентност,

гарантирана автономност, максимална поверителност и значително икономисване на мрежови ресурси.

В бъдеще се очаква все по-дълбока синергия между Edge AI и хибридните 5G/6G мрежи чрез концепцията **MEC (Multi-access Edge Computing)**. Навлизането на все по-ефективни NPU архитектури и технологии като TinyML ще позволи дори най-малките сензори с цена под един долар да притежават автономни умения за анализ. Специалността „Компютърни системи и технологии“ стои в самата основа на този процес, създавайки хардуера, протоколите и оптимизираните софтуерни платформи на утрешния свързан свят.

ЛИТЕРАТУРА:

[1] DENG, S., ZHAO, H., FANG, J., YIN, J., DUSIT, N., 2020. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7457-7469.

[2] SITUNAYAKE, D., WARDEN, P., 2023. TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. O'Reilly Media.

[3] SHI, W., CAO, J., ZHANG, Q., LI, Y., XU, L., 2016. Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646.

[4] NVIDIA Corporation, 2024. Edge AI Infrastructure and Jetson Embedded Systems Technical Architecture. White Paper.

[5] ARM Ltd., 2023. Deploying Artificial Intelligence on Ethos NPU and Cortex-M Architectures. Technical Report.

[6] ZHOU, Z., CHEN, X., LI, E., ZENG, L., LUO, K., 2019. Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. Proceedings of the IEEE, vol. 107, no. 8, pp. 1738-1762.

[7] Google Inc., 2024. TensorFlow Lite for Microcontrollers & Edge TPU Optimization Guide.

[8] ISO/IEC 23053:2022, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML). International Organization for Standardization.

STEGANOGRAPHIC CODING IN THREE DIMENSIONAL POLYGONAL MESHES THROUGH CYCLIC ROTATION OF VERTEX INDICES*

GEORGI A. KOZAREV

ABSTRACT: *Polygonal mesh steganography can exploit the order of representation without changing vertex coordinates, but geometric invariance does not guarantee correct facet orientation. This study formalizes cyclic one-bit-per-facet coding and establishes conditions for reliable blind extraction. The methodology combines mathematical analysis with existing MATLAB results for the Stanford Bunny model. The experiment embeds 1824 bits in a container with 86 632 facets with zero coordinate mean squared error and zero bit error rate. Ascending sorting may reverse facet orientation, whereas cyclic canonicalization preserves it without changing the extraction rule. Practical use requires synchronized vertex identifiers and facet order, followed by verification after STL serialization, while statistical undetectability and robustness to mesh processing remain open questions.*

KEYWORDS: *3D steganography, polygonal mesh, cyclic permutation, blind extraction, facet orientation*

DOI: https://doi.org/10.46687/MT26GAK

СТЕГАНОГРАФСКО КОДИРАНЕ В ТРИИЗМЕРНИ ПОЛИГОНАЛНИ МРЕЖИ ЧРЕЗ ЦИКЛИЧНА РОТАЦИЯ НА ИНДЕКСИТЕ НА ВЪРХОВЕТЕ

ГЕОРГИ А. КОЗАРЕВ

АБСТРАКТ: *Стеганографията в полигонални мрежи може да използва реда на представяне, без да променя координатите на върховете, но геометричната неизменност не гарантира коректна ориентация на фасетите. В изследването се формализира цикличното кодиране с един бит на фасета и се определят условията за надеждно сляпо извличане. Методологията съчетава математически анализ със съществуващи резултати от MATLAB за модела Stanford Bunny. В експеримента се вграждат 1824 бита в контейнер с 86 632 фасети при нулева средноквадратична грешка на координатите и нулев коефициент на битова грешка. Възходящото сортиране може да обърне ориентацията на фасетите, докато цикличната канонизация я запазва, без да променя правилото за извличане. Практическото приложение изисква синхронизирани идентификатори на върховете и ред на фасетите, последвани от проверка след сериализация в STL, а статистическата неоткриваемост и устойчивостта при обработка на мрежата остават открити въпроси.*

1 Въведение

Триизмерната стеганография използва цифрови геометрични модели като носители на скрити съобщения. Още ранните работи на Ohbuchi и съавтори показват, че триизмерните 3D (Three-Dimensional) модели могат да пренасят вградени данни [13]. При полигоналните мрежи информация може да се вгражда чрез промени в координатите [5], [6], чрез преобразувания на представянето [2], [7] или чрез други характеристики на модела [20]. Обзорът на Zhou и съавтори разглежда отделно методите в областта на пермутациите

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

и показва необходимостта качеството на контейнера да се оценява заедно с неговата откриваемост [20]. При класическите носители, като растерните изображения, широко се използва замяна на най-младшите, т.е. най-малко значимите битове на пикселите LSB (Least Significant Bit) [16].

Изследванията на Bogomjakov, Gotsman и Isenburg демонстрират кодиране чрез реда на съхраняване на върхове и стени без изменение на геометрията [2]. Авторите посочват и цикличното изместване на върховете в описанието на всяка фасета като допълнителен носител, използван преди това от Cheng и Wang при триъгълни фасети [2], [7]. Настоящият доклад разглежда по-ограничен локален механизъм, един бит се записва чрез избор на началния връх в описанието на отделен триъгълник. Представеният топологичен алгоритъм и експериментът в средата за матрични изчисления MATLAB са част от собствената разработка на автора.

Целта е да се формализират вграждането и сляпото извличане, да се анализират отчетените резултати и да се уточнят условията за коректна работа с формата STL (Standard Triangle Language). Допълнително се извежда вариант на канонизацията, който запазва ориентацията на фасетите. Приносът на анализа е в разграничаването на неизменни координати, неизменна свързаност и коректна ориентация, които изискват различни проверки.

2 Математически модел на контейнера.

Нека контейнерът е триъгълна мрежа с N върха и M фасети. Матрицата $\mathbf{V}$ съдържа пространствените координати, а всеки ред $\mathbf{f}_i$ на матрицата $\mathbf{F}$ е наредена тройка от индекси към $\mathbf{V}$. Допуска се, че трите индекса във всяка използвана фасета са различни и триъгълникът не е геометрично дегенериран:

$$\mathbf{V} \in \mathbb{R}^{N\times 3}, \mathbf{F} \in \{1, \dots, N\}^{M\times 3} \tag{1}$$

Тайното съобщение се представя като битов вектор $S = (s_1,\dots,s_K)$, където s_i е 0 или 1 и $1 \le K \le M$. При един бит на фасета суровият капацитет е M бита. Ако H бита се отделят за служебни данни, полезният капацитет намалява до $M - H$. В базовия вариант дължината K се предоставя на получателя предварително.

Терминът „топологичен“ тук обозначава обработката на структурната матрица. Цикличната ротация не добавя и не премахва върхове, ръбове или стени и не изменя тяхната инцидентност. По-точно методът използва излишъка в представянето на една и съща фасета, а не промяна на топологията на повърхността.

STL съхранява фасетите чрез нормала и координатите на трите им върха, а глобалната индексна таблица не е част от този формат [4], [17]. Матриците V и F са вътрешно представяне, получено след прочитане, например чрез stlread [11]. Следователно запазването на индекси между предавателя и получателя е условие на конкретната реализация, а не автоматично свойство на STL.

3 Базов алгоритъм за вграждане.

В базовия алгоритъм за всяка използвана фасета се формира възходящо сортирана тройка $a_i = (a_{i1},a_{i2},a_{i3})$, за която $a_{i1} < a_{i2} < a_{i3}$. Дефинира се операторът за циклично изместване наляво:

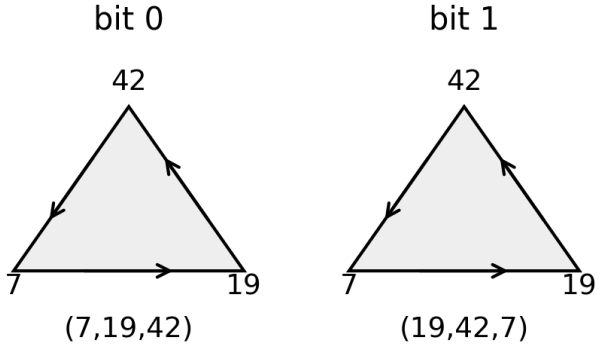
$$\mathrm{R}(a, b, c) = (b, c, a) \tag{2}$$

При бит 0 тройката се записва без изместване, а при бит 1 се прилага една ротация. Общото правило е:

$$\mathbf{f}_i^{\,s} = \mathrm{R}^{s_i}(\mathbf{a}_i), i = 1, \ldots, K \tag{3}$$

Геометричната матрица се копира без модификации: $\mathbf{V}^s = \mathbf{V}$. Фасетите след позиция K остават непроменени. Необходимо е предварително да се провери капацитетът, тъй като съобщение с повече от M бита не може да се вгради по тази схема без допълнителен контейнер.

Например базовата тройка (7,19,42) кодира бит 0, а тройката (19,42,7) кодира бит 1. Двата записа описват една и съща триъгълна област с еднаква циклична ориентация. Разликата е в началната позиция на описанието, както е показано на фиг. 1.



Фиг. 1. Локално кодиране чрез избор на начален връх при еднаква циклична ориентация

4 Сляпо извличане и декодиране.

Получателят използва стего-мрежата и известната дължина K, без да се нуждае от оригиналната мрежа. За всяка от първите K фасети се определя позицията j_i на минималния индекс. Тъй като минимумът е уникален, базовото състояние има $j_i = 1$, а еднократно ротираното състояние има $j_i = 3$:

$$j_i = \arg\min_j \mathbf{f}_{ij}^{\,s}, j \in \{1,2,3\} \tag{4}$$

Декодирането връща бит 0 при $j_i = 1$ и бит 1 при $j_i = 3$. Позиция 2 не е допустимо кодово състояние. В базовата реализация тя се интерпретира като 0, а за по-строга проверка на канала е целесъобразно да се отчита като невалидна позиция, вместо да се прикрива възможна грешка.

Таблица 1 съпоставя локалните състояния с извличаните битове. Тя показва и третата възможна ротация, която схемата не използва за полезна информация.

Таблица 1. Кодови състояния при базова тройка (7,19,42)

Тройка	$\mathbf{j_i}$	**Декодиране**
(7,19,42)	1	бит 0
(19,42,7)	3	бит 1
(42,7,19)	2	невалидно

След извличане потокът се групира в байтове. В реализацията се използва кодовата таблица ASCII (American Standard Code for Information Interchange) за текст на латиница. За български текст е необходимо предварително кодиране, например UTF-8 (Unicode Transformation Format – 8-bit), като K се определя по броя на байтовете, а не по броя на видимите символи. Сляпото извличане не означава възстановяване на първоначалния ред на описване на фасетите.

5 Запазване на ориентацията.

Изцяло възходящото сортиране изисква отделен анализ. Например (7,42,19) и (7,19,42) съдържат същите индекси, но имат противоположна ориентация. При STL редът на върховете трябва да е съгласуван с външната нормала съгласно правилото на дясната ръка [4], [17]. Затова нулевата грешка в координатите (MSE = 0) сама по себе си не доказва запазване на ориентацията.

Като доуточнение на базовата схема може да се използва канонизация C, която поставя минималния индекс на първо място само чрез циклично изместване. Останалите два индекса запазват цикличния си ред:

$$\mathrm{C}(\mathbf{f}_i) \;=\; \mathrm{R}^{j_i-1}(\mathbf{f}_i) \tag{5}$$

След канонизацията се прилага същото кодиране с две състояния без допълнителна ротация при бит 0 и с една ротация наляво при бит 1. Минималният индекс отново е на първа или трета позиция, така че правилото за извличане остава непроменено. Този вариант доуточнява базовия алгоритъм. Неговите свойства са изведени аналитично и не са част от измерванията на базовата MATLAB реализация.

За недегенериран триъгълник ненормираната нормала се задава с векторното произведение на две негови страни [3]:

$$\mathbf{n}(\mathbf{f}) \;=\; (\mathbf{v}_b \;-\; \mathbf{v}_a) \;\times\; (\mathbf{v}_c \;-\; \mathbf{v}_a) \tag{6}$$

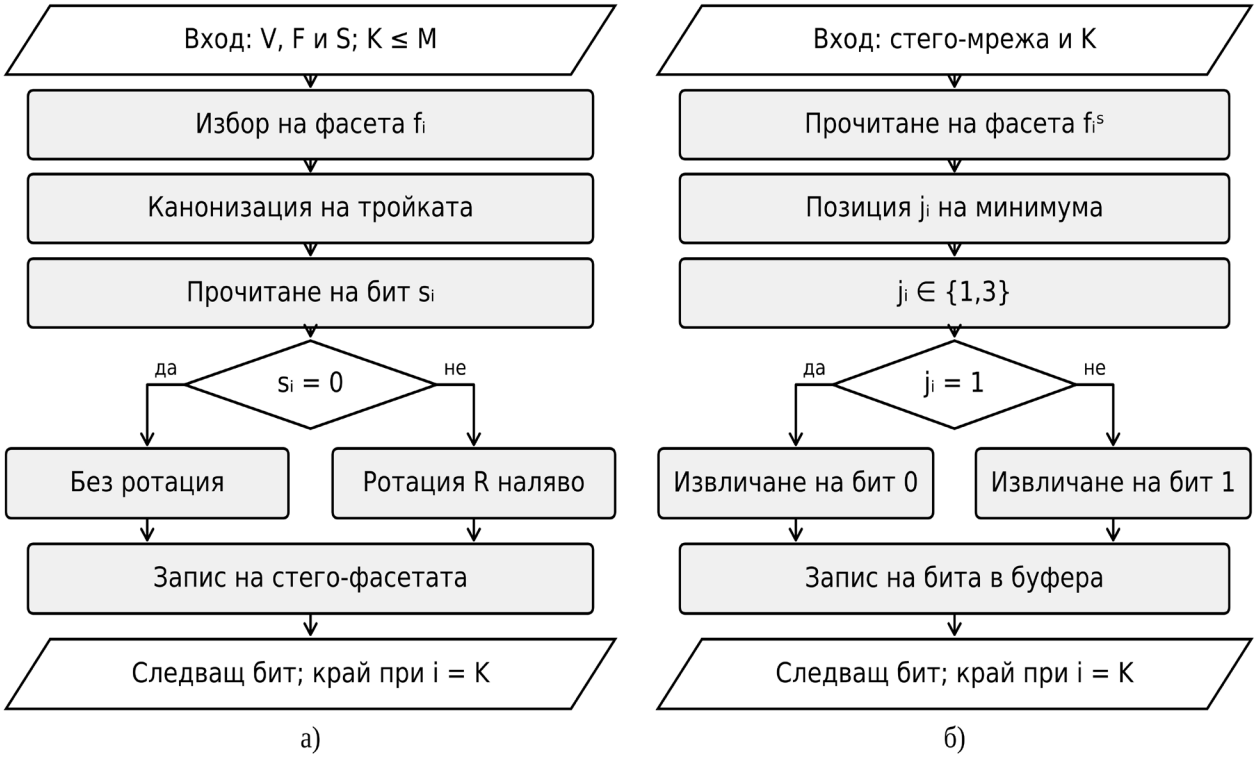
При циклична ротация **n**(R(**f**)) = **n**(**f**), докато размяната на два върха сменя знака. Канонизацията C и последващото кодиране използват единствено циклични ротации. Оттук следва запазване на ориентацията спрямо входната фасета. Това не поправя фасета, която още във входния модел е ориентирана неправилно.

6 Софтуерна реализация и сложност.

Последователностите за вграждане и извличане са обобщени на фиг. 2а и фиг. 2б. Блокът за канонизация при вграждане може да реализира базовото сортиране или доуточнената циклична канонизация. Двата варианта трябва да се разграничават при оценката на ориентацията. На схемата за извличане се предполага предварителна проверка за допустима позиция j_i, като при $j_i = 2$ се отчита невалидно състояние.

В MATLAB контейнерът се прочита чрез TR = stlread(filename), след което V = TR.Points и F = TR.ConnectivityList [11]. Работното копие F^s се обработва ред по ред. За базовия вариант се използват сортиране и циклично изместване, а за варианта със запазена ориентация сортирането се заменя с намиране на минимума и подходяща ротация.

Обработката на една тройка има постоянна сложност. Следователно вграждането и извличането на K бита са O(K), а копирането на цялата матрица **F** е O(M). Към тези оценки се добавя файловият вход и изход. При буфер от K бита допълнителната памет за извлеченото съобщение е O(K).



Фиг. 2. Функционални схеми: а) вграждане на един бит във всяка избрана фасета; б) сляпо извличане при допустими кодови състояния

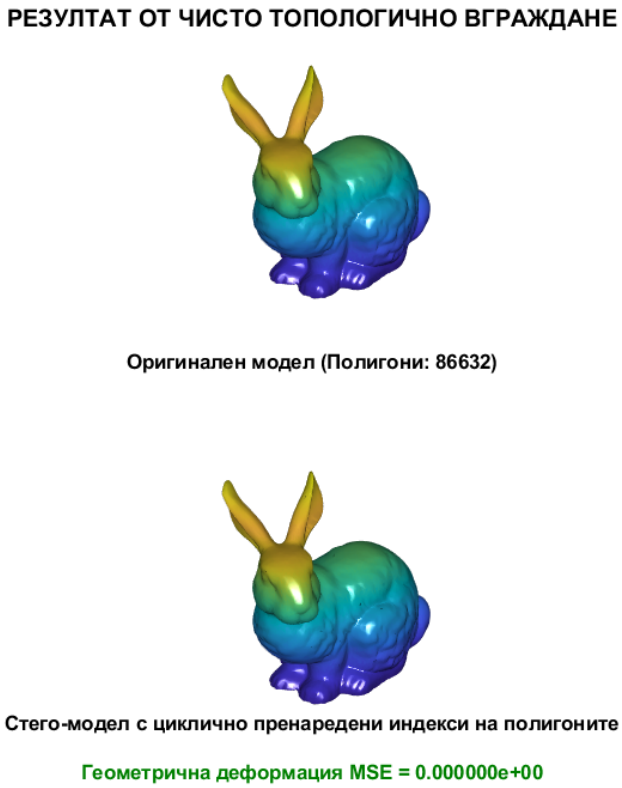
За запис се създава triangulation(F^s,V), която се подава на stlwrite [12]. Успешният запис трябва да бъде последван от повторно прочитане и сравнение на извлеченото съобщение. Тази проверка е различна от извличането директно от F^s в оперативната памет. При нова номерация на върховете минималният индекс може да се промени, дори геометрията да остане същата.

За преносимост е необходима съгласувана канонична номерация или друг детерминиран критерий за подреждане на върховете. Той трябва да се възпроизвежда от двете страни след файловото преобразуване. Освен това трябва да се запази редът на използваните фасети, понеже пренареждането му променя последователността на битовете.

7 Показатели и отчетени резултати.

В разработката е реализирана симулация в MATLAB с модела Stanford Bunny. Официалният архив на Stanford публикува реконструкция с 35947 върха и 69451 триъгълника във формат PLY (Polygon File Format) [15]. Моделът е реконструиран от 10 лазерни сканирания чрез метода на Turk и Levoy за съединяване на частични триъгълни мрежи в една обща повърхнина (zippering) [18]. За използвания STL контейнер конзолният отчет показва 86632 фасети и съобщение от 1824 бита, съответстващо на 228 ASCII символа. Разликата в броя на фасетите означава, че архивната PLY версия и използваният STL контейнер не трябва да се отъждествяват.

Фигура 3 представя визуалното сравнение от експеримента. Показаните повърхности имат еднакъв вид в тази визуализация. Изображението само по себе си не удостоверява нормалите на всички фасети или устойчивостта на файловия канал.



Фиг. 3. Оригинален и стего-модел Stanford Bunny при топологично кодиране

Геометричното изкривяване на контейнера се оценява чрез средноквадратичната грешка MSE (Mean Squared Error) между координатите на оригиналния и стего-модела. Тя се изчислява при съответстващи върхове като сумата на квадратите на разликите между всички 3N координатни компоненти, разделена на 3N. Понеже алгоритъмът не променя матрицата **V**, в индексното представяне тази величина е точно нула:

$$\mathbf{V}^s = \mathbf{V} \Rightarrow \mathrm{MSE} = 0 \tag{7}$$

Коефициентът на битова грешка BER (Bit Error Rate) при извличане на скритото съобщение е отношението на броя сгрешени битове към K, умножено по 100%. Стойностите от симулацията в MATLAB са обобщени в табл. 2. Заетостта на контейнера е пресметната от K/M и е обозначена като производна величина.

Заетостта е изчислена като *100 × 1824 / 86632*. Числото 928 е отчетеният в експеримента брой изменени фасети и не се приравнява автоматично на всички 1824 използвани позиции. Количеството използвани фасети и количеството действително променени записи са различни показатели.

Данните показват успешно възстановяване на съобщението в описаните условия и липса на геометрична деформация. В експериментите топологичният метод има най-ниските отчетени времена сред трите разгледани подхода. За възпроизводимо сравнение са необходими още версия на MATLAB, характеристики на хардуера и повторни измервания. Единичните времена не доказват общо предимство при всякакви модели и товари.

Таблица 2. Параметри и резултати от симулацията

Показател	**Стойност**
Фасети M	86 632
Съобщение K	1824 бита
ASCII символи	228
Суров капацитет	86 632 бита
Заетост K/M	2,105%
Отчетени изменени фасети	928
Време за вграждане	0,010036 s
Време за извличане	0,005408 s
MSE на координатите	0
Сгрешени битове	0
BER	0,00%

Неизменната геометрия е съгласувана с принципа на пермутационните методи в [2]. Разликата е, че разглежданата схема кодира локално по един бит на фасета, вместо да използва глобално пренареждане на списъци от примитиви. Поради различните механизми и експериментални условия не се прави количествено сравнение на скоростта или сигурността с [2].

8 Ограничения и откриваемост.

Запазването на координатите осигурява геометрична незабележимост, но не гарантира статистическа неоткриваемост [9]. В използваните фасети минималният индекс е само на първа или трета позиция. Така възниква структурен признак, който може да се изследва от специализиран стегоанализ. Подобно на задачите за активно откриване на обекти по характерни отклонения в отражения на сондиращ сигнал [8], стегоанализът търси статистически отклонения от очаквания модел на носителя. Оценката на сигурността изисква сравнение с немодифицирани файлове от същия процес на генериране и отделен детектор [10], [19], [20].

Базовата схема не включва таен ключ и не криптира съдържанието. Познаването на алгоритъма, реда на фасетите и K е достатъчно за прочитане, което не отговаря на принципа на Керкхофс, според който сигурността трябва да зависи единствено от тайния ключ [9]. При необходимост поверителността трябва да се осигури отделно, като при реален пренос се отчита и съвместимостта на криптирането с използваното канално кодиране и модулация [14], а ключово избиране на позиции може да се разглежда като бъдещо разширение, което също подлежи на оценка.

Методът е чувствителен към канонизация на фасетите, преномериране на върховете и промяна на реда на стените. Опростяване, ремешинг или поправка на мрежата могат да разрушат кодовите състояния. Устойчивост към тези операции не следва от BER = 0 в ненарушения канал. За STL следва да се проверяват отделно координатното закръгляване при сериализация и запазването на цикличния ред.

Таблица 3 обобщава връзката между типични операции върху мрежата и изискванията на декодера. Тя е аналитична оценка на механизма, а не експериментално измерена устойчивост.

Таблица 3. Операции върху контейнера и условия за извличане

Операция	**Очаквано влияние**
Запазени индекси и ред	Кодовите позиции се запазват
Циклично пренареждане на фасета	Може да промени нейния бит
Нова номерация на върховете	Може да промени минималния индекс
Нов ред на фасетите	Пренарежда битовия поток
Опростяване или ремешинг	Може да премахне кодирани фасети
STL запис и прочитане	Изисква проверка на координати, индекси и ред

9 Заключение

Разгледаният метод кодира по един бит в триъгълна фасета чрез избор между две циклични подредби. Вграждането и сляпото извличане имат линейна сложност спрямо дължината на съобщението. При непроменена матрица на върховете MSE е нула, а в симулацията в MATLAB е отчетен BER = 0,00%.

Анализът показва, че запазването на координатите трябва да се разглежда отделно от запазването на ориентацията. Канонизацията чрез циклично поставяне на минималния индекс в началото запазва входната ориентация и позволява същото правило за извличане.

Практическото приложение изисква синхронизирани идентификатори и ред на фасетите, както и проверка след файлов запис и повторно прочитане. Следващите изследвания трябва да обхванат различни 3D модели, различни STL четци, статистическа откриваемост и устойчивост към пренареждане. Така може да се оцени реалният канал за пренос на информация, извън идеализираното матрично представяне. Перспективна приложна област е скритият пренос на служебни данни в системите за управление, например на резултати от проследяване на маневриращи цели с филтър на Калман и интерактивен многомоделен подход [1].

ЛИТЕРАТУРА:

[1] Atanasov D. Tracking Maneuvering Target with Kalman Filter and Interactive Multiple Model. In: Scientific Research and Education in the Air Force – AFASES 2019. Brașov: “Henri Coandă” Air Force Academy, 2019, pp. 88–97, ISSN 2247-3173.

[2] Bogomjakov A., Gotsman C., Isenburg M. Distortion-Free Steganography for Polygonal Meshes. Computer Graphics Forum, Vol. 27, No. 2, 2008, pp. 637–642. DOI: 10.1111/j.1467-8659.2008.01161.x.

[3] Botsch M., Kobbelt L., Pauly M., Alliez P., Lévy B. Polygon Mesh Processing. Natick, MA: A K Peters, 2010, ISBN 978-1-56881-426-1.

[4] Burns M. The StL Format. Excerpt from Automated Fabrication, 1993. Available at: https://fabbers.com/tech/STL_Format (accessed 13 October 2026).

[5] Cayre F., Macq B. Data Hiding on 3-D Triangle Meshes. IEEE Transactions on Signal Processing, Vol. 51, No. 4, 2003, pp. 939–949.

[6] Chao M.-W., Lin C.-H., Yu C.-W., Lee T.-Y. A High Capacity 3D Steganography Algorithm. IEEE Transactions on Visualization and Computer Graphics, Vol. 15, No. 2, 2009, pp. 274–284.

[7] Cheng Y.-M., Wang C.-M. A High-Capacity Steganographic Approach for 3D Polygonal Meshes. The Visual Computer, Vol. 22, No. 9, 2006, pp. 845–855. DOI: 10.1007/s00371-006-0069-4.

[8] Dimitrov D., Kirov M.-A. Using Multi-Carrier Probing Signals for Detecting Non-Linear Objects. In: Scientific Research and Education in the Air Force – AFASES 2016. Brașov: "Henri Coandă" Air Force Academy, 2016, pp. 247–250. DOI: 10.19062/2247-3173.2016.18.1.33.

[9] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge: Cambridge University Press, 2009, ISBN 978-0-521-19019-0.

[10] Li Z., Bors A. G. Steganalysis of 3D Objects Using Statistics of Local Feature Sets. Information Sciences, Vol. 415–416, 2017, pp. 85–99. DOI: 10.1016/j.ins.2017.06.011.

[11] MathWorks. stlread — Create triangulation from STL file. MATLAB Documentation. Available at: https://www.mathworks.com/help/matlab/ref/stlread.html (accessed 13 October 2026).

[12] MathWorks. stlwrite — Create STL file from triangulation. MATLAB Documentation. Available at: https://www.mathworks.com/help/matlab/ref/stlwrite.html (accessed 13 October 2026).

[13] Ohbuchi R., Masuda H., Aono M. Embedding Data in 3D Models. In: Interactive Distributed Multimedia Systems and Telecommunication Services (IDMS 1997). Springer, 1997, pp. 1–10.

[14] Parvanov S. Research of Different Turbo Code Speeds, Types of Modulations, Decoding Methods and Their Compatibility with Encryption Techniques. Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference, Vol. II, 2024, pp. 232–236. DOI: 10.17770/etr2024vol2.8037.

[15] Stanford University Computer Graphics Laboratory. The Stanford 3D Scanning Repository. Stanford Bunny. Available at: https://graphics.stanford.edu/data/3Dscanrep/ (accessed 13 October 2026).

[16] Stoyanova V. T. Steganography System Using LSB Methods. In: Proceedings of the ENTRENOVA – ENTerprise REsearch InNOVAtion Conference, Split, Croatia, 6–8 September 2018, Vol. 4, pp. 381–387.

[17] Szilvási-Nagy M., Mátyási Gy. Analysis of STL Files. Mathematical and Computer Modelling, Vol. 38, 2003, pp. 945–960.

[18] Turk G., Levoy M. Zippered Polygon Meshes from Range Images. In: Proceedings of SIGGRAPH '94, Computer Graphics Proceedings, Annual Conference Series. ACM, 1994, pp. 311–318.

[19] Yang Y., Ivrissimtzis I. Mesh Discriminative Features for 3D Steganalysis. ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 10, No. 3, 2014, Article 27, pp. 1–13.

[20] Zhou H., Zhang W., Chen K., Li W., Yu N. Three-Dimensional Mesh Steganography and Steganalysis: A Review. arXiv preprint arXiv:2104.10203, 2021. Available at: https://arxiv.org/abs/2104.10203 (accessed 13 October 2026).

FROM CLASSIC QOS TO AGE OF INFORMATION AND FRESHNESS OF SERVICE IN DISTRIBUTED CONTROL SYSTEMS*

DRAGOMIR I. VASILEV, SREBRIN V. SHARBANOV

ABSTRACT: *Distributed automated control systems buffer requests under bursty traffic, where mean response time does not describe freshness at the receiver. The paper recalls Age of Information for an M/M/1 FIFO status-update model and the load near ρ≈0.531 that minimizes mean age in that model only. Freshness of Service is the share of completed requests whose queue wait is below a design threshold, kept apart from Age of Information and from rejected requests. Five finite-horizon runs compare static FIFO, non-preemptive LIFO, a hybrid that takes seven of every ten jobs from the tail and three from the head, and a tabular Q-learning agent that selects among those three once per second. Eight servers and exponential service of mean 40 ms are used. Below capacity the agent stays on FIFO and FoS is 100%. At 250 requests/s the agent reaches FoS 50.7%, between FIFO at 19.0% and the static hybrid at 59.4%, with a shorter maximum wait than the hybrid. Losses are zero. No significance test is reported.*

KEYWORDS: *QoS, Age of Information, Peak AoI, Freshness of Service, FoS, FIFO, LIFO, Head-of-Line blocking, bursty traffic*

DOI: https://doi.org/10.46687/MT26DIS

ОТ КЛАСИЧЕСКИ QOS КЪМ AGE OF INFORMATION И FRESHNESS OF SERVICE В РАЗПРЕДЕЛЕНИ АСОИУ

ДРАГОМИР И. ВАСИЛЕВ, СРЕБРИН В. ШАРБАНОВ

АБСТРАКТ: *Разпределените АСОИУ буферират заявки при пулсиращ трафик, а средното време за отговор не описва свежестта при получателя. Статията припомня Age of Information за M/M/1 FIFO при статус-обновяване и натоварването около ρ≈0,531, което минимизира средната възраст само в този модел. Freshness of Service е дял на завършилите заявки с чакане под проектен праг, отделно от AoI и от отказите. Пет прогона с краен хоризонт сравняват статични FIFO, непрекъсващ LIFO, хибрид със седем изваждания от края и три от началото и табличен Q-learning, който на всяка секунда избира между тях, при осем обслужващи устройства и експоненциално обслужване 40 ms. Под капацитета агентът остава на FIFO и FoS е 100%. При 250 заявки/s агентът достига FoS 50,7%, между FIFO с 19,0% и статичния хибрид с 59,4%, с по-късо максимално чакане от хибрида. Загуби няма. Проверка за значимост няма.*

1 Въведение

Развитието на автоматизирани системи за обработка на информацията и управление (АСОИУ) е свързано с преход към микросервисни архитектури, cloud/edge изчисления и асинхронни потоци от данни [1], [2]. В ядрото на тези системи стоят изчислителни опашки на ниво API Gateway, балансьори и брокери. Начинът на обслужване определя не само класическите QoS показатели, но и актуалността на доставяната информация за управлявания обект.

В масовата практика доминира FIFO. При стационарен трафик FIFO е прост и справедлив. При пулсиращ (bursty) трафик моментната интензивност λ може многократно

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

да надхвърли капацитета $\boldsymbol{\mu}$. Опашката се запълва; новите заявки чакат зад стотици по-стари — Head-of-Line (HoL) блокиране [2], [3]. В системи за реално време стойността на информацията намалява с времето.

Това мотивира прехода от класически QoS към Age of Information (AoI), Peak AoI и Freshness of Service (FoS) за request–response среди [4], [5], [6].

2 Архитектура на АСОИУ и ролята на опашките

В разглежданите АСОИУ заявката минава през опашка, преди да бъде обслужена: на API шлюз, в балансьор или пред пул от работни нишки. От дисциплината на тази опашка зависят и класическите QoS показатели, и това колко актуални са данните при получателя. Същата схема се среща в индустриално управление, SCADA и телеметрия, както и в уеб услуги с променлив товар [7], [8].

През последното десетилетие част от тези системи се разделиха от един монолит към по-малки услуги, често пакетирани в контейнери [9], [10], [1], [7]. За управлението на опашката са достатъчни два начина на обмен:

1. Заявка–отговор. REST върху HTTP [11]. gRPC е RPC върху HTTP/2 [12], [13]. Междинен прокси (например Envoy в service mesh) може да добави още един буфер по пътя [14].

2. Събития. Производителят публикува в брокер, а потребителят чете по-късно. Типични реализации са Kafka, RabbitMQ и сходни опашки [15], [16], [17], [7].

Самият възел държи опашка в ядрото или в потребителското пространство (socket backlog, опашка на пула в JVM), за да не изчерпи нишките и връзките към базата при кратък пик [18], [2].

Класическите модели често приемат стационарен вход. В системите, които се разглеждат тук, трафикът е пулсиращ: по-дълги спокойни интервали и кратки пикове, в които моментното $\boldsymbol{\lambda}$ надхвърля $\boldsymbol{\mu}$ [19], [20]. Пикът идва от сензори, които предават заедно [21], от масово потребителско събитие или от повторни опити. Ако вътрешен ресурс забави отговора, клиентът праща заявката отново и опашката на шлюза расте допълнително [7].

На входа често се ограничава скоростта. Leaky bucket изглажда пика с цената на изчакване за всяка заявка. Token bucket пропуска кратък пик и го прехвърля към опашката на услугата.

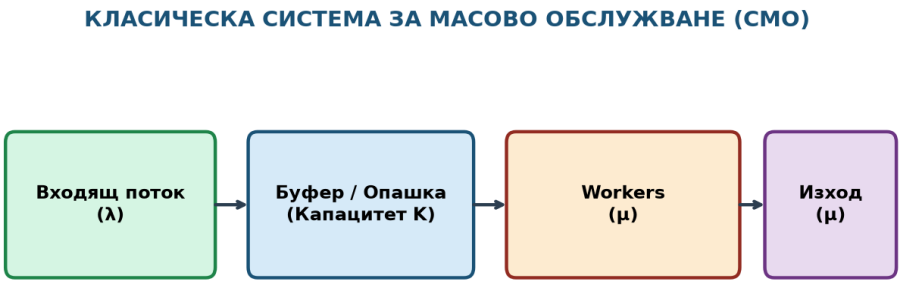
След шлюза подразбираната дисциплина е FIFO. Новата заявка чака зад по-старите. Това е блокиране на главата на линията (Head-of-Line blocking — HoL) [22]. За телеметрия или състояние на процес закъснението прави данните по-малко полезни: клиентът затваря връзката по таймаут, а сървърът довършва работа, чийто резултат вече не се използва.



Фиг. 1. Блокиране на главата на линията (HoL) при FIFO.

3 Класически модели и дисциплини

Теорията на масовото обслужване (Queueing Theory) се явява фундаменталният математически апарат за анализиране на процесите на чакане и обработка в изчислителните и телекомуникационни мрежи. Една класическа система за масово обслужване (СМО) се състои от три основни компонента: входящ поток от заявки с интензивност λ, буферна памет (опашка) с максимален капацитет K и обслужващи канали (workers) с обща интензивност на обслужване μ (Фиг. 2).



Фиг. 2. Класическа структура на система за масово обслужване.

Математическото описание на тези системи използва разширената нотация на Кендъл $\boldsymbol{A/S/c/K/N/D}$ [2], [23], [24]. В литературата редът на последните символи варира; тук той е този:

$$\boldsymbol{A/S/c/K/N/D}$$

D е дисциплината на обслужване. За сравнението на FIFO, LIFO и хибрида тя се обсъжда отделно от A, S, c, K и N, но остава шестият символ на нотацията. Буквата D вътре в A означава детерминиран интервал между пристигания и не е дисциплината. Останалите значения са:

- A е разпределението на интервалите между пристиганията (M означава експоненциално разпределени интервали, еквивалентно на Поасонов входящ поток; D — детерминирани интервали; G — общо разпределение).
- S е разпределението на времето за обслужване (M — експоненциално, D — константно, G — общо).
- c е броят на паралелните обслужващи устройства.
- K е максималният брой заявки в системата (опашка и обслужване). По подразбиране $K = \infty$.
- N е размерът на източниковата популация. По подразбиране $N = \infty$ (отворена система).

Едноканални системи за масово обслужване (M/M/1)

В класическия модел $M/M/1$, заявките пристигат по Поасонов закон с интензивност λ, а времето за обслужване се подчинява на експоненциално разпределение с параметър μ. Опашката е с неограничен капацитет, а дисциплината е FIFO. Коефициентът на натоварване (интензивност на трафика) се дефинира като:

$$\rho = \frac{\lambda}{\mu} \quad (1)$$

За да бъде системата стабилна и да не нараства опашката неограничено, трябва да е изпълнено условието $\rho < 1$ [25], [3], [26], [27].

В стационарен режим при $\boldsymbol{\rho < 1}$ стандартните средни за $\boldsymbol{M/M/1}$ с FIFO са $\boldsymbol{L = \rho/(1-\rho)}$, $\boldsymbol{L_q = \rho^2/(1-\rho)}$, $\boldsymbol{W = 1/(\mu-\lambda)}$ и $\boldsymbol{W_q = \rho/(\mu-\lambda)}$ [28], [25], [3], [29]. Законът на Литъл $\boldsymbol{L = \lambda W}$ се прилага към същата система; при откази $\boldsymbol{\lambda}$ е интензивността на приетите заявки, а граничният преход важи, когато границите съществуват [30]. При $\boldsymbol{c}$ канала капацитетът е $\boldsymbol{c\mu}$.

Многоканални системи за масово обслужване (M/M/c)

В реалните АСОИУ обработката на заявки се извършва паралелно от пул от работни нишки (Thread Pool), което се моделира математически като многоканална система $M/M/c$ [31] с c обслужващи устройства [25], [2]. Общата интензивност на натоварване в този случай е:

$$\boldsymbol{\rho = \frac{\lambda}{c \cdot \mu}} \quad (2)$$

Системата е стабилна при $\rho < 1$.

Вероятността заявка да чака при $\boldsymbol{M/M/c}$ с неограничена опашка и $\boldsymbol{\rho < 1}$ се дава от формулата на Ерланг-С, а средното чакане е $\boldsymbol{W_q = P_Q/(c\mu(1-\rho))}$ [32], [25]. Пълният израз е стандартен и не се възпроизвежда.

Влияние на вариацията на обслужването: Модел M/G/1

В реалните софтуерни системи времето за обработка на заявка рядко е чисто експоненциално (Марковско). То зависи от сложността на заявката, мрежовите забавяния към базите данни и кеширането, придобивайки произволно разпределение с математическо очакване $\mathbb{E}[S] = 1/\mu$ и дисперсия σ_S^2. Този случай се описва чрез модела $M/G/1$ [2], [3].

При $\boldsymbol{M/G/1}$, Поасонов вход, FIFO, независимо обслужване и $\boldsymbol{\rho < 1}$ средното чакане расте с квадрата на коефициента на вариация на обслужването (формула на Полачек–Хинчин) [33], [3], [34]. От формулата не следва, че пулсиращият вход на прототипа е $\boldsymbol{M/G/1}$.

Тежкоопашати продължителности на процеси са отчетени за Unix натоварване при динамично балансиране [35]. От тази работа не следва, че същото е измерено свойство на всяка база данни.

Сравнение на опашковите дисциплини

Изборът на дисциплина на обслужване определя разпределението на времето за изчакване между отделните заявки [2], [23]. В Таблица 1 сложността е за едно добавяне или едно изваждане при структура с достъп до двата края за постоянно време, например deque. Тя не е свойство на дисциплината сама по себе си. Основните дисциплини са представени [36] в таблицата:

- FIFO (First-In-First-Out): Обслужва по ред на пристигане и запазва този ред. Не дава еднакво чакане на всички заявки: чакането зависи и от дължината на обслужване на предните задачи. При пик новите заявки стоят зад по-старите (HoL) [2], [22].
- LIFO (Last-In-First-Out): Обслужва най-новата чакаща заявка и при непрекъсващо обслужване не прекъсва заявката, която вече се изпълнява, така че новата може да чака заради текущата работа. В редица модели за статус-актуализации LIFO намалява AoI на успешно доставените пакети спрямо FIFO [6], [37], [38], но при

REST клиентът чака отговора на своята заявка и резултатът не се пренася. Стара заявка може да чака дълго и при $\rho < 1$. При $\rho \geq 1$ стандартната система $M/G/1$ не е устойчива и няма стационарно разпределение на дължината и на чакането [2]; от това не следва нито монотонен растеж във всеки момент, нито неограничена дисперсия при всяка дисциплина.

- SRPT (Shortest Remaining Processing Time): Винаги обслужва заявката с най-кратко оставащо време и допуска прекъсване. При известни размери минимизира средния престой [39], [40]. В уеб сървър размерът обикновено не е известен преди изпълнението, затова SRPT остава ориентир, а не директна политика за REST заявки.

Processor Sharing (PS): Дели капацитета поравно между активните заявки (всеки от N получава $1/N$ от μ). Това е теоретичен модел на времеделение [41], [42]. Сложността не е свойство на дисциплината: наивна реализация с преглед на всички активни заявки е $O(N)$, а конкретният оверхед зависи от структурата от данни.

Таблица 1. Представяне на основните дисциплини

Дисциплина	Добавяне и изваждане	Риск от гладуване	Защита от HoL	Основна област
FIFO	$O(1)$ при deque	нисък при стабилен режим	няма	транзакции, бази данни
LIFO	$O(1)$ при deque	има и при $\rho < 1$	сред чакащите, без прекъсване	статус-актуализации
SRPT	$O(\log N)$ при известен размер	за дългите задачи	при прекъсване	CPU с известен размер
Processor Sharing	зависи от реализацията	ограничен от дяла $1/N$	има	времеделение

FIFO и LIFO са крайности: първата пази реда, но при пик задържа новите заявки; втората обслужва новите първи, но може да остави старите без практическа горна граница. В постановката на модела третото действие е хибрид върху една опашка с вход винаги в края: на всеки десет изваждания седем са от края и три от началото. Това не са две отделни опашки. Името Dual-Queue по-нататък означава същия хибрид като действие на агента; Dual Queue при De Schepper и съавтори е друга архитектура и се разграничава в свързаните работи. Агентът избира между FIFO, LIFO и този хибрид според състоянието на опашката.

4 От латентност към AoI и FoS

В класическия софтуерен инженеринг и мрежово проектиране качеството на обслужването се измерва с т.нар. QoS (Quality of Service) показатели [43]:

- Латентност на мрежата (Network Latency): Времето за физически транспорт на данни.
- Време за реакция на сървъра (Server Response Time): Общото време, изминало от получаването на заявката до връщането на отговора.
- Пропускателна способност (Throughput): Скоростта на обработка на транзакции.

Тези показатели описват колко бързо се пренася и обслужва заявката. По-надолу „чакане“ е времето в опашката W, а „време за отговор“ е $W + S$. Думата „латентност“ се ползва само за този QoS смисъл, не като име на AoI. Показателите не описват колко стара е информацията при получателя [6], [4].

Възраст на информацията (Age of Information — AoI)

За дефиниране на актуалността на данните около 2011–2012 г. Kaul, Yates и Gruteser въвеждат концепцията за Възраст на информацията (Age of Information — AoI) [4], [44], [5], [45]. По-късни обзори и монографии разширяват теорията и приложенията [46], [47], [6], [48], [49], [50].

Нека източникът периодично генерира пакети с информация в моменти $\boldsymbol{t_1, t_2, \dots, t_i, \dots}$. Всеки пакет съдържа времеви печат на генериране. Тези пакети се предават през мрежа с опашка и се доставят на получателя в моменти $\boldsymbol{t'_1, t'_2, \dots, t'_i, \dots}$.

Текущото знание на получателя се определя от последното успешно доставено съобщение към момент $\boldsymbol{t}$. При допускане, че пакетите се доставят в реда на генериране, индексът на това съобщение може да се запише като:

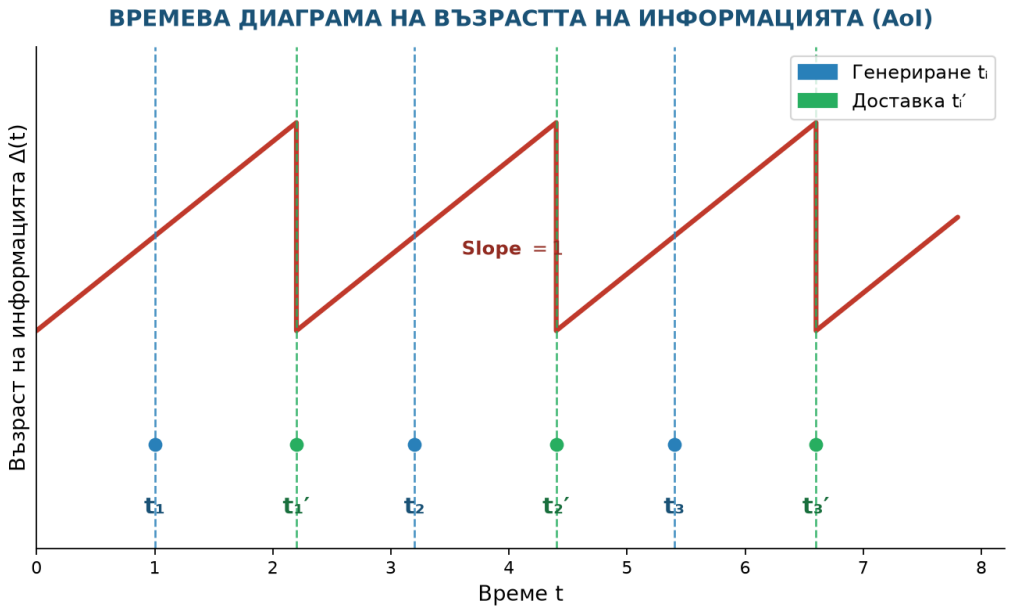
$$\boldsymbol{N(t) = \max\{\, i : t'_i \le t \,\}} \tag{3}$$

При доставка извън ред индексът е аргументът на максимума на печата за генериране сред вече доставените пакети. Времевият печат на генериране на това съобщение е $U(t) = t_{N(t)}$. Тогава Възрастта на информацията $\Delta(t)$ в момент t се дефинира като:

$$\boldsymbol{\Delta(t) = t - U(t)} \tag{4}$$

Математическото изменение на AoI във времето има триъгълен (sawtooth) характер (Фиг. 3):

Между доставките възрастта нараства линейно с наклон 1. В момента на доставка $\boldsymbol{t'_i}$ тя пада до престоя на пакета, $\boldsymbol{t'_i - t_i}$.



Фиг. 3. Времево изменение на Възрастта на информацията (AoI).

За $\boldsymbol{M/M/1}$ при FIFO, Поасонов вход, експоненциално обслужване и стационарен режим $\boldsymbol{\rho < 1}$ средното AoI е изведено от Kaul, Yates и Gruteser [4]:

$$\mathbb{E}[\boldsymbol{\Delta}] = \frac{\mathbf{1}}{\boldsymbol{\mu}}\left(\mathbf{1} + \frac{\mathbf{1}}{\boldsymbol{\rho}} + \frac{\boldsymbol{\rho}^{\mathbf{2}}}{\mathbf{1}-\boldsymbol{\rho}}\right) \tag{5}$$

Това уравнение разкрива фундаментална зависимост (Фиг. 3): минималната възраст на информацията не се постига при екстремно ниско или екстремно високо натоварване.

- При ниско натоварване ($\rho \to 0$) закъснението на пакетите в опашката е минимално, но интервалът между генерирането на пакети е много голям, което води до остаряване на информацията на получателя поради липса на нови съобщения.
- При високо натоварване ($\rho \to 1$) пакетите се генерират често, но изпитват огромно закъснение поради престоя им в препълнената FIFO опашка.
- Математическият минимум на средното AoI за $M/M/1$ FIFO система се постига при оптимално натоварване:

$$\rho_{\text{opt}} \approx 0{,}531$$

Стойността е корен на уравнението, получено в същата работа при диференциране на формулата по ρ [4]. Обзорът на Yates и съавтори предава същия израз и същия минимум [47]. Обзорът на Kosta, Pappas и Angelakis остава източник за рамката на AoI, не заместител на този извод [6].

Минимумът се вижда и с пряко заместване. Нека се означи

$$\boldsymbol{g(\rho)} = \mathbf{1} + \frac{\mathbf{1}}{\boldsymbol{\rho}} + \frac{\boldsymbol{\rho}^{\mathbf{2}}}{\mathbf{1}-\boldsymbol{\rho}} \tag{6}$$

така че $\mathbb{E}[\Delta] = g(\rho)/\mu$ при $\rho < 1$. Числата в Таблица 2 са стойности на тази формула, не измервания.

Таблица 2. Средно AoI за M/M/1 FIFO по формулата на Kaul, Yates и Gruteser. $\mu = 25\ \text{s}^{-1}$ отговаря на средно обслужване 40 ms на едно устройство.

ρ	$g(\rho) = \mu\,\mathbb{E}[\Delta]$	$\mathbb{E}[\Delta]$ **при** $\mu = 25\ \text{s}^{-1}$
0,2	6,05	0,24 s
0,4	3,77	0,15 s
0,5	3,50	0,14 s
0,531	3,48	0,14 s
0,7	4,06	0,16 s
0,9	10,21	0,41 s

Около $\boldsymbol{\rho = 0{,}5}$ кривата е плоска: $\boldsymbol{g(0{,}5) = 3{,}50}$ и $\boldsymbol{g(0{,}531) = 3{,}48}$. Малко отклонение от „оптималното“ натоварване почти не мести средната възраст. При $\boldsymbol{\rho = 0{,}9}$ членът $\boldsymbol{\rho^2/(1-\rho)}$ вече доминира и средната възраст е около три пъти по-голяма, отколкото в минимума. $\boldsymbol{\mu = 25\ \text{s}^{-1}}$ е само мащаб за едно устройство. Прототипът работи с няколко паралелни канала, затова таблицата не е прогноза за неговите опити.

За подобряване на свежестта се въвеждат т.нар. политики за управление на пакети (Packet Management) [37]. Ако в опашката се поддържа капацитет $\boldsymbol{K = 1}$ и пристигането на нов пакет изхвърля стария необслужен пакет от буфера, средното AoI се подобрява значително при високо натоварване. Този подход обаче води до загуба на транзакции, което е недопустимо при системи, изискващи надеждна доставка на съобщения.

Пикова възраст на информацията (Peak Age of Information — PAoI)

Освен средния AoI се следи и стойността му непосредствено преди следващата доставка. За тази цел се използва пикова възраст на информацията (Peak AoI — PAoI) [6], [37].

При доставка в реда на генериране $\boldsymbol{t_i'}$ е моментът на доставяне на пакет $\boldsymbol{i}$, а $\boldsymbol{t_{i-1}}$ е моментът на генериране на предишния пакет. Пиковата възраст непосредствено преди тази доставка е [37]:

$$\boldsymbol{A_i = t_i' - t_{i-1}} \tag{7}$$

Това не е глобалният максимум на $\Delta(t)$ за целия период. Записът следва дефиницията на Costa, Codreanu и Ephremides за пика преди приемане на поредното обновяване [37]; обзорът на Kosta, Pappas и Angelakis я предава в същия вид [6]. Сама по себе си метриката не дава гаранция за време на реакция.

Свежест на обслужването (Freshness of Service — FoS)

В стандартна система заявка–отговор без печат за момента на генериране на данните AoI не се смята само от чакането на заявката. Ако такива печати има, AoI се дефинира и там. Затова тук FoS е допълващ оперативен показател, не заместител на AoI.

FoS е процентният запис на оценката за вероятността чакането да е под прага сред заявките, които са завършили и имат известно $\boldsymbol{W}$. Оценява се случайната величина $\boldsymbol{W}$, не отделното наблюдение. Отхвърлените не влизат в тази сума:

$$\widehat{\mathrm{P}}(\mathrm{W} < \mathrm{T}) = \frac{1}{\mathrm{n_{done}}} \sum_{\mathrm{i=1}}^{\mathrm{n_{done}}} 1\{\mathrm{W_i} < \mathrm{T}\} \tag{8}$$

$$\mathrm{FoS(T)} = 100\% \cdot \widehat{\mathrm{P}}(\mathrm{W} < \mathrm{T}) \tag{9}$$

Загубите са отделен дял:

$$\boldsymbol{\widehat{P}_{loss} = \frac{n_{rej}}{n_{arr}}} \tag{10}$$

където:

- n_{done} е броят завършили заявки с известно чакане; заявка, която още чака в края на интервала, не влиза, защото W_i не е известно;
- n_{arr} е броят пристигнали към опашката, а n_{rej} е броят отхвърлени при пълен буфер;
- W_i е времето за изчакване на завършила заявка i в опашката (не общото време за отговор $R_i = W_i + S_i$);
- T е предварително зададеният праг;
- $\mathbf{1}\{\cdot\}$ е индикаторна функция.

Няма една скала, която да събере FoS и загубите. Ефективността е наборът: FoS сред завършилите, $\hat{P}_{\mathrm{loss}}$, средно чакане, P95 и P99 на чакането, време за отговор $W + S$ и пропускателна способност.

Оценката е само върху завършилите. При прекъснато наблюдение тя може да е пристрастна: най-дълго чакащите често са още в опашката и отпадат от $\boldsymbol{n_{done}}$, така че FoS изглежда по-добър. При експеримент генерацията е за фиксиран период, след което има време за довършване на приетите заявки. Незавършените към края се броят отделно и не се крият в знаменателя на FoS.

За проектен праг е избран $\boldsymbol{T = 1\,s}$ за уеб-ориентирани API. Този избор не следва от Google Core Web Vitals. Interaction to Next Paint (INP) мери колко бързо страницата отговаря

визуално на кликване, докосване или клавиш, до следващото изрисуване. По документацията към 2 септември 2025 г. стойност до $\mathbf{200\,ms}$ се води добра, а над $\mathbf{500\,ms}$ — лоша [51]. Това е браузърна интерактивност, не чакане в backend опашка. Чувствителността към други стойности на $\boldsymbol{T}$ (напр. $\mathbf{100\,ms}$, $\mathbf{500\,ms}$, $\mathbf{1\,s}$) остава за експерименталната проверка.

$\widehat{\boldsymbol{P}}(\boldsymbol{W} < \boldsymbol{T})$ е оценката по завършилите заявки, а FoS($\boldsymbol{T}$) е същата величина в проценти. Тя не мери времето за отговор $\boldsymbol{W_i + S_i}$, не включва отхвърлените и не замества AoI. Името не е принос. Търсенето в края на главата не установява, че употребата на този дял за избор на дисциплина е нова. Самата дефиниция не показва, че такъв избор е по-добър от FIFO.

В Таблица 3 е представен сравнителен анализ на характеристиките на разгледаните метрики за оценка на времевите показатели на информационните потоци.

Таблица 3. Сравнителен анализ на характеристиките на разгледаните метрики за оценка на времевите показатели на информационните потоци.

Метрика	Формална дефиниция	Фокус на измерване	Предимства	Недостатъци / Ограничения
Време за отговор	$R_i = W_i + S_i$	опашка и обслужване	лесно за измерване	не е мрежова латентност и не отчита възрастта на данните
AoI	$t - U(t)$	Свежест при получателя	Улавя динамиката на обновяване	Изисква непрекъснато следене
Peak AoI	$t_i' - t_{i-1}$	пик преди поредната доставка	удобна за пикове	не е глобалният максимум на $\Delta(t)$
Freshness of Service	$\hat{P}(W < T)$	Дял на навременните заявки	Оперативно приложима в request–response API	Зависи от избора на прага T

Три записа изглеждат близки до FoS и не са едно и също нещо. Разликата е в часовника и във въпроса, който числото задава (Таблица 4).

Таблица 4. FoS и близките показатели.

Показател	Въпрос	Часовник	Връзка с FoS
Срок върху чакането	какъв дял има $W < T$	опашка	съвпада с FoS при същия T
Срок върху отговора	какъв дял има $W + S$ под праг	опашка и обслужване	не е FoS
P99 на чакането	под какъв праг попадат 99%	опашка	квантил, не дял под фиксиран T
AoI	колко е стара последната доставка	генерация и доставка	иска статус-поток
FoS(T)	$\hat{P}(W < T)$ по извадката	опашка	$100\% \cdot \hat{P}(W < T)$

Ако даден срок е положен върху същото чакане $\boldsymbol{W}$ и прагът е същият, дялът навреме е FoS. Няма отделна теорема в съвпадението. Разликата се появява, когато срокът мери

времето за отговор $\boldsymbol{W_i + S_i}$: заявката може да изчака малко и после да се обработва дълго. Тогава тя минава прага на FoS и пропуска срока за отговор.

P99 е квантил. Той отговаря къде по оста на чакането се събират 99% от заявките. FoS($\boldsymbol{T}$) отговаря какъв дял стои вляво от избран праг, например $\mathbf{1\,s}$. От едното число не се възстановява другото, ако няма цялата крива на разпределението [43].

AoI иска печат на генериране и печат на доставка и строи процеса $\boldsymbol{\Delta(t)}$ при получателя [4], [45]. FoS иска само чакането на заявката в опашката. Затова се смята в заявка–отговор без постоянен поток от обновявания. Не казва на каква възраст е последната успешно приета информация.

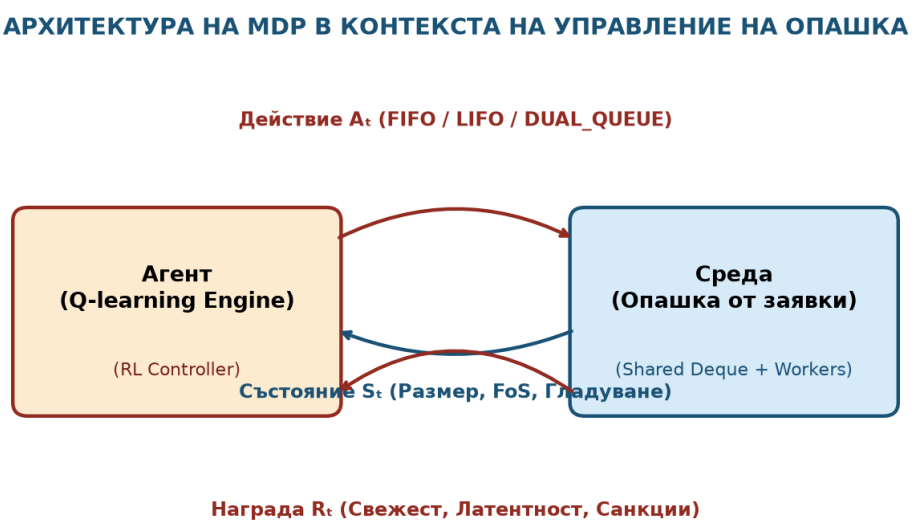
Честотата по $\boldsymbol{n}$ завършили заявки е оценка в извадка. Тя се доближава до стационарна вероятност, когато процесът е стабилен и прозорецът е дълъг [43]. При претоварване или при откази от пълен буфер в сумата влизат само заявките, които изобщо са наблюдавани. Тогава FoS описва тази извадка, не произволна траектория на системата.

FoS не е успешност на системата. Ако отхвърлените при пълен буфер заявки не влизат в $\boldsymbol{n}$, делът сред приетите може да е висок, докато голяма част от входа се губи. До него следва да се отчитат поне четири неща: FoS($\boldsymbol{T}$) само сред приетите заявки; дял отхвърлени или загубени; средно чакане и P95/P99 на чакането; време за отговор $\boldsymbol{W + S}$ и пропускателна способност. Само първото число не описва системата.

5 Обучение с подкрепление като контекст

Сложността и нестационарността на трафика в съвременните АСОИУ налагат прилагането на методи от изкуствения интелект, по-специално обучение с подкрепление (Reinforcement Learning — RL) [52].

Обучението с подкрепление се моделира чрез математическата рамка на Марковските процеси на вземане на решения (Markov Decision Process — MDP). Един MDP процес се дефинира като кортеж [53] от състояния, действия, вероятности за преход, функции на наградата и дисконтов фактор (Фиг. 4) [54]:



Фиг. 4. MDP рамка за управление на опашкова дисциплина.

- S е пространството от състояния на опашката.
- A е пространството от възможни действия: FIFO, LIFO или хибридът Dual-Queue (седем изваждания от края и три от началото върху една опашка).
- $P(s' \mid s, a)$ е вероятностната функция за преход на средата в ново състояние s' след прилагане на действие a в състояние s.
- $R(s, a)$ е функцията на наградата (Reward Function), която количествено оценява качеството на избраното действие.
- γ е дисконтовият фактор за бъдещите награди ($\gamma \in [0,1)$).

Целта на агента е стратегия, която максимизира очакваната дисконтирана награда. Оптималната стойност удовлетворява уравнението на Белман [55], [54]. Вероятностите за преход при променлив вход не са известни, затова се използва безмоделен Q-learning на Watkins [56], [57].

При внедряване на RL алгоритми за управление на процеси в реално време, проектантите се сблъскват с избора между табличен Q-learning и дълбоко обучение с подкрепление (Deep Q-Networks — DQN) [58], [59], [60]. Сравнителният анализ на двата подхода е представен в Таблица 5:

Таблица 5. Сравнителен анализ на двата подхода

Критерий за сравнение	**Табличен Q-learning**	**Дълбоко обучение с подкрепление (DQN)**
Математическо представяне	Таблица $Q(S, A)$ в оперативната памет	Дълбока невронна мрежа $Q(s, a; \theta)$
Мащабируемост	малко дискретно S	по-голямо пространство от състояния; действията остават дискретни
Изчислителна сложност	обръщение към таблица с фиксиран размер	права стъпка през мрежа
Време за решение	зависи от език, процесор и размер на таблицата; не се приема за универсална константа	също зависи от реализацията; GPU не е задължителен
Риск от разходимост	класически условия за сходимост	възможна нестабилност на обучението
Кога е уместен	малко дискретно пространство от състояния и дискретни действия	по-голямо или високомерно пространство от състояния при дискретни действия; непрекъснати действия изискват друг алгоритъм

Табличният Q-learning е уместен, когато състоянията и действията са малко и дискретни. За модела по-нататък пространството е декартовото произведение на трите признака от Таблица 6, общо 18 състояния. Времето за обръщение към таблицата зависи от реализацията. DQN остава вариант при по-богато наблюдение и при дискретни действия [58], [59], [60].

Кодовете в Таблица 6 отделят интервала от измерената величина: $\boldsymbol{q}$ е код за броя чакащи $\boldsymbol{Q}$, а $\boldsymbol{f}$ е код за процента FoS, не самият процент. FoS за състоянието се смята върху плъзгащ прозорец от $\mathbf{10\,s}$, а наблюдението се взема в края на епоха от $\mathbf{1\,s}$. Колко завършили заявки трябват в прозореца, за да се приеме оценката, остава параметър на експеримента.

В модела действието се избира веднъж на епоха и важи за целия пул. Когато чакането на главата надхвърли $\mathbf{3000\,ms}$, избраният LIFO се заменя с хибрида, въведен при сравнението на дисциплините. Наградата отчита FoS, средното забавяне и максималното

чакане; делът на отхвърлените се води отделно. Наградата и предпазителят се формализират отделно от този обзор.

Таблица 6. Кодове на признаците. $|\mathrm{S}| = 3 \cdot 3 \cdot 2 = 18$ комбинации, без изключени.

Признак	Код	Условие
дължина на опашката Q (брой чакащи, не размер на заявката)	$q = 0$	$Q \leq 5$
	$q = 1$	$5 < Q \leq 50$
	$q = 2$	$Q > 50$
FoS	$f = 0$	$\mathrm{FoS} < 30\%$
	$f = 1$	$30\% \leq \mathrm{FoS} < 80\%$
	$f = 2$	$\mathrm{FoS} \geq 80\%$
индикатор за гладуване	$s_{\mathrm{flag}} = 0$	$\mathrm{MaxWait} \leq 3000\,\mathrm{ms}$
	$s_{\mathrm{flag}} = 1$	$\mathrm{MaxWait} > 3000\,\mathrm{ms}$

Свързани резултати за опашка и възраст на информацията

Kaul, Yates и Gruteser определят колко често източникът да подава обновяване към $\boldsymbol{M/M/1}$ с FIFO [4]. Оптимумът около $\boldsymbol{\rho \approx 0,531}$ е за този модел и засяга интензивността на генериране, не дисциплината на сървъра. В последваща работа същите автори показват, че при опашка от статуси LIFO може да държи по-ниско AoI, защото новото обновяване обезценява чакащото старо [45]. REST заявка не носи това допускане: клиентът чака отговора на своето повикване.

Costa, Codreanu и Ephremides намаляват AoI, като изхвърлят или заменят остарял пакет в буфера [37]. Когато доставката не бива да се губи, същата операция е загубена заявка. Sun и съавтори решават при семплера дали да се изпрати нова проба, или да се изчака [48]. Kadota и съавтори избират кой възел да предаде в безжична мрежа [49], Talak, Karaman и Modiano добавят ограничения от интерференция [38], а Bedewy, Sun и Shroff разглеждат обслужване на последно генерирания пакет първи, включително през повече от един хоп [50]. Yates и Kaul дават възрастта при много източници [5]. Обзорите събират тази линия [46], [47], [6].

Общата им мярка е възраст при получателя, а новото обновяване замества старото. Тук мярката е дял на заявките с чакане под праг, старото повикване не се изхвърля, а изборът е между три дисциплини върху една опашка при неизвестен вход. Затова изброените резултати не се пренасят като готова политика за API опашка. Сравнението не установява, че комбинацията е единствена в литературата.

Altman, Ayesta и Prabhu анализират балансиране между сървъри с processor sharing [61], а Gupta и Harchol-Balter дават самонастройващ се прием на заявки [62]. И двете работи са за опашки без обучение с подкрепление. Ограниченията в обучението се цитират по Achiam и съавтори [63] и по обзора на García и Fernández [64]. Името Dual Queue при De Schepper, Albisser, Tilmans и Briscoe означава две опашки за L4S и класически TCP с общ капацитет [65], не превключване между FIFO и LIFO.

6 Постановка и числено сравнение

От обзора следват три неща.

1. При пик FIFO задържа новите заявки зад по-старите. Чистият LIFO съкращава чакането на новите, но може да остави старите без практическа горна граница.

2. FoS(T) е дял на завършилите заявки с чакане под праг. Отказите и още чакащите се броят отделно. Показателят не замества AoI и сам по себе си не показва полза от управление.
3. Към трите статични дисциплини е добавен табличен Q-learning, който на всеки 1 s избира една от тях. Предпазителят заменя LIFO с хибрида, ако главата чака над 3 s.

Сравнението е симулация на една опашка с $c = 8$ обслужващи устройства и експоненциално обслужване със средно 40 ms, така че капацитетът е 200 заявки/s. Входът е Поасонов. Генерацията трае 20 s, след което приетите заявки се довършват. Опашката е безкрайна. FoS е дял на завършилите с чакане под 1 s. Хибридът на всеки десет изваждания взема седем от края и три от началото. Четвъртият ред е табличен Q-learning: на всеки 1 s избира между трите дисциплини по 18-те състояния от модела, с априорна таблица, $\alpha = 0{,}1$, $\gamma = 0{,}9$ и $\varepsilon = 0{,}05$. Ако избраният LIFO завари глава с чакане над 3 s, той се заменя с хибрида. Обучението е вътре в прогона, не върху предварителна извадка. Направени са пет независими прогона. Няма проверка за статистическа значимост. Таблица 7 дава средните.

Таблица 7. Средни от пет прогона. Загуби няма. При еднакво λ броят завършили съвпада, затова пропускателната способност не разделя редовете. Средното време за отговор е средното чакане плюс средното обслужване и също не ги разделя.

λ (req/s)	Дисциплина	FoS (%)	Средно чакане (ms)	P99 (ms)	Макс. чакане (ms)
100	FIFO	100,0	0,7	21,2	47,8
100	LIFO	100,0	0,7	20,2	84,1
100	хибрид	100,0	0,7	20,9	71,4
100	агент	100,0	0,7	21,3	47,8
150	FIFO	100,0	7,6	64,9	96,4
150	LIFO	100,0	7,2	142,2	427,2
150	хибрид	100,0	7,3	114,1	193,7
150	агент	100,0	7,6	66,5	99,5
200	FIFO	100,0	229,6	506,8	540,2
200	LIFO	96,6	235,7	7496,3	14343,3
200	хибрид	90,9	231,6	1543,3	1735,6
200	агент	92,1	227,5	1690,5	1867,7
250	FIFO	19,0	2556,5	4968,4	5025,1
250	LIFO	80,3	2575,7	23652,1	24844,9
250	хибрид	59,4	2597,6	11370,5	11639,4
250	агент	50,7	2556,9	7752,2	7835,6

При $\boldsymbol{\lambda = 100}$ и $\mathbf{150}$ FoS е $\mathbf{100}\%$ и в петте прогона. Агентът избира почти само FIFO: средно $\mathbf{20,2}$ и $\mathbf{20,4}$ епохи FIFO срещу $\mathbf{0,6}$ хибрид. При $\boldsymbol{\lambda = 200}$ FIFO държи FoS $\mathbf{100}\%$. Агентът вече дели епохите, средно $\mathbf{11,6}$ FIFO и $\mathbf{8,6}$ хибрид, и FoS пада до $\mathbf{92,1}\%$ (от $\mathbf{86,2}$ до $\mathbf{100}$). При $\boldsymbol{\lambda = 250}$ средният FoS е $\mathbf{19,0}\%$ за FIFO, $\mathbf{50,7}\%$ за агента (от $\mathbf{49,4}$ до $\mathbf{53,2}$), $\mathbf{59,4}\%$ за хибрида и $\mathbf{80,3}\%$ за LIFO. Максималното чакане е около $\mathbf{5,0\,s}$, $\mathbf{7,8\,s}$, $\mathbf{11,6\,s}$ и $\mathbf{24,8\,s}$. Агентът избира средно $\mathbf{6,8}$ епохи FIFO, $\mathbf{0,4}$ LIFO и $\mathbf{18,4}$ хибрид. Предпазителят се

включва средно $\mathbf{0,4}$ пъти, защото LIFO почти не се избира. При $\boldsymbol{\rho \geq 1}$ числата са за краен хоризонт с довършване, не за стационарен режим.

7 Заключение

Обзорът отделя средното време за отговор от възрастта на данните при получателя и записва FoS като дял на завършилите заявки с чакане под праг, отделно от AoI и от отказите. Свързаните работи управляват статус, семплер или прием.

Предимството на хибрида Dual-Queue и на агента е смяната на дисциплината според товара. Под капацитета агентът остава на FIFO и FoS е $\mathbf{100}\%$. При $\boldsymbol{\lambda = 250}$ статичният хибрид и агентът вдигат FoS спрямо FIFO ($\mathbf{59,4}\%$ и $\mathbf{50,7}\%$ срещу $\mathbf{19,0}\%$) и скъсяват максималното чакане спрямо LIFO (около $\mathbf{11,6\,s}$ и $\mathbf{7,8\,s}$ срещу $\mathbf{24,8\,s}$). Агентът стои между FIFO и статичния хибрид, защото част от епохите остават FIFO. При тази смяна делът на завършилите с чакане под $\mathbf{1\,s}$ остава над дела на само FIFO, а максималното чакане остава под това на само LIFO.

Средното чакане при $\boldsymbol{\lambda = 250}$ остава около $\mathbf{2,6\,s}$ и при четирите реда. Броят завършили съвпада, затова пропускателната способност стои еднаква. При един фиксиран висок товар по FoS отпред е LIFO, а по къса опашка отпред е FIFO. Хибридът и агентът стоят между двете дисциплини: компромис при смяна на товара, а не общо подобрение по FoS, средно чакане и пропускателна способност едновременно. Загуби няма. Прогоните са пет, на краен хоризонт с довършване, без проверка за значимост.

ЛИТЕРАТУРА:

[1] Fowler, M. Microservices: a definition of this new architectural term. Martinfowler.com, 2014.

[2] Harchol-Balter, M. Performance Modeling and Design of Computer Systems: Queueing Theory in Action. Cambridge University Press, 2013.

[3] Kleinrock, L. Queueing Systems, Volume I: Theory. John Wiley & Sons, 1975.

[4] Kaul, S., Yates, R. & Gruteser, M. Real-time status: How often should one update? IEEE INFOCOM, 2731—2735, 2012. doi:10.1109/INFCOM.2012.6195689.

[5] Yates, R. D. & Kaul, S. K. The age of information: Real-time status updating by multiple sources. IEEE Transactions on Information Theory, 65(3), 1807—1827, 2019.

[6] Kosta, A., Pappas, N. & Angelakis, V. Age of information: A new concept, metric, and tool. Foundations and Trends in Networking, 12(3), 162—259, 2017.

[7] Newman, S. Building Microservices: Designing Fine-Grained Systems. O'Reilly Media, 2nd edition, 2021.

[8] Tanenbaum, A. S. & Van Steen, M. Distributed Systems: Principles and Paradigms. Pearson, 3rd edition, 2017.

[9] Burns, B., Grant, B., Oppenheimer, D., Brewer, E. & Wilkes, J. Borg, Omega, and Kubernetes. ACM Queue, 14(1), 70—93, 2016.

[10] Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R. & Safina, L. Microservices: yesterday, today, and tomorrow. In Present and Ulterior Software Engineering, Springer, 195—216, 2017.

[11] Fielding, R. T. Architectural Styles and the Design of Network-based Software Architectures. PhD dissertation, University of California, Irvine, 2000.

[12] gRPC Authors. gRPC: A high performance, open source universal RPC framework. grpc.io Documentation, 2024. Available: https://grpc.io/docs/

[13] Belshe, M., Peon, R. & Thomson, M. Hypertext Transfer Protocol Version 2 (HTTP/2). RFC 7540, IETF, 2015.

[14] Calcote, L. & Butcher, Z. Istio: Up and Running. O'Reilly Media, 2019.

[15] Kreps, J., Narkhede, N. & Rao, J. Kafka: a distributed messaging system for log processing. NetDB, 2011.

[16] Kleppmann, M. Designing Data-Intensive Applications. O'Reilly Media, 2017.

[17] Hohpe, G. & Woolf, B. Enterprise Integration Patterns. Addison-Wesley, 2003.

[18] Goetz, B., Peierls, T., Bloch, J., Bowbeer, J., Lea, D. & Holmes, D. Java Concurrency in Practice. Addison-Wesley Professional, 2006.

[19] Barford, P. & Crovella, M. E. Generating representative web workloads for network and server performance evaluation. Sigmetrics, 151—160, 1998.

[20] Crovella, M. E. & Bestavros, A. Self-similarity in World Wide Web traffic: evidence and possible causes. IEEE/ACM Transactions on Networking, 1996.

[21] Jiang, Z., Zhou, S. & Niu, Z. Optimal status update timeliness in massive IoT by elastic multiplexing. IEEE GLOBECOM, 1—7, 2018.

[22] Kurose, J. F. & Ross, K. W. Computer Networking: A Top-Down Approach Featuring the Internet. Pearson Education, 2013.

[23] Wierman, A. Scheduling for Today's Computer Systems: Bridging Theory and Practice. PhD thesis, Carnegie Mellon University, 2007.

[24] Kendall, D. G. Stochastic processes occurring in the theory of queues and their analysis by the method of the imbedded Markov chain. Annals of Mathematical Statistics, 24(3), 338—354, 1953.

[25] Gross, D. & Harris, C. M. Fundamentals of Queueing Theory. John Wiley and Sons, 3rd edition, 1998.

[26] Kingman, J. F. C. The single server queue in heavy traffic. Proceedings of the Cambridge Philosophical Society, 57(4), 902—904, 1961.

[27] Baccelli, F. & Brémaud, P. Elements of Queueing Theory. Springer, 2nd edition, 2003.

[28] Allen, A. O. Probability, Statistics, and Queueing Theory with Computer Science Applications. Academic Press, 2nd edition, 1990.

[29] Asmussen, S. Applied Probability and Queues. Springer, 2nd edition, 2003.

[30] Little, J. D. C. A proof of the queueing formula $L = \lambda \cdot W$. Operations Research, 1961.

[31] Kleinrock, L. Queueing Systems, Volume II: Computer Applications. John Wiley & Sons, 1976.

[32] Erlang, A. K. The theory of probabilities and telephone conversations. Nyt Tidsskrift for Matematik B, 20, 33—39, 1909.

[33] Pollaczek, F. Über eine aufgabe der wahrscheinlichkeitstheorie. Mathematische Zeitschrift, 32, 64-100, 1930.

[34] Khinchin, A. Y. Mathematical Methods in the Theory of Queueing. Griffin, London, 1960.

[35] Harchol-Balter, M. & Downey, A. B. Exploiting process lifetime distributions for dynamic load balancing. ACM Transactions on Computer Systems, 15(3), 253—285, 1997.

[36] Conway, R. W., Maxwell, W. L. & Miller, L. W. Theory of Scheduling. Addison-Wesley, 1967.

[37] Costa, M., Codreanu, M. & Ephremides, A. On the age of information in status update systems with packet management. IEEE Transactions on Information Theory, 62(4), 1897—1910, 2016.

[38] Talak, R., Karaman, S. & Modiano, E. Optimizing information freshness in wireless networks under general interference constraints. ACM MobiHoc, 2018.

[39] Bansal, N. & Harchol-Balter, M. Analysis of SRPT scheduling: investigating unfairness. Sigmetrics, 279—290, 2001.

[40] Schrage, L. E. & Miller, L. W. The queue M/G/1 with the shortest remaining processing time discipline. Operations Research, 14(4), 670—684, 1966.

[41] Aalto, S., Ayesta, U., Borst, S., Misra, V. & Núñez Queija, R. Beyond processor sharing. Performance Evaluation Review, 34(4), 36—43, 2007.

[42] Nuñez-Queija, R. Processor-sharing models for integrated-services networks. PhD thesis, Eindhoven University of Technology, 2000.

[43] Jain, R. The Art of Computer Systems Performance Analysis. John Wiley & Sons, 1991.

[44] Kaul, S., Gruteser, M., Rai, V. & Kenney, J. Minimizing age of information in vehicular networks. IEEE SECON, 350—358, 2011.

[45] Kaul, S., Yates, R. & Gruteser, M. Status updates through queues. Conference on Information Sciences and Systems (CISS), 2012.

[46] Sun, Y., Kadota, I., Talak, R. & Modiano, E. Age of Information: A New Metric for Information Freshness. Springer, 2019.

[47] Yates, R. D., Sun, Y., Brown, D. R., Kaul, S. K., Modiano, E. & Ulukus, S. Age of information: An introduction and survey. IEEE Journal on Selected Areas in Communications, 39(5), 1183—1210, 2021.

[48] Sun, Y., Uysal-Biyikoglu, E., Yates, R., Koksal, C. E. & Shroff, N. B. Update or wait: How to keep your data fresh. IEEE Transactions on Information Theory, 63(11), 7492—7508, 2017.

[49] Kadota, I., Sinha, A., Uysal-Biyikoglu, E., Singh, R. & Modiano, E. Scheduling policies for minimizing age of information in broadcast wireless networks. IEEE/ACM Transactions on Networking, 26(6), 2637—2650, 2018.

[50] Bedewy, A. M., Sun, Y. & Shroff, N. B. Minimizing the age of information through queues. IEEE Transactions on Information Theory, 65(8), 5215—5232, 2019.

[51] Google. Interaction to Next Paint (INP). web.dev, публикувано 6 май 2022, последно обновено 2 септември 2025. Available: https://web.dev/articles/inp (достъп на 17 октомври 2026).

[52] Sutton, R. S. & Barto, A. G. Reinforcement Learning: An Introduction. MIT Press, 2nd edition, 2018.

[53] Puterman, M. L. Markov Decision Processes: Discrete Stochastic Dynamic Programming. John Wiley & Sons, 1994.

[54] Bertsekas, D. Dynamic Programming and Optimal Control, Vol. 1 & 2. Athena Scientific, 3rd edition, 2005.

[55] Bellman, R. Dynamic Programming. Princeton University Press, 1957.

[56] Watkins, C. J. & Dayan, P. Q-learning. Machine Learning, 8(3-4), 279—292, 1992.

[57] Watkins, C. J. C. H. Learning from Delayed Rewards. PhD thesis, University of Cambridge, 1989.

[58] Mnih, V., Kavukcuoglu, K., Silver, D. et al. Human-level control through deep reinforcement learning. Nature, 518(7540), 529—533, 2015.

[59] Ceran, E. T., Gündüz, D. & György, A. A reinforcement learning approach to age of information in multi-user networks. IEEE PIMRC, 1967—1971, 2018.

[60] van Hasselt, H., Guez, A. & Silver, D. Deep reinforcement learning with double Q-learning. AAAI Conference on Artificial Intelligence, 2094—2100, 2016.

[61] Altman, E., Ayesta, U. & Prabhu, B. Load balancing in processor sharing systems. Telecommunication Systems, 47(1-2), 35—48, 2011.

[62] Gupta, V. & Harchol-Balter, M. Self-adaptive admission control policies for resource-sharing systems. ACM Sigmetrics, 311-322, 2009.

[63] Achiam, J., Held, D., Tamar, A. & Abbeel, P. Constrained policy optimization. International Conference on Machine Learning (ICML), 22—31, 2017.

[64] García, J. & Fernández, F. A comprehensive survey on safe reinforcement learning. Journal of Machine Learning Research, 16(1), 1437—1480, 2015.

[65] De Schepper, K., Albisser, O., Tilmans, O. & Briscoe, B. Dual queue coupled AQM: Deployable very low queuing delay for all. arXiv:2209.01078, 2022.

EXPERIMENTAL STUDY ON THE IMPACT OF DATA PREPROCESSING ON CLUSTERING QUALITY*

NELI A. ARABADZHIEVA-KALCHEVA

ABSTRACT: *The effects of feature scaling on K-Means and Ward's agglomerative clustering are examined using the Iris and Digits datasets. Original, standardized and Min–Max scaled features are compared by the Silhouette score, Davies–Bouldin index and Adjusted Rand Index (ARI). Across 12 experiments, standardization does not consistently improve clustering. On Digits, Ward's method applied to original features attains the best agreement with known classes (ARI = 0.794).*

KEYWORDS: *clustering; K-Means; hierarchical clustering; preprocessing; feature scaling; cluster validation*

DOI: https://doi.org/10.46687/MT26NAK

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ НА ВЛИЯНИЕТО НА ПРЕДВАРИТЕЛНАТА ОБРАБОТКА ВЪРХУ КАЧЕСТВОТО НА КЛЪСТЕРИЗАЦИЯТА

НЕЛИ А. АРАБАДЖИЕВА-КАЛЧЕВА

АБСТРАКТ: *Изследва се влиянието на мащабирането на признаците върху качеството на клъстеризацията чрез K-Means и агломеративния метод на Уорд. Върху наборите Iris и Digits са сравнени оригинални, стандартизирани и Min–Max нормализирани данни. Оценяването включва коефициент на силуета, индекс на Дейвис–Болдин и коригиран индекс на Ранд (ARI). Резултатите от 12 експеримента показват, че стандартизацията невинаги подобрява качеството.*

1 Въведение

Клъстеризацията е метод за машинно обучение без учител, при който обектите се групират според сходството на признаците им. Често използвани алгоритми са K-Means [1] и агломеративната йерархична клъстеризация по метода на Уорд [2]. Тъй като и двата метода се основават на разстояния, предварителното мащабиране може да промени полученото групиране.

Изборът на мащабиране влияе върху относителната тежест на признаците и геометрията на клъстерите. Целта на изследването е да се оцени как стандартизацията и Min–Max нормализацията променят резултатите на двата алгоритъма спрямо непреобразуваните данни.

2 Алгоритми и показатели за оценка

K-Means разделя наблюденията в предварително зададен брой групи, като минимизира сумата от квадратите на евклидовите разстояния до центровете им. Използвана е инициализация k-means++, намаляваща риска от неблагоприятен избор на начални

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

центрове [3]. Агломеративният подход с връзка на Уорд последователно обединява групи така, че нарастването на вътрешноклъстерната дисперсия да бъде минимално [2].

Сравняват се три варианта на признаците: без преобразуване; стандартизация до средна стойност 0 и стандартно отклонение 1; Min–Max мащабиране до интервала [0, 1]. Преобразуванията се прилагат поотделно към всеки признак. За неизменящи се признаци мащабираните стойности остават нулеви.

Използвани са три показателя: Silhouette Score (Silh.) за компактност и разделимост на групите [4], Davies–Bouldin Index (DB) за съотношението между вътрешна разсеяност и междуклъстерно разделяне [5] и Adjusted Rand Index (ARI) за съответствието с известните класове, коригирано за случайно съвпадение [6]. За Silh. и ARI по-високата стойност е по-добра, а за DB — по-ниската. Известните класове участват единствено при изчисляване на ARI, а не при обучението.

3 Експериментална постановка

Експериментите са реализирани на Python със scikit-learn 1.8.0 [7]. Анализирани са Iris (150 обекта, 4 признака, 3 класа) и Digits (1797 изображения на ръкописни цифри, 64 признака, 10 класа). За всяка комбинация от набор данни, предварителна обработка и алгоритъм е изчислено отделно групиране — общо 12 експеримента.

Броят на клъстерите е зададен на 3 за Iris и 10 за Digits. K-Means използва init="k-means++", n_init=20, max_iter=300 и random_state=42, а йерархичният алгоритъм — linkage="ward". Silh. и DB се пресмятат в пространството на обработените признаци, а ARI — спрямо оригиналните класове.

4 Резултати и анализ

Таблица 1. Резултати от клъстеризацията на Iris (3 клъстера)

Обработка	**Алгоритъм**	**Silh. ↑**	**DB ↓**	**ARI ↑**
Без обработка	K-Means	0.553	0.662	0.730
Без обработка	Ward	0.554	0.656	0.731
Стандартизация	K-Means	0.460	0.834	0.620
Стандартизация	Ward	0.447	0.803	0.615
Min–Max	K-Means	0.505	0.760	0.716
Min–Max	Ward	0.505	0.748	0.720

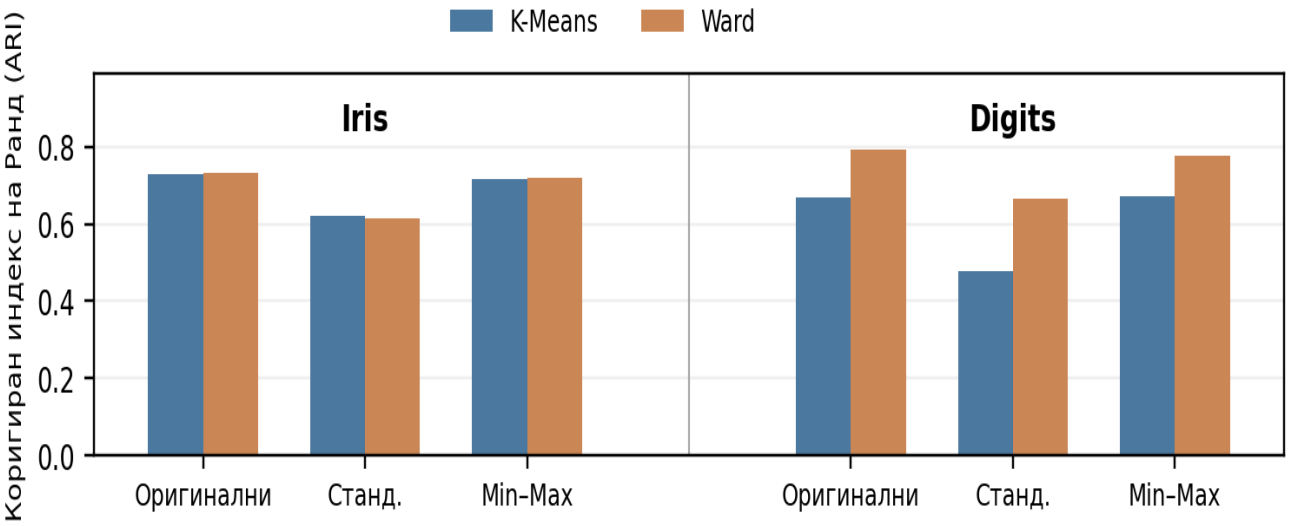
За Iris най-високите стойности на трите показателя са получени при оригиналните данни: Ward постига Silh. = 0,554, DB = 0,656 и ARI = 0,731 (табл. 1). При стандартизация

ARI на K-Means намалява от 0,730 на 0,620, а при Ward — от 0,731 на 0,615. Min–Max обработката дава междинни резултати.

Таблица 2. Резултати от клъстеризацията на Digits (10 клъстера)

Обработка	Алгоритъм	Silh. ↑	DB ↓	ARI ↑
Без обработка	K-Means	0.182	1.923	0.669
Без обработка	Ward	0.178	1.889	0.794
Стандартизация	K-Means	0.142	1.886	0.478
Стандартизация	Ward	0.125	1.967	0.664
Min–Max	K-Means	0.181	1.927	0.672
Min–Max	Ward	0.176	1.887	0.777

За Digits алгоритъмът Ward върху оригиналните данни постига ARI = 0,794 срещу 0,669 при K-Means, макар K-Means да има малко по-висок Silh. (0,182 срещу 0,178). Стандартизацията понижава ARI съответно до 0,664 и 0,478 (табл. 2). На фиг. 1 е представено сравнението на стойностите на ARI за двата алгоритъма при трите варианта на предварителна обработка върху Iris и Digits.



Фиг. 1. Изменение на коригирания индекс на Ранд (ARI) при различна предварителна обработка

От фиг. 1 се вижда, че при Iris и Digits стандартизацията води до по-ниски стойности на ARI и за двата алгоритъма. При Digits Min–Max мащабирането запазва близки до

оригиналните стойности: 0,672 за K-Means и 0,777 за Ward. По-слабите резултати при стандартизацията може да са свързани с увеличеното влияние на пикселни признаци с ниска вариация; това предположение изисква допълнителна проверка. Silh. и DB следва да се сравняват предпазливо между различни мащабирания, тъй като самите разстояния се променят.

5 Заключение

Проведените 12 експеримента показват, че предварителната обработка може съществено да промени качеството на клъстеризацията. При двата анализирани набора стандартизацията намалява ARI и за двата алгоритъма, докато Min–Max мащабирането има по-ограничено влияние. Най-висок ARI за Digits е постигнат чрез Ward върху оригиналните признаци (0,794).

Изводите се отнасят до два набора данни, фиксиран брой клъстери и конкретни параметри. В бъдеще могат да бъдат изследвани допълнителни набори, устойчиви методи за мащабиране и стабилността при различни инициализации. Мащабирането следва да се избира според измереното качество, а не автоматично.

ЛИТЕРАТУРА:

[1] MacQueen, J. Some methods for classification and analysis of multivariate observations. Proc. 5th Berkeley Symposium on Mathematical Statistics and Probability, 1 (1967), 281–297.

[2] Ward, J. H., Jr. Hierarchical grouping to optimize an objective function. Journal of the American Statistical Association, 58(301) (1963), 236–244. DOI: 10.1080/01621459.1963.10500845.

[3] Arthur, D., Vassilvitskii, S. k-means++: The advantages of careful seeding. Proc. 18th ACM–SIAM Symposium on Discrete Algorithms (2007), 1027–1035.

[4] Rousseeuw, P. J. Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. Journal of Computational and Applied Mathematics, 20 (1987), 53–65. DOI: 10.1016/0377-0427(87)90125-7.

[5] Davies, D. L., Bouldin, D. W. A cluster separation measure. IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-1(2) (1979), 224–227. DOI: 10.1109/TPAMI.1979.4766909.

[6] Hubert, L., Arabie, P. Comparing partitions. Journal of Classification, 2 (1985), 193–218. DOI: 10.1007/BF01908075.

[7] Pedregosa, F. et al. Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12 (2011), 2825–2830.

MACHINE LEARNING METHODS IN ENVIRONMENTAL AND GEOSPATIAL RESEARCH: METHODOLOGICAL PRINCIPLES FOR MODEL SELECTION*

KAMEN K. KALCHEV

ABSTRACT: *Environmental and geospatial studies increasingly combine field observations, geographic information systems, remote sensing and machine learning. The direct transfer of a high-performing algorithm from a generic benchmark, however, does not guarantee reliable spatial prediction. This paper presents a review-based methodological framework in which model selection starts from the research task, target variable, data structure, scale, sample design and required interpretability. Particular attention is paid to classification and regression problems, tree ensembles, support vector machines, gradient boosting and deep learning, as well as to spatial autocorrelation, training-data quality, spatial validation and explainable artificial intelligence. The proposed workflow treats validation and transferability as integral parts of model selection and is intended as a general basis for future environmental and geospatial applications.*

KEYWORDS: *machine learning, environmental data, geospatial data, GIS, remote sensing, spatial validation, explainable artificial intelligence*

DOI: https://doi.org/10.46687/MT26KKK

МЕТОДИ ЗА МАШИННО ОБУЧЕНИЕ В ЕКОЛОГИЧНИ И ГЕОПРОСТРАНСТВЕНИ ИЗСЛЕДВАНИЯ: МЕТОДОЛОГИЧНИ ПРИНЦИПИ ПРИ ИЗБОРА НА МОДЕЛ

КАМЕН К. КАЛЧЕВ

АБСТРАКТ: *Екологичните и геопространствените изследвания все по-често обединяват теренни наблюдения, географски информационни системи, дистанционни изследвания и машинно обучение. Високата точност на даден алгоритъм в стандартен набор от данни обаче не гарантира надеждна пространствена прогноза. В статията се предлага обзорно-методологична рамка, при която изборът на модел започва от изследователската задача, целевата променлива, структурата и мащаба на данните, начина на формиране на извадката и необходимостта от интерпретируемост. Разгледани са класификационни и регресионни задачи, ансамблови модели, SVM, gradient boosting и дълбоко обучение, както и проблемите на пространствената автокорелация, качеството на обучаващите данни, пространствената валидация и обяснимия изкуствен интелект.*

1 Въведение

Развитието на дистанционните изследвания, сензорните системи и отворените геопространствени бази данни превръща екологията и науките за Земята в области с нарастващ обем разнородна информация. Съвременните изследвания могат едновременно да използват теренни измервания, метеорологични и хидроложки редове, цифрови модели на релефа, тематични GIS слоеве, сателитни изображения и данни за човешка дейност. Машинното обучение предоставя средства за откриване на зависимости, класификация, прогнозиране и картографиране в такава многомерна среда [1, 2].

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

При геопространствените задачи обаче алгоритъмът не може да бъде разглеждан независимо от структурата на данните. Наблюденията са свързани с конкретно място и време, често са пространствено автокорелирани, неравномерно разпределени и получени чрез различни методики. Това създава риск моделът да възпроизведе локалната структура на обучаващата извадка, без да притежава необходимата способност за обобщаване към нови райони или периоди [2]. Поради тази причина изборът на метод следва да бъде част от цялостна методология, а не решение, основано единствено на популярността на даден алгоритъм или на максимална стойност на една метрика.

Целта на настоящата работа е да систематизира основните критерии за избор на методи за машинно обучение при екологични и геопространствени изследвания и да предложи последователна рамка, приложима към различни бъдещи задачи. Подходът е обзорно-методологичен и се основава на съвременни обзори в областта на екологията, геопространственото моделиране и дистанционните изследвания, допълнени с основополагащи публикации за разглежданите алгоритми [1–12].

2 Особености на екологичните и геопространствените данни

Първата особеност е пространствената зависимост. Близко разположените наблюдения често имат сходни стойности поради непрекъснатостта на природните процеси. Температура, валежи, растителност, почвени свойства, замърсяване и разпространение на видове могат да проявяват ясно изразена пространствена автокорелация. Ако съседни точки попаднат едновременно в обучаващата и тестовата извадка, моделът може да получи прекалено оптимистична оценка, защото тестовите данни практически не са независими от обучаващите [2, 5].

Втората особеност е пространствената и времевата неоднородност на извадките. Теренните измервания са скъпи и поради това често са концентрирани около достъпни места. Редките екологични явления водят до небалансирани класове, а промени в методиката на измерване или в сензорите могат да породят несъвместими времеви серии. При сателитната класификация качеството, размерът, балансът и пространственото разпределение на обучаващите данни са критични за крайната точност [4].

Третата особеност е хетерогенността на източниците. В една задача могат да участват непрекъснати числови показатели, категорийни признаци, растерни и векторни слоеве, изображения и времеви редове. Това означава, че изборът на модел трябва да следва не само целта на изследването, но и представянето на данните. Метод, подходящ за таблични признаци, не е непременно оптимален за многоканални изображения, а модел, който работи добре при интерполация в познат район, може да бъде ненадежден при пространствен трансфер [2, 12].

3 Изследователската задача като водещ критерий при избора на модел

Най-естествената отправна точка е типът на целевата променлива. При класификация се предсказва дискретен клас – например вид земно покритие, наличие на определено местообитание, категория на екологичен риск или наличие на замърсяване. При регресия се прогнозира непрекъсната величина – температура, концентрация на замърсител, индекс за качество на водата, биомаса или друга количествена характеристика. При анализ на изображения задачата може да бъде разширена до сегментация или откриване на обекти.

При таблични данни с нелинейни зависимости и взаимодействия между признаците ансамбловите модели на дървета са естествен кандидат. Random Forest комбинира

множество дървета, обучени с рандомизация на примери и признаци, като по този начин намалява вариацията и е устойчив спрямо шум [6]. Методът е широко използван при пространствени и екологични задачи, но при добавяне на координати или други пространствени прокси променливи ползата не е универсална; тя зависи от целта на прогнозата, разпределението на наблюденията и остатъчната пространствена автокорелация [12].

Когато класовете са разделими чрез сложна граница и броят на обучаващите примери е ограничен, Support Vector Machine (SVM) е подходящ кандидат. Чрез kernel функции методът може да конструира нелинейни граници с добра способност за обобщаване [7]. При класификация на земно покритие със Sentinel-2 Random Forest и SVM са сред традиционно силните методи, като обзорите показват, че резултатът зависи от броя на обучаващите примери, броя на класовете, терена и предварителната обработка [3]. Следователно изборът между тях следва да бъде експериментален, а не предварително фиксиран.

При сложни таблични задачи с множество нелинейни взаимодействия gradient boosting моделите са друга подходяща група. XGBoost изгражда последователно дървета, които коригират грешките на предходния ансамбъл и включва механизми за регуляризация и ефективна работа с разредени данни [8]. Този тип модели е особено полезен, когато целта е висока прогнозна точност при структурирани екологични показатели, но изисква внимателно настройване на хиперпараметрите и независима оценка на способността за обобщаване.

Когато основният източник е изображение и са налични достатъчно означени данни и изчислителни ресурси, дълбокото обучение позволява автоматично извличане на пространствени характеристики. CNN, U-Net и други архитектури имат значими приложения в класификацията и сегментацията на изображения от дистанционни изследвания [9]. Те обаче не са автоматично предпочитан избор: при малки извадки или когато е необходима ясна интерпретация, по-простите модели могат да бъдат по-надеждни и по-лесни за възпроизвеждане.

Таблица 1. Връзка между характеристиките на задачата и избора на модел

Характеристика на задачата	Подходяща група модели	Основно предимство	Основен риск/ограничение
Таблични данни, нелинейни зависимости	Random Forest / boosting	Работа с взаимодействия между признаците	Пренастройване и пространствено „запаметяване“
Малка/средна означена извадка, сложна граница	SVM	Добра генерализация при подходящ kernel	Чувствителност към мащабиране и параметри
Многоспектрални изображения с ръчно зададени признаци	RF / SVM	Подходящи при умерен обем означени данни	Качеството на обучаващата извадка е критично
Големи набори от изображения	CNN / U-Net и други DL модели	Автоматично извличане на пространствени признаци	Необходимост от много данни и изчислителни ресурси
Модел за научна интерпретация и управление	Интерпретируем модел или ML + XAI	Обяснение на факторите и проверка от експерт	Обяснението не доказва причинност

4 Критерии за надежден избор и сравнение на модели

Сравнението на алгоритми има научна стойност само ако условията са еднакви. Една и съща обучаваща и тестова схема, едни и същи входни признаци и предварително избрани метрики позволяват да се оцени реалната полза от по-сложния модел. Като базова линия е полезно да се включи по-прост модел, например линейна или логистична регресия, когато постановката го позволява. Ако сложен ансамблов модел не подобрява съществено качеството, по-простият вариант може да бъде предпочетен поради по-добра интерпретируемост и възпроизводимост.

Метриката трябва да съответства на изследователската цел. При балансирана класификация общата точност е удобна, но при редки класове може да бъде подвеждаща. Precision, recall и F1-score дават по-пълна картина, а при бинарни задачи могат да се използват ROC-AUC или PR-AUC. При регресия често се използват MAE, RMSE и R^2, като изборът между тях зависи от чувствителността към големи грешки и целта на прогнозата. Необходимо е да се показва не само среден резултат, но и вариабилността между отделните разпределения или пространствени блокове.

Отделен критерий е преносимостта. Моделът може да бъде много точен в района, от който са събрани данните, но да се влоши при нови пространствени или времеви условия. Съвременният геопространствен анализ поставя все по-силен акцент върху разликата между интерполация и екстраполация, върху покритието на обучаващите данни и върху несигурността извън познатия диапазон [2, 12]. Затова „най-добрият“ модел следва да се определя спрямо бъдещия сценарий на използване, а не само спрямо една тестова извадка.

5 Пространствена валидация и предотвратяване на завишена точност

Кръстосаната валидация е стандартен инструмент за оценяване на модели, но случайното разпределяне на наблюденията не винаги е подходящо за пространствени данни. Roberts et al. показват, че пренебрегването на времевата, пространствената или йерархичната структура може да доведе до сериозно подценяване на прогнозната грешка [5]. При геопространствена задача близките наблюдения могат да се окажат в различни folds и моделът да бъде оценяван върху обекти, които са твърде сходни с обучаващите.

Практично решение е използването на пространствени блокове, при които цели области се отделят за валидация. Размерът на блока трябва да е съобразен с мащаба на пространствената зависимост и с реалната цел: прогноза в съседни ненаблюдавани места, трансфер към друг район или прогнозиране в бъдещ период. При наличие на времева динамика може да се приложи и времево блокиране или комбинирана пространствено-времева схема. Качеството на обучаващата извадка и нейното покритие остават основни условия за надеждна оценка [4].

Следователно в геопространствените изследвания валидацията не е последна техническа стъпка, а част от самата дефиниция на задачата. Модел, който печели при случайна cross-validation, но губи при пространствено разделяне, не трябва автоматично да бъде избран за картографиране или пространствен трансфер.

6 Интерпретируемост и обясним изкуствен интелект

При екологични изследвания целта често не е единствено да се прогнозира стойност, а да се разберат факторите, които са свързани с нея. Това поставя изискване за интерпретируемост. При по-прости статистически модели връзката между входовете и прогнозата е по-пряка, докато ансамблите и дълбоките модели са по-трудни за обяснение.

SHAP (SHapley Additive exPlanations) предлага обща рамка за оценяване на приноса на отделните признаци към конкретни прогнози и към глобалното поведение на модела [10]. Голям обзор в науките за околната среда и Земята показва, че SHAP и Shapley-базираните методи са най-често използваната група XAI техники сред разгледаните публикации [11]. Това ги прави подходящ инструмент за проверка дали моделът използва екологично смислени зависимости и за идентифициране на признаци, които доминират прогнозата.

Интерпретацията обаче трябва да бъде предпазлива. Високата SHAP стойност показва принос към поведението на конкретния модел, но не доказва причинно-следствена връзка. Корелирани признаци, пространствена зависимост и промени в разпределението на данните могат да променят обяснението [11]. Поради това XAI е необходимо да се комбинира с експертно екологично знание и с независима проверка, а не да се използва като автоматичен заместител на научната интерпретация.

7 Предложена методологична рамка

На основата на разгледаните изследвания може да се предложи обща последователност за бъдещи екологични и геопространствени приложения. Първо се формулира конкретната научна хипотеза или управленски въпрос и се определя дали задачата е класификация, регресия, сегментация или откриване на промени. Второ се анализират източниците, качеството, пространственото покритие, времевата съпоставимост, липсващите стойности и балансът на класовете. Трето се създава набор от признаци, който съчетава данните без изтичане на информация между обучение и тест.

Четвъртата стъпка е избор на ограничен набор от модели, представящи различни нива на сложност. Вместо да се сравняват много алгоритми без ясна причина, е по-подходящо да се избере базов модел и един или два по-сложни кандидата, съответстващи на типа данни. При таблични екологични данни това могат да бъдат базова регресия и ансамблови модели; при спектрална класификация – RF и SVM; при големи изображения – подходяща deep-learning архитектура.

Петата стъпка е предварително дефиниране на валидационна схема и метрики, съответстващи на реалното бъдещо използване. При пространствен трансфер се предпочита пространствено блокирана проверка; при прогноза във времето – времево разделяне; при комбинирана задача – пространствено-времева схема. Шестата стъпка е настройване на хиперпараметрите само в рамките на обучаващите данни, за да не се допуска информационно изтичане.

Последните стъпки включват сравнение на резултатите, анализ на грешките по класове и райони, оценка на несигурността и интерпретация на най-подходящия модел. Когато се използва сложен модел, SHAP или друга XAI техника може да добави обяснителен слой, но резултатите трябва да се съпоставят с домейн знание. Този работен поток позволява алгоритъмът да бъде следствие от научната постановка, а не отправна точка на изследването.

8 Заключение

Машинното обучение разширява възможностите за анализ на екологични и геопространствени данни, но надеждността на резултатите зависи в по-голяма степен от правилната постановка на задачата, качеството на данните и валидационната схема, отколкото от избора на един „модерен“ алгоритъм. Random Forest, SVM, gradient boosting и дълбоките модели имат различни силни страни и следва да бъдат използвани според типа на целевата променлива, обема и структурата на данните, необходимостта от пространствен трансфер и изискванията за интерпретируемост.

Особено важни са пространствената автокорелация, представителността на обучаващите извадки и независимото оценяване. При научни и управленски приложения високата прогнозна точност трябва да бъде допълнена с анализ на несигурността и с обяснение на поведението на модела. Предложената рамка е достатъчно обща, за да бъде използвана като методологична основа при бъдещи изследвания върху водни, крайбрежни, сухоземни и урбанизирани екосистеми, без да обвързва анализа с конкретен географски обект или един предварително избран алгоритъм.

ЛИТЕРАТУРА:

[1] Wu, J., Luo, Y., Liu, F., Liao, C., Wang, Y., He, H., Tong, D., Liu, Z., Zhao, Y., Meng, X., Sun, C., Zhou, J., Zhang, J., Huang, Y., Machine learning in ecology: Current status and future directions in the big data era. Geography and Sustainability, 7 (5) (2026), 100533. https://doi.org/10.1016/j.geosus.2026.100533.

[2] Koldasbayeva, D., Tregubova, P., Gasanov, M., Zaytsev, A., Petrovskaia, A., Burnaev, E., Challenges in data-driven geospatial modeling for environmental research and practice. Nature Communications, 15 (2024), 10700. https://doi.org/10.1038/s41467-024-55240-8.

[3] Phiri, D., Simwanda, M., Salekin, S., Nyirenda, V.R., Murayama, Y., Ranagalage, M., Sentinel-2 Data for Land Cover/Use Mapping: A Review. Remote Sensing, 12 (14) (2020), 2291. https://doi.org/10.3390/rs12142291.

[4] Moraes, D., Campagnolo, M.L., Caetano, M., Training data in satellite image classification for land cover mapping: a review. European Journal of Remote Sensing, 57 (1) (2024), 2341414. https://doi.org/10.1080/22797254.2024.2341414.

[5] Roberts, D.R., Bahn, V., Ciuti, S., Boyce, M.S., Elith, J., Guillera-Arroita, G., Hauenstein, S., Lahoz-Monfort, J.J., Schröder, B., Thuiller, W., Warton, D.I., Wintle, B.A., Hartig, F., Dormann, C.F., Cross-validation strategies for data with temporal, spatial, hierarchical, or phylogenetic structure. Ecography, 40 (8) (2017), 913-929. https://doi.org/10.1111/ecog.02881.

[6] Breiman, L., Random Forests. Machine Learning, 45 (2001), 5-32. https://doi.org/10.1023/A:1010933404324.

[7] Cortes, C., Vapnik, V., Support-vector networks. Machine Learning, 20 (1995), 273-297. https://doi.org/10.1007/BF00994018.

[8] Chen, T., Guestrin, C., XGBoost: A Scalable Tree Boosting System. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2016), 785-794. https://doi.org/10.1145/2939672.2939785.

[9] Paheding, S., Saleem, A., Siddiqui, M.F.H., Rawashdeh, N., Essa, A., Reyes, A.A., Advancing horizons in remote sensing: a comprehensive survey of deep learning models and applications in image classification and beyond. Neural Computing and Applications, 36 (2024), 16727-16767. https://doi.org/10.1007/s00521-024-10165-7.

[10] Lundberg, S.M., Lee, S.-I., A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems, 30 (2017).

[11] Schiller, J., Stiller, S., Ryo, M., Artificial intelligence in environmental and Earth system sciences: explainability and trustworthiness. Artificial Intelligence Review, 58 (2025), 316. https://doi.org/10.1007/s10462-025-11165-2.

[12] Milà, C., Ludwig, M., Pebesma, E., Tonne, C., Meyer, H., Random forests with spatial proxies for environmental modelling: opportunities and pitfalls. Geoscientific Model Development, 17 (2024), 6007-6033. https://doi.org/10.5194/gmd-17-6007-2024.

IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)

IVO V. VELIKOV

ABSTRACT: *This publication is based on The Handbook of Homeland Security, 2023 edition, and the publication of Lora Hadzhidimova, probably a Bulgarian scholar whom I have no opportunity to know, according to what is written about her - she represents Old Dominion University, Norfolk, VA, United States. The vast majority of the text and citations are the work of this author. However, the theme is so relevant that we allow ourselves to copy this article for the Bulgarian environment, with our additions and comments.*

KEYWORDS: *Immigration and Customs Enforcement (ICE); US Department of Homeland Security; structure, functions and tasks of Immigration and Customs Enforcement (ICE)*

DOI: https://doi.org/10.46687/MT26IVV

ИМИГРАЦИОННА И МИТНИЧЕСКА СЛУЖБА (ICE) НА САЩ

ИВО В. ВЕЛИКОВ

АБСТРАКТ: *Настоящата публикация се основава на The Handbook of Homeland Security, издание 2023 г., и публикацията на Lora Hadzhidimova, вероятно български учен, когото нямам възможност да познавам, според написаното за нея - представлява Old Dominion University, Norfolk, VA, United States. Огромната част от текста и цитиранията са дело на този автор. Тематиката обаче е толкова актуална, че си позволяваме да копираме за българската среда тази статия, с наши допълнения и коментари.*

Въведение

Агенцията за имиграция и митнически контрол (ICE) е правителствена агенция, създадена през 2003 г. като част от Министерството на вътрешната сигурност на САЩ. Тя обединява две предишни агенции – Митническата служба на САЩ (USCS - U.S. Customs Service) и Службата за имиграция и натурализация (INS - Immigration and Naturalization Service). Бюджетът на ICE тогава е приблизително 6 милиарда долара годишно разпределени между петте ѝ клона – Разследвания на вътрешната сигурност (HIS - Homeland Security Investigations), Операции по правоприлагане и отстраняване (ERO-Enforcement and Removal Operations), Служба на главния юрисконсулт (OPLA - Office of the Principal Legal Advisor), Звеното за управление и администрация и Службата за професионална отговорност (Office of Professional Responsibility)1. (Department of Homeland Security, 2017)

Интересът към тази агенция се породи от последната една година, когато поради предизборните обещания на новият стар президент Тръмп, той съвсем сериозно се зае с имиграционната политика на страната си - почти веднага чрез указ обяви извънредно положение на южната граница (б.а. – с Мексико) (Мартинов, 2025), с което привлече Националната гвардия, армейски части (б.а. – първоначално 1000, намерение да достигнат 10 000)(Карабоев, 2025) и всички структури за сигурност в района за обезпечаване на потока от имигранти, а през цялата 2025 година преструктурира Агенцията за имиграция и митнически контрол, за да я превърне във водеща такава, и дори не само в рамките на Министерството на вътрешната сигурност.

1 Функции на отделните елементи

Основните функции на ICE са свързани с прилагането на законите за границите, имиграцията, търговията и сигурността, предназначени да гарантират и поддържат обществената безопасност и ред. Отговорностите на звеното ERO включват определяне на лица, които не са граждани на САЩ и подлежат на експулсиране, както и задържането и депортирането им, ако е необходимо. То е разделено на шест оперативни звена – Отдел „Полеви операции“, който управлява и контролира работата на 24 полеви офиса; Отдел „Правоприлагане“, отговарящ за действията, предприети от властите за задържане на незаконно пребиваващи в САЩ чужденци; Отдел „Управление на попечителството“, отговарящ за процедурите по време на задържането; Отдел „Извеждане“, отговарящ за физическите действия по депортиране и правилната координация с чуждестранни правителства; Отдел „Здравни услуги на ICE“, който контролира здравните нужди на задържаните; и Отдел „Оперативна поддръжка“, който играе ролята на административния апарат на ERO, осигурявайки правилно финансово, бюджетно, човешки ресурси и организационно функциониране на цялото звено. ERO поддържа и директория, която проследява местоположението на задържаните, на които вече е присвоен „Регистрационен номер на чужденец“. Лица под 18-годишна възраст не се регистрират чрез системата, както и лица, които вече са били депортирани. Посещенията в центровете за задържане, разположени в 30 щата, са разрешени, когато са уговорени с отговорните органи. В допълнение към това, линията за докладване и информация за задържания приема запитвания за насилие, малтретиране, сериозни психически и физически здравословни проблеми на задържаните и техните родителски права и предоставя обща информация за задържаните лица. За да осигури ICE прозрачност и публичност на работата си, задържаните, роднини и познати на задържаните, неправителствени организации (НПО), адвокати, съветници и обществеността могат да получат информация за задържаните чужденци. Съгласно раздел 287(g) от Закона за имиграцията и гражданството за делегиране на имиграционни правомощия, изпълнителният заместник-директор на ERO може да подпише споразумение с федерална, щатска или местна структура за делегиране на определени прерогативи, които са в рамките на отговорностите на ICE за гарантиране на обществената безопасност и ефикасността на разследванията и процедурите на правоприлагащите органи. Служителите, които изпълняват задълженията и функциите на ERO, трябва да отговарят на следните квалификационни критерии: американско гражданство, завършена проверка на миналото, липса на висящи или завършени дисциплинарни производства срещу длъжностното лице и натрупан опит на длъжността.

Отделът HSI изпълнява широк спектър от функции, насочени предимно към гарантиране, че движението на стоки и хора през границата на САЩ ще бъде в съответствие с граничните и митническите закони. В този аспект HSI провежда операции както в Съединените щати, така и в чужбина, за да постигне гореспоменатите цели. Звеното също така се състои от осем подразделения – Вътрешни операции, Международни операции, Национален център за координация на правата върху интелектуалната собственост, Управление на информацията, Разследващи програми, Подкрепа на мисиите, Разследвания в областта на националната сигурност и Служба за разузнаване.

Звеното за вътрешни операции контролира и провежда разследвания в своите 26 вътрешни офиса, разположени в източен, централен и западен клон.

Международните операции си сътрудничат с чуждестранни юрисдикции в опит да установят контрол върху движението на стоки и лица през границите на САЩ.

То има два компонента – Международни операции Изток и Международни операции Запад. Първият обхваща операции, изпълнявани в Европа, Африка, Близкия изток, Азия и Тихоокеанския регион, тъй като всеки център в тези географски региони има отделно командване. Вторият включва кампании в северноамерикански щати извън САЩ, Централна Америка, Южна Америка и Карибите. Специфичният характер на усилията в чужбина изисква отчитане както на централното ръководство на HSI, така и на американските посланици в съответните страни.

Националният координационен център за права върху интелектуална собственост провежда операции, свързани със защитата на пазара от стоки, които не отговарят на изискванията за интелектуална собственост на законите на САЩ за стоки, разпространявани както във физическото, така и/или в онлайн пространството.

Звеното за управление на информацията работи за събиране и разпространение на информация за случаи на HSI. То отговаря за споделянето на данните между различните офиси в Министерството на вътрешната сигурност. Освен това се стреми да включи ефективни технологични решения в разследванията и да повиши общата надеждност на проведените статистически анализи.

Разследващите програми целят да укрепят националната сигурност чрез различни традиционни и кибероперации. Специално определени екипи се борят с наркокартелите и контрабандата на наркотици през границата на САЩ, с печалбите от нея и с всякакви други финансови облаги, произтичащи от контрабанда и/или други незаконни дейности (Тепавичарова, В., 2022). Освен това, звеното за разследващи програми ръководи криминалистична лаборатория, оборудвана за изследване на пръстови отпечатъци и ръкописни документи, за да подпомогне разследващите усилия на HSI.

Отделът за подкрепа на мисиите в HSI служи като механизъм, осигуряващ правилно финансово, бюджетно, логистично, политическо и планиране на човешките ресурси, както и консултиране на американски служители, изпълняващи задължения като дипломатически представители в чужбина.

Разследванията по линия на национална сигурност разкриват доста разнообразен набор от отговорности. Това подразделение служи като антитерористично звено, което се стреми да предотврати престъпните групировки да се сдобият с оръжия за масово унищожение (ОМУ) от различен вид – химически, биологични или каквато и да е американска технология, която би могла да подпомогне изграждането на такива. Тази структура се занимава и с действията, свързани с военнопрестъпници и лица, обвинени в нарушения на правата на човека и геноцид. Друга задача на Националната служба за разследвания на сигурността е да поддържа Информационната система за студенти и обменни посетители (SEVIS - Student and Exchange Visitor Information System), която събира данни за всеки студент, който не е от САЩ и се стреми да получи университетска или друга квалификация от допустими американски образователни институции. Макар и в звеното HSI да има отдел „Национална сигурност“, неговите функции не се свързват с противодействие на шпионажа, а както бе посочен с борба с тероризма, което изисква „координирани действия по разследване на противодържавни посегателства“ (Михайлов, 2026).

Основната задача на Службата за разузнаване е да събира и разпространява доклади за случаи и/или информацията, събрана по отношение на случаите, в рамките на HSI. Данните се отнасят до традиционни и киберпрестъпления, извършени както в Съединените щати, така и в чужбина, включително тероризъм, кражба на самоличност, измами, пране на пари, контрабанда, нарушения на интелектуалната собственост и други.

Отделът за управление и администрация няма независими оперативни функции, но осигурява общо ръководство и надзор на други звена. Освен това, той е отговорен за широк спектър от административни задължения, като например управление на бюджета и финансите, информационните системи, процесите на наемане, съоръженията и оборудването.

Достъпът до информацията, която тази служба събира и поддържа за дейността на своите клонове, е безплатен за обществеността и гарантиран от Закона за свобода на информацията. Лицата могат да получат информация по писмено искане до агенцията.

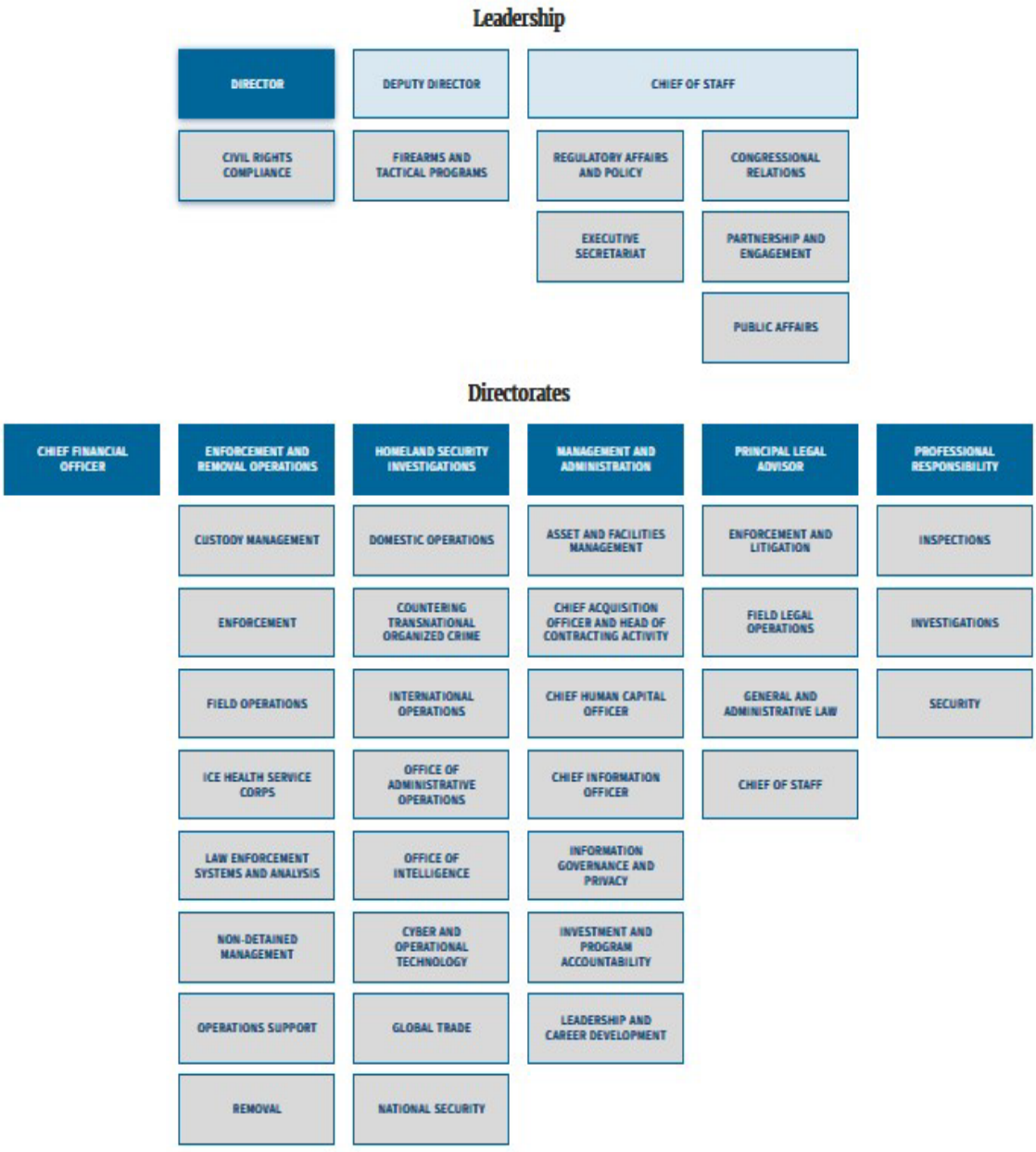
Конгресът на САЩ установява три изключения от това правило. Всички те се отнасят до националните интереси за сигурност и правоприлагащите органи: (1) случаи на криминални разследвания, при които разкриването на информация би могло да създаде пречки за операциите, (2) случаи на наказателноправни органи, при които самоличността на информатор не е била официално разкрита, и (3) класифицирани записи на ФБР за случаи на международен тероризъм и събиране на международна разузнавателна информация (FOIA, 2018).

Службата за професионална отговорност е отговорна за целостта на провежданите операции и тяхното съответствие със законите и професионалната етика. Тя разследва два вида нарушения. Първо, предполагаеми „нарушения на щатското или федералното наказателно право“ и второ, твърдения, които „подкопават способността на агенцията да изпълнява своята мисия“ (ICE, 2018). Сигнал за нарушения може да бъде изпратен по телефон, имейл и поща и може да дойде от правителствена агенция, затворници или обществеността.

OPLA (Office of the Principal Legal Advisor) се състои от юристи и административни служители, които инициират, ръководят и контролират производствата за отстраняване на лица, за които няма законни основания за престой в Съединените щати и са нарушили федералните или щатските закони. OPLA е описано като най-голямата правна програма в DHS, с над 1 700 адвокати и около 300 служители в подкрепа. То остава изключителният представител на DHS в имиграционните производства за депортация пред EOIR и предоставя правни услуги на всички програми на ICE.(ICE, 2026 г.) OPLA не се включва в оперативната схема, защото: изпълнява юридическа, а не оперативна функция; трябва да бъде независима от оперативните дирекции, за да дава обективни правни становища; обслужва всички звена, затова е позиционирана директно под Principal Legal Advisor, а не под HSI, ERO или други оперативни линии.

Четири подразделения в рамките на OPLA изпълняват различни функции по отношение на лидерството и управлението („Началник на персонала“), правните услуги („Правоприлагане и съдебни спорове“), разпределянето на правни консултации на местните правоприлагащи органи („Теренни правни операции“) и предоставянето на експертни съвети в различни категории право – търговско, административно, правителствена информация, трудово и трудово право („Общо право“). Адвокатите на OPLA защитават действията на служителите на ICE пред федералните юрисдикции и работят заедно с Министерството на правосъдието в съдебни спорове срещу незаконно пребиваващи в САЩ чужденци, които са обект на експулсиране.

Табл. 1. Структурна схема на агенцията ICE



2 Предизвикателства и опасения

Две от най-големите опасения, свързани с ICE, са свързани със задържането на имигранти, условията, в които пребивават, техните права и нужди, особено на уязвимите групи, и някои предизвикателства, които поставят под въпрос цялостната ефективност на агенцията.

Съобщава се, че задържаните изразяват повишени нива на стрес поради потенциално депортиране, липса на достъп до здравни грижи и липса на прозрачност, справедливост и обективност в сътрудничеството между местните правоохранителни органи и ICE (Hacker et al., 2011). Ако медицинският персонал открие състояние или заболяване след преглед на имигрант, той получава лечение от Отдела за здравни услуги за имигранти (DIHS).

Лечението обаче много често е непълно поради депортирането на пациента (Schneider and Lobato, 2007).

Още по-проблематични са случаите на задържане, свързани с уязвими групи като деца и жертви на трафик. Децата на нелегални имигранти страдат от голям брой последици след задържането на родителите си, особено в случаите на самотно родителство. Актът на задържане обикновено води до значителна емоционална тежест за психиката на подрастващите и други неприятни последици от финансов характер, например. Ако последва депортиране, децата или заминават с родителите си в съответните си страни на произход, или могат да останат в приемна грижа, в случай че самите те са граждани на САЩ. Ако станат част от системата за приемна грижа, родителите нямат право да ги посещават през следващите 3–10 години (McLeigh, 2010). Цената, която задържането на родители имигранти нанася върху децата им, често се изразява в повишена тревожност, депресия и дори агресивно поведение (Phillips and Gleeson, 2007).

Друга уязвима група от населението са жертвите на трафик на хора. Те са група, под специалната закрила на Закона за защита на жертвите на трафик и насилие от 2000 г. Самият закон е критикуван заради ограничените си ресурси за защита на жертвите на всички форми на трафик на хора, независимо от тежестта на случая (Chacón, 2010). Освен това, служителите на реда срещат значителни трудности при разпознаването и доказването, че определен нелегален имигрант е станал жертва на трафик на хора (Clawson and Dutch, 2016).

Друг набор от предизвикателства, пред които е изправена ICE, се отнася до цялостната ефективност на политиките, които агенцията следва. Един от основните въпроси, повдигнати в това отношение, е дали програмите и мерките, приети и изпълнявани от ICE, чиято крайна цел е да намалят нивата на престъпност в Съединените щати, са продуктивни. Успехът на две подобни програми, които ICE подкрепя – Делегирането на имиграционни правомощия, раздел 287(g), част от Закона за имиграцията и гражданството, и програмата „Сигурни общности“ – е обект на сравнение и оценка в литературата. Последната се характеризира като подобрено продължение на първата.

Докато в първия случай местните правоприлагащи органи си сътрудничат и партнират с ICE на доброволна основа, във втория случай федералните структури представляват директно задължително сътрудничество. Независимо от различията си, и двете инициативи са пример за делегиране на функции от федералните структури (ICE) на местните правоприлагащи органи.

Ефективността на сътрудничеството зависи до голяма степен от ресурсите, с които разполагат местните агенции, и от финансовите стимули за тях. Окръзите, които имат договори с частни центрове за задържане или сключват Междуправителствено споразумение за услуги (IGSA), са положително корелирани с по-висок брой депортации (Jaeger, 2016). Независимо от това, проучване разкрива, че общите нива на престъпност не са били повлияни от броя на задържаните имигранти като част от програмата „Сигурни общности“ (Miles and Cox, 2014). Друга негативна страна на съвместната кампания сочи фактът, че и двете програми „могат да генерират стимули за служителите да арестуват хора предимно по подозрение, че са нелегални имигранти, знаейки, че те ще бъдат проверени чрез програмата и вероятно ще бъдат подложени на процедура по експулсиране“ (Capps et al., 2011).

Формите на сътрудничество между федералните и местните структури често водят до расово профилиране, в резултат на недостатъчно или липсващо обучение на местните

служители на реда, чиито отговорности са да прилагат федералните имиграционни политики (Briggs, 2014). Освен това, подобни практики биха могли да породят недоверие между общността и правоприлагащите органи. Те биха могли също да доведат до страх от докладване на престъпления на властите от нелегални имигранти, които биха могли да поемат ролята или на жертва, или на свидетел.

3 Тактики на полицейската държава – критичен поглед на Джонатан Рауч

Тръмп превръща ICE през 2025 г. в разрастваща се паравоенна структура, която броди из страната безконтролно, претърсва и задържа чужденци и граждани без заповеди, използва сила демонстративно, действа с маски, получава оскъдно обучение, лъже за дейността си и ѝ е казано, че се ползва с "абсолютен имунитет". През 2025 г. той увеличава състава на агенцията повече от два пъти, а бюджетът ѝ вече надвишава комбинираните бюджети на всички други федерални правоприлагащи агенции, както и военните бюджети на всички държави с изключение на 15. "Това ще засегне всяка общност, всеки град", отбеляза наскоро Дейвид Биър, учен от Института Катон. "Наистина почти всеки в нашата страна ще се сблъска с това, по един или друг начин."

В Минеаполис и другаде агенцията се държи буквално провокативно, понякога брутално и вероятно незаконно - поведение, което Тръмп и неговият екип насърчават, отразяват в пресата и изпращат снимачни екипи да го популяризират, може би с надеждата да предизвикат насилствена съпротива, която би оправдала по-нататъшни репресии - стандартна стратегия в едни много по-агресивни режими. Неотдавнашната поява на министъра на вътрешната сигурност Кристи Ноем (б.а. – освободена в началото на 2026 г. от Тръмп) с табела "Един от нашите, всички ваши" сякаш намеква за друга подобна на фашистка тактика - колективното наказание - както и решението на администрацията да наводни Минеаполис с хиляди полицаи, след като жителите там започнаха да протестират срещу федералните тактики - приоритет, който беше изрично наказателен.(The Atlantic, 2026 г).

Броят на служителите и агентите на ICE се е увеличил драстично през 2025 г.: официалните изявления на Министерството на вътрешната сигурност и ICE показват, че работната сила на агенцията е приблизително 22 000 служители и агенти до края на годината - увеличение с около 12 000 от очакваните 10 000 по-рано през годината - въпреки че вътрешните данни на ICE и обобщенията на трети страни отчитат малко по-различни данни, което създава неяснота около точния брой на персонала.(factually.co, 2026 г.)

Заключение

ICE е сложна структура с много отдели и подразделения. Тя се управлява в съответствие с основните политически принципи, очертани от администрацията на президента. Тя се стреми да включи многостранни инициативи, които включват както местни, така и федерални агенции, както и публичния, и частния сектор. Някои от тези кампании стават обект на критика. Други просто демонстрират предизвикателствата, пред които е изправена ICE при изпълнението на своите задължения. Под внимание се поставят най-вече етиката на кампаниите и процедурите, които ICE предприема. По-специално, в центъра на дебатите относно успеха и морала на ICE стоят опасенията за здравето на имигрантите, благополучието на децата, чиито родители са задържани чужденци без

документи, практиките за расово профилиране и мотивите за сключване на публично-частни партньорства, целящи осигуряване на повече места за задържане. Функциите и програмите на ICE повдигат много въпроси, които стоят на границата между борбата за равенство и човешки и граждански права, от една страна, и граничния контрол, политиките за сигурност и безопасността на общността, от друга. Общата проблематика на мигрантите и миграционната сигурност е разгледана в (Станев, Методиева и Диманова, 2020). Миграционната сигурност се разглежда и като компонент на корпоративната сигурност (Metodieva & Simeonova, 2024).

Общият извод от казаното до тук реферира с два много важни извода. В началото на втория си мандат правителството на Тръмп превърна ICE във суперструктура, част от друга вече създадена суперструктура, каквото е Министерството на вътрешната сигурност, от една страна, и от друга – дейността на тази агенция е често във фокуса на общественото мнение поради някои практики на ръба на закона и дори преминавайки общоприетите лимити за законност. Последното не е „чудо невиждано“ за службите за сигурност, където и да е по света, но при ICE тези практики стават прекалено често и прекалено натрапчиво, най-вече за обществата с развити демократични традиции.

ЛИТЕРАТУРА:

[1] Department of Homeland Security (2017, June 13). Written testimony of CBP for a House Appropriations Subcommittee on Homeland Security hearing titled “Immigration and Customs Enforcement & Customs and Border Protection FY18 Budget Request”. Retrieved February 09, 2018, from https://www.dhs.gov/news/2017/06/13/written-testimony-cbp- house-appropriations-subcommittee-homeland-security-hearing

[2] Briggs, C. (2014). The reasonableness of a race-based suspicion: The fourth amendment and the costs and benefits of racial profiling in immigration enforcement. Southern California Law Review, 88, 379.

[3] Capps, R., Rosenblum, M. R., Rodriguez, C., & Chishti, M. (2011). Delegation and divergence: A study of 287 (g) state and local immigration enforcement. Washington, DC: Migration Policy Institute, 20.

[4] Chacón, J. M. (2010). Tensions and trade-offs: Protecting trafficking victims in the era of immigration enforcement. University of Pennsylvania Law Review, 158(6), 1609–1653.

[5] Станев С., Методиева Цв., Диманова Д. Мигранти и миграционна сигурност. SocioBrains, Issue 65, January 2020, с. 151–164, ISSN 2367-5721.

[6] Clawson, H. J., & Dutch, N. (2016). Identifying victims of human trafficking: Inherent challenges and promising strategies for the field. US Department of Health and Human Services Office of the Assistant Secretary for Planning and Evaluation.

[7] Coon, M. (2017). Local immigration enforcement and arrests of the hispanic population. Journal on Migration & Human Security, 5, 645.

[8] factually.co/ How many ice agents were employed by the US government in 2025, 2026 от https://factually.co/fact-checks/politics/how-many-ice-agents-employed-2025-cecc14?utm_source=copilot.com

[9] FOIA.gov (Freedom of Information Act), (2018). Retrieved January 28, 2018, from https://www.foia.gov/index.html

[10] Hacker, K., Chu, J., Leung, C., Marra, R., Pirie, A., Brahimi, M., … Marlin, R. P. (2011). The impact of immigration and customs enforcement on immigrant health: Perceptions of immigrants in Everett, Massachusetts, USA. Social Science & Medicine, 73(4), 586–594.

[11] ICE (Immigration and Customs Enforcement), (2018). Retrieved January 28, 2018, from https://www.ice.gov/

[12] Jaeger, J. (2016). Securing communities or profits? The effect of federal-local partnerships on immigration enforcement. State Politics & Policy Quarterly, 16(3), 362–386.

[13] McLeigh, J. D. (2010). How do immigration and customs enforcement (ICE) practices affect the mental health of children? American Journal of Orthopsychiatry, 80(1), 96.

[14] Miles, T. J., & Cox, A. B. (2014). Does immigration enforcement reduce crime? Evidence from secure communities. The Journal of Law and Economics, 57(4), 937–973.

[15] Phillips, S. D., & Gleeson, J. P. (2007). What we know now that we didn't know then about the criminal justice system's involvement in families with whom child welfare agencies have contact. Center for Social Policy and Research.

[16] Schneider, D. L., & Lobato, M. N. (2007). Tuberculosis control among people in US immigration and customs enforcement custody. American Journal of Preventive Medicine, 33(1), 9–14.

[17] Карабоев, П., Тръмп затвори южната граница за мигранти, армията ще разположи до 10 хил. души, Дневник, 23.01.2025 г., отhttps://www.dnevnik.bg/sviat/2025/01/23/4733318_trump_zatvori_jujnata_granica_za_migranti_armiiata/

[18] Мартинов, Л., Тръмп каза, че първото му действие като президент на САЩ ще бъде да обяви извънредно положение на южната граница, БТА, 20.01.2025 г., от https://www.bta.bg/bg/news/world/818124-tramp-kaza-che-parvoto-mu-deystvie-kato-prezident-na-sasht-shte-bade-da-obyavi-#%D1%83%D0%BA%D0%B0%D0%B7%20%D0%BD%D0%B0%20%D0%A2%D1%80%D1%8A%D0%BC%D0%BF%20%D0%B7%D0%B0%20%D0%B8%D0%B7%D0%B2%D1%8A%D0%BD%D1%80%D0%B5%D0%B4%D0%BD%D0%BE%20%D0%BF%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5

[19] Михайлов, А. Шпионажът като секюритизиран проблем, сп. Геополитика и геостратегия, бр. 2/2026, с. 108-117.

[20] Рауч, Дж., Джонатан Рауч за Америка при Тръмп: Да, това е фашизъм, сп. The Atlantic, 01.02.2026 г, https://news.bg/comments/dzhonatan-rauch-za-amerika-pri-tramp-da-tova-e-fashizam.html

[21] Тепавичарова, В. Участие на жени в терористична дейност. С., 2022, с.135-136.

[22] Metodieva Ts., Simeonova I. Migration security as a component of corporate security. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 27, Shumen, 2024, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 163–169. https://doi.org/10.46687/jsar.v27i1.416

PROTECTION OF USER DATA IN DIGITAL GAMING ENVIRONMENTS*

BORISLAVA T. NEDKOVA, DANIEL R. DENEV

ABSTRACT: *Digital gaming environments process significant amounts of personal data, creating both opportunities for improved user experience and challenges related to information security. This paper examines the main aspects of user data protection in gaming platforms by analyzing the types of collected data, key cybersecurity risks, protection technologies, and the applicable regulatory framework. The study emphasizes the importance of cooperation between developers, service providers, regulatory authorities, and users to ensure effective protection of personal information.*

KEYWORDS: *digital games, personal data, cybersecurity*

DOI: https://doi.org/10.46687/MT26BTN

ЗАЩИТА НА ПОТРЕБИТЕЛСКИТЕ ДАННИ В ДИГИТАЛНИТЕ ИГРОВИ СРЕДИ

БОРИСЛАВА Т. НЕДКОВА, ДАНИЕЛ Р. ДЕНЕВ

АБСТРАКТ: *Дигиталните игрови среди обработват значителни обеми лични данни, което създава както възможности за подобряване на потребителското изживяване, така и предизвикателства, свързани със защитата на информацията. Докладът разглежда основните аспекти на защитата на потребителските данни чрез анализ на събираната информация, основните рискове за киберсигурността, използваните технологии за защита и приложимата нормативна рамка. Подчертава се необходимостта от съвместни усилия между разработчици, доставчици на услуги, регулаторни органи и потребители за ефективна защита на личната информация.*

1 Въведение

Развитието на информационните технологии доведе до значително разширяване на дигиталната игрова индустрия. Онлайн игрите вече не представляват единствено средство за развлечение, а сложни виртуални екосистеми, в които милиони потребители ежедневно обменят информация и взаимодействат помежду си. Това превръща защитата на потребителските данни в особено важен въпрос. С нарастването на броя на играчите се увеличава и количеството събирана информация. Игровите компании използват данните за управление на потребителски профили, анализ на игровото поведение и предлагане на персонализирано съдържание. Този процес създава множество ползи, но едновременно с това поражда и рискове за поверителността. Проблемите, свързани със сигурността на данните, стават все по-актуални поради увеличаващия се брой кибератаки срещу онлайн платформи. Хакерски пробиви могат да доведат до кражба на лична информация, финансови загуби и нарушаване на доверието между потребителите и организациите. Особено внимание следва да се обърне на факта, че значителна част от аудиторията на дигиталните игри е съставена от непълнолетни потребители. Това налага по-високи

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

стандарти за сигурност и по-строг контрол върху начина, по който се обработват личните данни. В условията на цифровизация защитата на информацията се превръща в стратегически фактор за устойчивото развитие на игровата индустрия. Компаниите трябва да инвестират в технологии и политики за сигурност, които да гарантират защита на своите потребители. Целта на настоящия доклад е да анализира основните предизвикателства и решения, свързани със защитата на потребителските данни в дигиталните игрови среди, както и да представи добри практики за повишаване на сигурността. На фиг. 1 е показана схема на защита на потребителските данни.



Фиг. 1. Защита на потребителски данни в дигитални игри

2 Събиране и обработка на потребителски данни в игровите платформи

Съвременните игрови платформи функционират чрез събиране на различни видове информация за своите потребители. При регистрация обикновено се изискват основни данни като потребителско име, електронна поща и дата на раждане. Тази информация служи за създаване и управление на потребителски профили. Освен основните регистрационни данни, платформите често събират техническа информация за използваните устройства. Това включва IP адрес, тип операционна система, хардуерни характеристики и данни за интернет връзката. Подобна информация се използва за оптимизиране на производителността и сигурността на услугите. Игровите компании анализират и поведението на потребителите по време на игра. Събират се данни за времето, прекарано в игра, предпочитани режими, честота на влизане и взаимодействие с други играчи. Чрез тези анализи разработчиците подобряват игровото съдържание и потребителското изживяване. В много случаи се обработват и финансови данни, свързани с покупки на виртуални предмети, абонаменти или допълнителни услуги. Тези данни изискват високо ниво на защита, тъй като тяхното компрометиране може да доведе до сериозни финансови последици за потребителите. Събирането на данни трябва да се извършва при спазване на принципите на прозрачност и законност. Потребителите трябва да бъдат ясно информирани каква информация се събира, за какви цели ще бъде използвана

и колко дълго ще бъде съхранявана. Това е основен елемент от защитата на личната неприкосновеност. Таблица 1 показва събирани данни от игровите платформи.

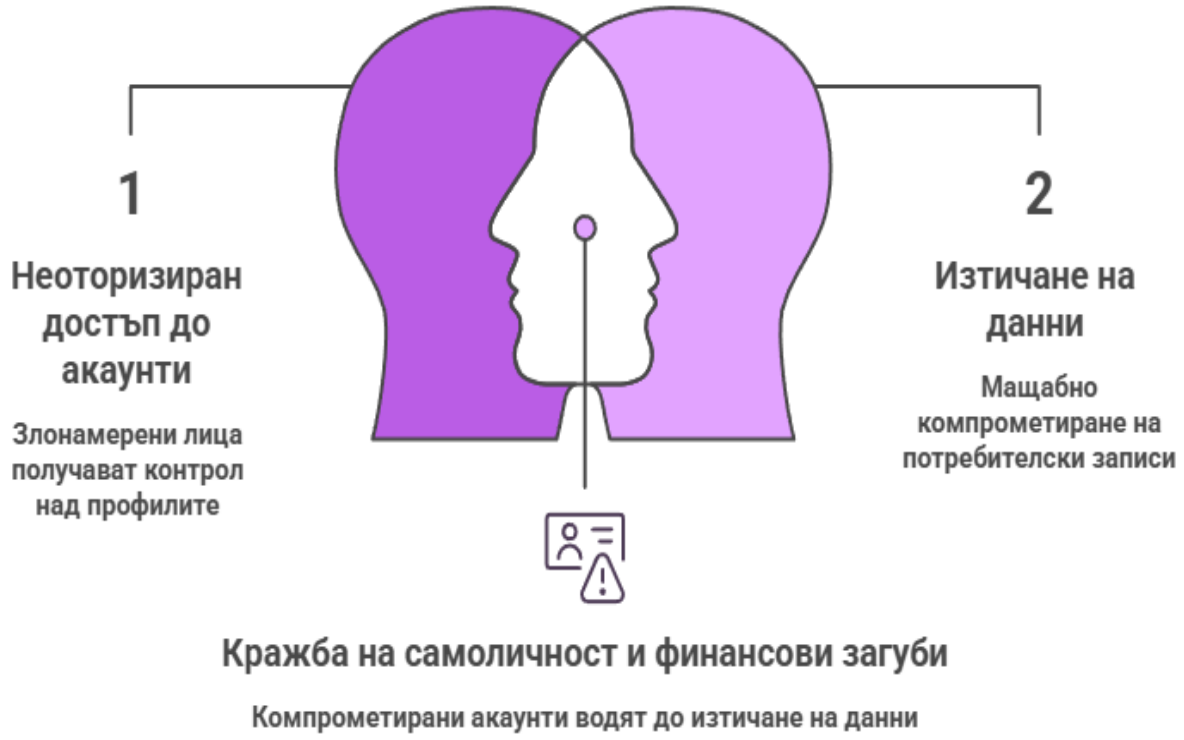
Таблица 1. Видове потребителски данни, събирани в игровите платформи

Вид данни	Примери	Цел на събирането	Потенциални рискове
Лични данни	Потребителско име, имейл адрес, дата на раждане	Създаване и управление на потребителски профил	Кражба на самоличност, неоторизиран достъп
Данни за удостоверяване	Пароли, кодове за достъп	Осигуряване на сигурен вход в системата	Пробив в акаунтите при слаба защита
Технически данни	IP адрес, устройство, операционна система	Подобряване на производителността и сигурността	Проследяване на потребителската активност
Данни за игрово поведение	Време на игра, постижения, предпочитания	Анализ и персонализиране на съдържанието	Нарушаване на поверителността
Комуникационни данни	Чат съобщения, форумни публикации	Поддръжка на социално взаимодействие между играчите	Тормоз, изтичане на лична информация
Финансови данни	Банкови карти, покупки в играта, абонаменти	Обработка на плащания и транзакции	Финансови измами и кражба на средства
Данни за местоположение	GPS информация, регион на достъп	Регионални услуги и защита на акаунта	Нежелано проследяване на потребителя

3 Основни рискове за сигурността на потребителските данни

Един от най-сериозните рискове в дигиталните игрови среди е неоторизираният достъп до потребителски акаунти. Заплахите за игровата индустрия и съвременните киберзаплахи са разгледани в [2, 10]. Злонамерени лица често използват фишинг атаки, злонамерен софтуер или откраднати пароли, за да получат достъп до профилите на играчите. Изтичането на данни представлява друга съществена заплаха. При успешна атака срещу игрова платформа могат да бъдат компрометирани милиони потребителски записи. Това включва лична информация, финансови данни и история на потребителската активност. Социалното инженерство също е широко разпространен метод за атака. Престъпниците често се представят за представители на игрови компании или за други играчи, за да получат поверителна информация. Този тип атаки разчитат предимно на човешки грешки и недостатъчна информираност. Особено уязвими са младите потребители, които невинаги разпознават потенциалните опасности в онлайн среда. Те могат лесно да споделят лични данни или да станат жертва на измамни практики, което увеличава риска от злоупотреби. Последиците от нарушенията на сигурността могат да бъдат значителни. Освен финансови загуби и кражба на самоличност, подобни инциденти

водят до загуба на доверие към платформите и могат да нанесат сериозни репутационни щети на организациите, които ги управляват. Фиг. 2 показва схема на пресичане на заплахи.

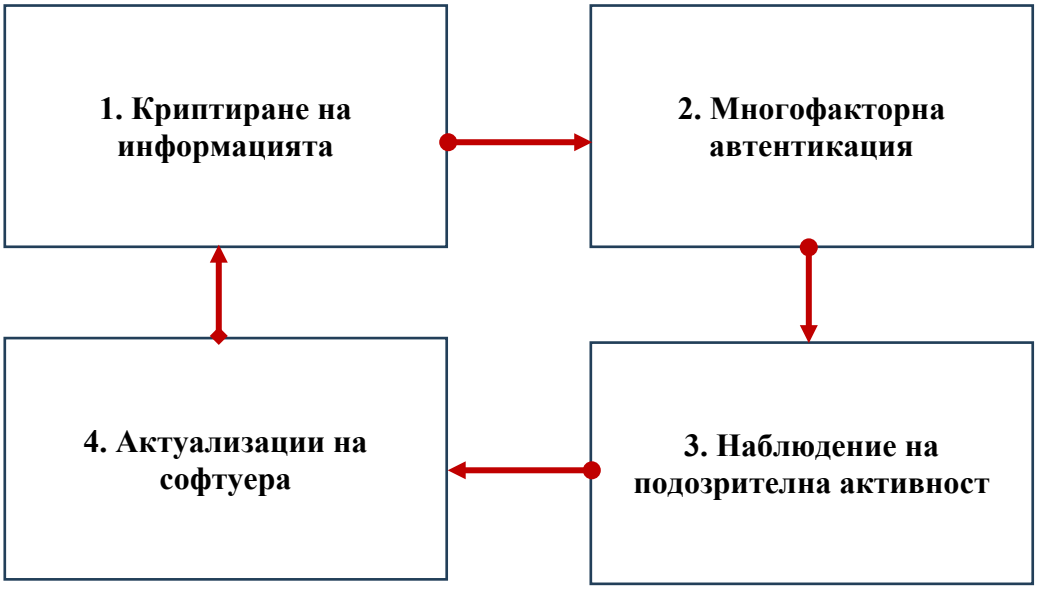


Фиг. 2. Пресичащи се заплахи за сигурността на онлайн игрите

4 Технологии и механизми за защита на потребителските данни

Развитието на дигиталните технологии доведе до създаването на разнообразни механизми за защита на личната информация в игровите среди. Тези технологии имат за цел да предотвратят неоторизиран достъп до данни и да гарантират сигурността на потребителските профили. С нарастването на киберзаплахите използването на надеждни средства за защита става все по-необходимо. Един от най-разпространените методи за защита е криптирането на информацията. Чрез него данните се преобразуват в специален формат, който може да бъде разчетен единствено от упълномощени лица или системи. Това означава, че дори при прихващане на информацията от трети страни тя остава неразбираема и практически неизползваема без необходимия ключ за декриптиране. Приложението на нелинейни функции за защита на информацията в комуникационни системи е разгледано в [1]. Друга важна технология е многофакторната автентикация. Тя изисква потребителят да потвърди своята самоличност чрез повече от един метод за удостоверяване. Например освен парола може да бъде изискан код, изпратен на мобилен телефон или генериран от специално приложение. Този подход значително намалява риска от неправомерен достъп до акаунти. Игровите компании използват и системи за наблюдение на подозрителна активност. Чрез автоматизирани алгоритми се откриват необичайни действия като многократни неуспешни опити за вход, влизане от необичайни локации или внезапни промени в поведението на потребителя. При установяване на подобни действия системата може временно да ограничи достъпа или да поиска допълнително потвърждение на самоличността. Съществена роля играят и редовните актуализации на софтуера. Уязвимостите в системите могат да бъдат

използвани от злонамерени лица за достъп до чувствителна информация. Чрез своевременното прилагане на актуализации и корекции се намалява вероятността подобни слабости да бъдат експлоатирани. Сигурността при програмиране с JavaScript е разгледана в [9]. По този начин технологичните решения се превръщат в основен инструмент за гарантиране на сигурността в дигиталните игрови среди. Фиг. 3 е показана схема на цикъла на сигурността.



Фиг. 3. Цикъл на сигурността в дигиталните игрови среди

5 Законодателна и регулаторна рамка за защита на данните

Правните аспекти на киберсигурността, поверителността и защитата на данните в ЕС са разгледани в [3, 6], а прилагането на GDPR е предмет на [5, 7, 8]. Специализирани изследвания разглеждат обработката на данни за проследяване на ботнети [4] и автоматизираното вземане на решения [11].

Защитата на личните данни не зависи единствено от технологиите, а и от съществуването на ясни правни норми. През последните години държавите и международните организации разработиха множество регулации, които определят как трябва да се събират, обработват и съхраняват потребителските данни. Тези правила имат за цел да защитят правата на гражданите в цифровата среда. Един от най-значимите нормативни актове е Общият регламент относно защитата на данните (GDPR) на Европейския съюз. Той въвежда строги изисквания към организациите относно прозрачността при обработката на лична информация. Компаниите са задължени ясно да информират потребителите за начина, по който използват техните данни. Регламентът предоставя и редица права на потребителите. Сред тях са правото на достъп до личните данни, правото на коригиране на неточна информация и правото на изтриване на данни при определени условия. Тези механизми дават възможност на хората да упражняват по-голям контрол върху собствената си информация. Особено внимание се отделя на защитата на децата в онлайн среда. Много законодателства изискват специални мерки при обработката на данни на непълнолетни лица. Игровите компании трябва да гарантират, че информацията на младите потребители се обработва по сигурен и отговорен начин. Спазването на

нормативните изисквания е важно както за потребителите, така и за организациите. Нарушенията могат да доведат до значителни финансови санкции и репутационни щети. Поради тази причина законодателната рамка играе ключова роля за изграждането на доверие и сигурност в дигиталните игрови среди.

КАЗУС: Онлайн игрова платформа разполага с общо 12 000 регистрирани потребители. След вътрешен одит са установени следните данни:

— 10 800 потребители са дали изрично съгласие за обработка на данните си.
— 600 потребители са активирали двуфакторна автентикация.
— 11 400 профила използват силни пароли.
— 300 потребители са подали искане за изтриване на данни.
— 270 от исканията са обработени в законовия срок.

При проверка са открити 180 профила с непълна информация относно съгласието за обработка на данни.

Задача 1: Процент потребители с дадено съгласие

$$P_1 = \frac{\text{Брой потребители със съгласие}}{\text{Общ брой потребители}} \times 100 \quad (1)$$

$$P_1 = \frac{10800}{12000} \times 100 = 0{,}9 \times 100 = 90\% \quad (2)$$

Задача 2: Процент потребители с двуфакторна автентикация

$$P_2 = \frac{9600}{12000} \times 100 = 0{,}8 \times 100 = 80\% \quad (3)$$

Задача 3: Процент профили със силни пароли

$$P_3 = \frac{11400}{12000} \times 100 = 0{,}95 \times 100 = 95\% \quad (4)$$

Задача 4: Процент изпълнени искания за изтриване на данни

$$P_4 = \frac{270}{300} \times 100 = 0{,}9 \times 100 = 90\% \quad (5)$$

Задача 5: Процент профили с установени несъответствия

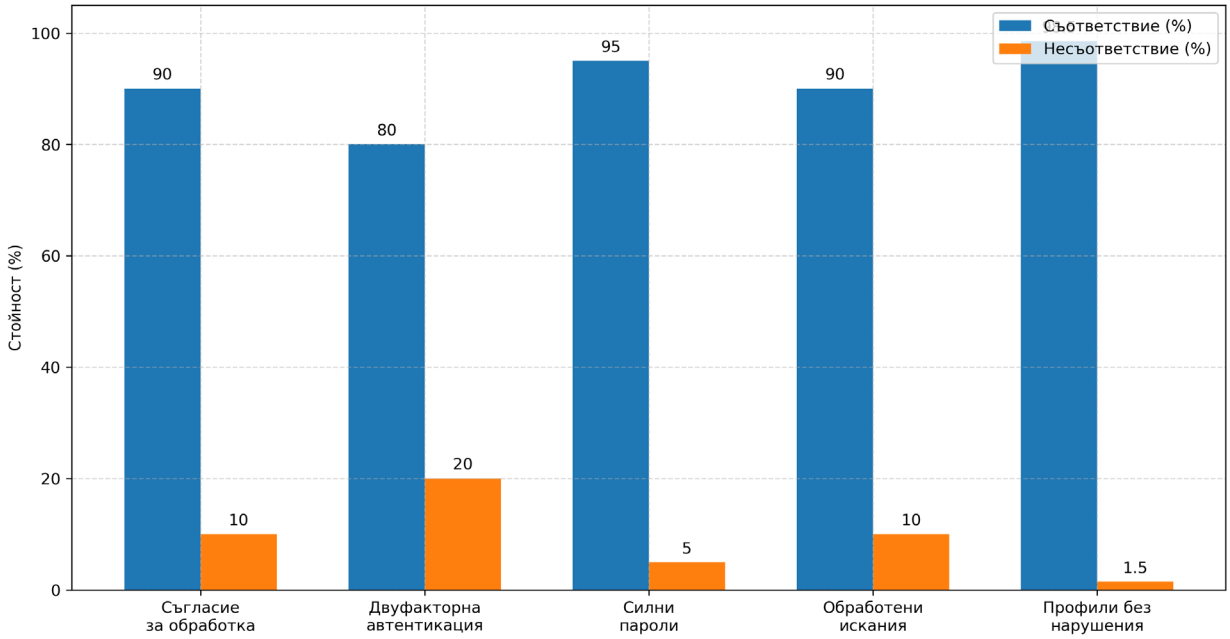
$$P_5 = \frac{180}{12000} \times 100 = 0{,}015 \times 100 = 1{,}5\% \quad (6)$$

Общ показател за съответствие

Нека се изчисли среден процент на съответствие чрез използване на четирите основни показателя:

$$C = \frac{P_1+P_2+P_3+P_4}{P_{ОБЩ}} = \frac{90+80+95+90}{4} = \frac{355}{4} = 88{,}75\% \quad (7)$$

Заключение по казуса: Полученият показател за съответствие е 88,75%, което показва високо ниво на спазване на изискванията за защита на личните данни. Въпреки това организацията следва да подобри използването на двуфакторна автентикация и да отстрани установените несъответствия при обработката на потребителските данни. Това ще повиши нивото на сигурност и ще намали риска от нарушения на регулаторните изисквания. На фиг. 4 са показани показатели за защита на данните в игровата платформа.



Фиг. 4. Показатели за защита на данните в игровата платформа

6 Ролята на разработчиците и игровите компании

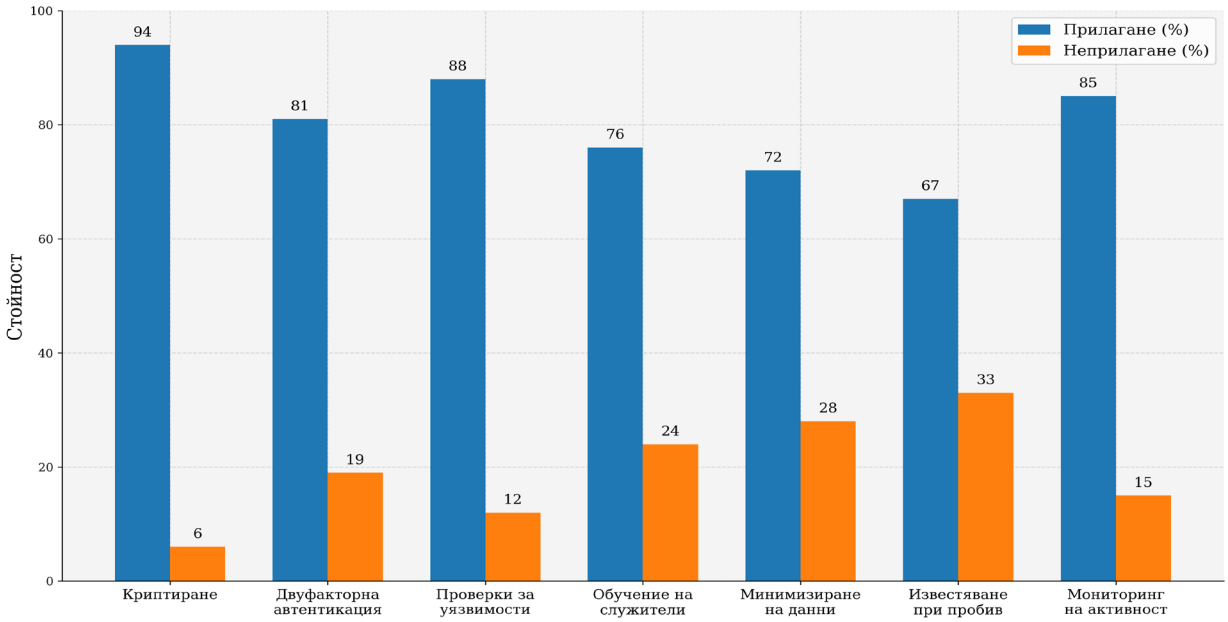
Разработчиците на игри и компаниите, които управляват игровите платформи, носят основна отговорност за сигурността на потребителските данни. Те определят начина, по който се събира и обработва информацията, както и мерките за нейното съхранение и защита. Следователно тяхната роля е решаваща за изграждането на безопасна дигитална среда. Една от най-важните задачи на организациите е прилагането на принципа за защита на данните още при проектирането на системите. Това означава сигурността да бъде заложена в самата архитектура на платформата, а не да се добавя като допълнителен елемент на по-късен етап. Подобен подход намалява риска от възникване на сериозни уязвимости. Компаниите трябва също така да ограничават събирането на информация само до данните, които са действително необходими за предоставянето на услугата. Прекомерното събиране на информация увеличава риска при евентуален пробив и затруднява управлението на сигурността. Важен аспект е обучението на служителите, които работят с чувствителна информация. Човешкият фактор остава една от основните причини за инциденти, свързани със сигурността. Поради това организациите трябва редовно да провеждат обучения и да изграждат култура на информационна сигурност. Освен технически и организационни мерки, компаниите трябва да поддържат открита комуникация с потребителите. При възникване на инциденти е важно засегнатите лица да бъдат своевременно уведомени и да получат информация за необходимите действия. По този начин се повишава доверието и се намаляват негативните последици от евентуални

нарушения на сигурността. Таблица 2 показва прилаганите мерки от игровите компании за защита на потребителските данни.

Таблица 2. Прилагани мерки от игровите компании

Мярка за защита	Брой платформи (от 100)	Процент (%)
Криптиране на потребителските данни	94	94
Двуфакторна автентикация	81	81
Редовни проверки за уязвимости	88	88
Обучение на служителите по киберсигурност	76	76
Политика за минимизиране на данните	72	72
Автоматично известяване при пробив	67	67
Система за мониторинг на подозрителна активност	85	85

От представените данни се наблюдава, че най-разпространената практика сред игровите компании е използването на криптиране на потребителските данни, което се прилага от 94% от платформите. Висок дял имат също редовните проверки за уязвимости (88%) и системите за мониторинг на подозрителна активност (85%), което показва стремеж към превантивна защита. По-ниски стойности се наблюдават при политиките за минимизиране на данните (72%) и автоматичното уведомяване на потребителите при инциденти (67%). Това показва, че част от организациите все още не прилагат напълно принципите за прозрачност и ограничаване на обработваната информация. Обучението на служителите по киберсигурност е въведено в 76% от платформите, което потвърждава значението на човешкия фактор за защитата на данните. Резултатите показват, че въпреки широкото разпространение на техническите мерки, организационните практики продължават да се нуждаят от допълнително развитие. На фиг. 5 е показана диаграма на резултатите.



Фиг. 5. Резултати от прилагани мерки

7 Добри практики за потребителите при защита на личните данни

Въпреки че организациите носят значителна отговорност за сигурността, самите потребители също играят важна роля в процеса на защита на личните данни. Чрез прилагането на добри практики те могат значително да намалят риска от злоупотреби и неоторизиран достъп до своите профили. Една от най-важните мерки е използването на силни и уникални пароли. Много потребители продължават да използват лесни за отгатване комбинации или една и съща парола за множество услуги. Това улеснява злоумишлениците и увеличава вероятността от компрометиране на акаунтите. Активирането на многофакторна автентикация представлява допълнително ниво на защита. Дори при кражба на парола нападателят няма да може лесно да получи достъп до профила без втория фактор за удостоверяване. Поради това все повече платформи препоръчват или изискват използването на подобни механизми. Потребителите трябва да бъдат внимателни и при споделянето на лична информация в игровите среди. Онлайн игрите често включват чатове, форуми и социални функции, които създават възможност за комуникация с непознати лица. Разкриването на чувствителни данни може да доведе до различни форми на злоупотреба. Необходимо е също така редовно да се актуализират устройствата и приложенията, използвани за достъп до игровите платформи. Проблемите на информационната сигурност при мобилни устройства са разгледани в [12]. Актуализациите съдържат корекции на уязвимости и подобрения в сигурността. Съчетаването на техническа защита и информирано потребителско поведение е ключов фактор за намаляване на рисковете в дигиталната среда. Друг важен аспект от защитата на личните данни е редовното преглеждане на настройките за поверителност в игровите платформи. Много потребители не обръщат внимание на разрешенията, които предоставят при регистрация или използване на допълнителни услуги. Периодичната проверка на настройките позволява ограничаване на достъпа до чувствителна информация и контрол върху данните, които се споделят с трети страни [5, 8].

8 Заключение

Защитата на потребителските данни в дигиталните игрови среди представлява едно от най-важните предизвикателства пред съвременната игрова индустрия. С развитието на онлайн платформите и увеличаването на броя на потребителите значението на информационната сигурност продължава да нараства. Личните данни се превръщат в ценен ресурс, който изисква надеждна защита. Анализът показа, че игровите платформи събират разнообразна информация за своите потребители, включително лични, технически и финансови данни. Тези данни са необходими за функционирането и развитието на услугите, но същевременно създават рискове, свързани с тяхното неправомерно използване или компрометиране. Съществуват различни заплахи за сигурността, сред които кибератаки, изтичане на информация, социално инженерство и злоупотреби с потребителски профили. За ограничаването на тези рискове се използват съвременни технологии като криптиране, многофакторна автентикация и системи за мониторинг на подозрителна активност. От съществено значение е и наличието на ефективна нормативна рамка, която да определя ясни правила за обработката на лични данни. Законодателството предоставя защита на потребителите и създава задължения за организациите, които работят с чувствителна информация. В заключение може да се посочи, че успешната защита на потребителските данни изисква съвместни усилия между разработчици, компании, държавни институции и самите потребители. Само чрез прилагането на комплексен подход, съчетаващ технологии,

регулации и информираност, може да бъде гарантирана сигурността и поверителността в съвременните дигитални игрови среди.

ЛИТЕРАТУРА:

[1] Цанков Ц. С. Приложения на нелинейните функции за защита на информацията в комуникационните системи. Университетско издателство „Епископ К. Преславски“, Шумен, 2018, 204 с., ISBN 978-619-201-212-0.

[2] Nardone M., Cybersecurity Threats and Attacks in the Gaming Industry: Secure Game Players' and Developers' Data and Systems, 2025, Apress, ISBN 979-8-8688-1491-4, pp. 1–106.

[3] Porcedda G., Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, 2023, Hart Publishing, ISBN 9781509939398, pp. 1–352.

[4] Böck L., Andersen M. F., Demetzou K., Karuppayah S., Mühlhäuser M., Vasilomanolakis E., Processing of Botnet Tracking Data under the GDPR, 2022, Computer Law & Security Review, Vol. 45, Article 105652, ISSN 0267-3649, pp. 1–18.

[5] Sharma S., Data Privacy and GDPR Handbook, 2019, Wiley, ISBN 9781119594246, pp. 1–496.

[6] Papakonstantinou V., De Hert P., The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play, 2024, Taylor & Francis, ISBN 9781040001608, pp. 1–154.

[7] Hublet F., Basin D., Krstić S., Enforcing the GDPR, 2024, Lecture Notes in Computer Science, Springer Nature Switzerland, pp. 400–422, DOI: 10.1007/978-3-031-51476-0_20.

[8] Besemer L., Privacy and Data Protection based on the GDPR, 2020, Van Haren Publishing, ISBN 9789401806787, pp. 1–340.

[9] Nikolov, L. G., Fetfov, O. M., Borisova, A. R. Security Concerns in JavaScript Coding. Proceedings of the Scientific Conference MATTEH 2018, Vol. 2, Part 2, Communication and Computer Technologies, Shumen, 2018, pp. 27–31, ISSN 1314-3921.

[10] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144, ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[11] Simeonova I. How GDPR treats automated decision-making. Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2025, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 164–175. https://doi.org/10.46687/jsar.v29i1.461

[12] Stoyanova, V. Problems with Information Security on Mobile Devices. Industry 4.0, 2019, p. 200. https://stumejournals.com/journals/i4/2019/4/200

THE ROLE OF ENCRYPTION IN THE SECURITY OF COMMUNICATION NETWORKS*

ILKER A. HATIB, ALEKS YA. DANEV

ABSTRACT: *Encryption is a fundamental mechanism for protecting information in modern communication networks. With the growth of digital technologies and the volume of exchanged data, the risks of unauthorized access, interception and manipulation of information also increase. This report examines the importance of encryption in ensuring the confidentiality, integrity and authenticity of data in communication networks. The main cryptographic methods, their application and the challenges to security in the modern digital environment are analyzed.*

KEYWORDS: *encryption, communication, networks*

DOI: https://doi.org/10.46687/MT26IAH

РОЛЯТА НА КРИПТИРАНЕТО ЗА СИГУРНОСТТА НА КОМУНИКАЦИОННИТЕ МРЕЖИ

ИЛКЕР А. ХАТИБ, АЛЕКС Я. ДАНЕВ

АБСТРАКТ: *Криптирането е основен механизъм за защита на информацията в съвременните комуникационни мрежи. С нарастването на цифровите технологии и обема на обменяните данни се увеличават и рисковете от неоторизиран достъп, прихващане и манипулиране на информацията. Настоящият доклад разглежда значението на криптирането за осигуряване на поверителност, цялостност и автентичност на данните в комуникационните мрежи. Анализирани са основните криптографски методи, тяхното приложение и предизвикателствата пред сигурността в съвременната цифрова среда.*

1 Въведение

Развитието на информационните и комуникационните технологии доведе до значително увеличаване на обмена на данни между потребители, организации и устройства. Интернет, мобилните комуникации и облачните услуги са се превърнали в неразделна част от ежедневието и бизнеса. В същото време нараства необходимостта от защита на чувствителната информация срещу кибератаки и злоупотреби. Криптирането представлява фундаментален инструмент за гарантиране на сигурността на комуникационните мрежи, като осигурява защита на данните по време на тяхното съхранение и предаване. Информационното общество се характеризира с непрекъснат обмен на данни между милиарди потребители и устройства по целия свят. Този процес създава значителни възможности за развитие на икономиката, образованието и науката, но едновременно с това поражда нови рискове за сигурността на информацията. Защитата на комуникационните канали се превръща в основно изискване за нормалното функциониране на съвременните цифрови системи. През последните десетилетия киберпрестъпността се развива с изключително бързи темпове, като атаките стават все по-сложни и трудно откриваеми. Хакерски групи, организирани престъпни организации и дори държавни структури използват разнообразни методи за получаване на достъп до чужди информационни ресурси.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

Това налага внедряването на надеждни механизми за защита още на ниво комуникационна инфраструктура. Комуникационните мрежи обхващат широк спектър от технологии – локални мрежи, мобилни системи, интернет платформи и сателитни комуникации. Всяка от тях е изправена пред специфични заплахи и уязвимости, които могат да доведат до компрометиране на обменяната информация. Поради тази причина сигурността трябва да бъде разглеждана като комплексен процес, включващ технически, организационни и управленски мерки [3, 4, 12]. Съвременните организации все по-често зависят от цифрови ресурси за изпълнение на ежедневните си дейности. Загубата на информация или нейната компрометация може да доведе до сериозни финансови загуби, прекъсване на работните процеси и увреждане на репутацията. В този контекст криптирането се утвърждава като един от най-надеждните инструменти за минимизиране на подобни рискове. Изследването на ролята на криптирането е от особено значение в условията на постоянно нарастваща дигитализация. Разбирането на неговите принципи, възможности и ограничения позволява по-ефективно изграждане на сигурни комуникационни среди и подпомага развитието на устойчиви информационни системи, способни да отговорят на съвременните изисквания за защита на данните. На фиг. 1 е показана необходимост от криптиране в комуникационните мрежи.

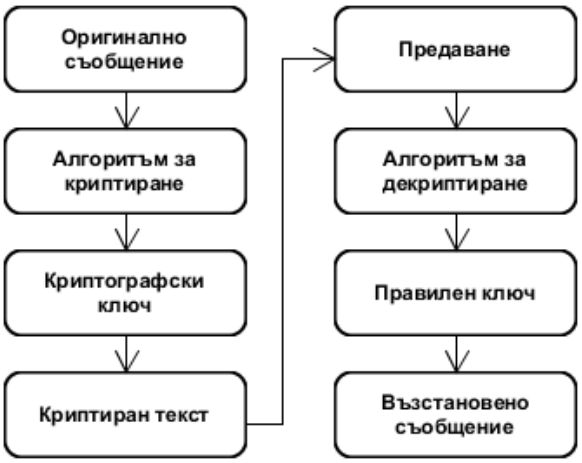


Фиг. 1. Необходимост от криптиране в комуникационните мрежи

2 Същност и принципи на криптирането

Криптирането представлява процес на преобразуване на информацията от четим вид в неразбираем формат чрез използване на математически алгоритми и криптографски ключове. Само лица или системи, които притежават съответния ключ за декриптиране, могат да възстановят оригиналното съдържание на съобщението. Основната цел на криптирането е да предотврати достъпа до информацията от неоторизирани лица, дори когато тя бъде прихваната по време на предаването. Криптографията има дълга история, която започва още в древността с използването на различни методи за скриване на съобщения. С развитието на математиката и компютърните науки криптирането се превръща в сложна дисциплина, основана на алгоритми и изчислителни модели. Днес то е неизменна част от информационната сигурност и защитата на цифровите комуникации. Основен елемент в криптографските системи е криптографският ключ. Неговата дължина и сложност оказват пряко влияние върху нивото на сигурност. Колкото по-дълъг е ключът, толкова по-трудно става неговото разбиване чрез методи за груба сила и други

криптоаналитични техники. Криптирането разчита на математически функции, които са лесни за изпълнение в една посока, но изключително трудни за обръщане без необходимия ключ. Именно тази характеристика осигурява устойчивостта на съвременните криптографски алгоритми срещу неоторизиран достъп. При проектирането на криптографски системи се вземат предвид различни видове атаки, включително анализ на трафика, статистически анализ и опити за разгадаване на ключовете. Това налага непрекъснато усъвършенстване на алгоритмите и методите за защита. Ефективността на криптирането зависи не само от използвания алгоритъм, но и от правилното управление на ключовете. Неправилното съхранение или разпространение на ключовете може да компрометира сигурността дори при използване на най-надеждните криптографски решения. На фиг. 2 е показан процесът на криптиране [1].



Фиг. 2. Основен процес на криптиране

3 Видове криптографски методи

Съществуват два основни вида криптографски системи – симетрично и асиметрично криптиране. При симетричното криптиране един и същ ключ се използва както за криптиране, така и за декриптиране на данните. Този метод се отличава с висока скорост и ефективност, което го прави подходящ за обработка на големи обеми информация. Асиметричното криптиране използва двойка ключове – публичен и частен. Публичният ключ служи за криптиране на информацията, докато частният се използва за нейното декриптиране. Този подход осигурява по-висока сигурност при обмена на ключове и е широко използван в интернет комуникациите. Симетричните алгоритми като AES са сред най-широко използваните решения за защита на информацията. Те предлагат висока производителност и са подходящи за криптиране на големи количества данни в реално време. Едно от основните предизвикателства при симетричното криптиране е сигурното разпределение на криптографския ключ между комуникиращите страни. Ако ключът бъде прихванат, защитата на информацията става неефективна. Асиметричните алгоритми като RSA и ECC решават проблема с обмена на ключове чрез използването на двойка свързани ключове. Това позволява сигурна комуникация между страни, които никога преди не са обменяли секретна информация. В практиката често се използват хибридни криптографски системи, които комбинират предимствата на симетричното и асиметричното криптиране.

По този начин се постига както висока сигурност, така и добра производителност. Освен криптиране на данни, съвременните криптографски методи включват и механизми за удостоверяване, управление на цифрови сертификати и защита на мрежовите протоколи. Това разширява значително приложението на криптографията извън обикновеното кодиране на информация. В таблица 1 са показани видовете криптографски методи и техните характеристики [1]. Приложението на криптографската защита в комуникационните мрежи е разгледано при протоколите TLS и SSL [2] и при изграждането на виртуални частни мрежи [5].

Таблица 1. Видове криптографски методи и техните характеристики

Вид криптиране	Принцип на работа	Предимства	Недостатъци	Примери
Симетрично криптиране	Един и същ ключ се използва за криптиране и декриптиране	Висока скорост, ниско натоварване на системата	Трудно сигурно разпространение на ключа	AES, DES, 3DES, Blowfish
Асиметрично криптиране	Използват се два ключа – публичен и частен	По-сигурен обмен на ключове, висока надеждност	По-бавно от симетричното криптиране	RSA, ECC, ElGamal
Хибридно криптиране	Комбинира симетрично и асиметрично криптиране	Съчетава скорост и сигурност	По-сложна реализация	TLS/SSL, HTTPS
Хеширане	Генерира уникален цифров отпечатък на данните	Проверка на целостта на информацията	Не позволява възстановяване на оригиналните данни	SHA-256, SHA-3, MD5
Цифров подпис	Използва частен ключ за подписване и публичен за проверка	Автентичност и неотричане на авторството	Изисква инфраструктура за управление на ключове	RSA Signature, DSA, ECDSA

4 Роля на криптирането за поверителността на данните

Една от най-важните функции на криптирането е защитата на поверителността на информацията. В комуникационните мрежи ежедневно се обменят лични данни, финансови транзакции, корпоративна информация и други чувствителни ресурси. Криптирането гарантира, че дори ако данните бъдат прихванати от злонамерени лица, тяхното съдържание ще остане недостъпно без необходимия ключ за декриптиране. По този начин се намалява рискът от изтичане на информация и финансови загуби. Защитата на личните данни е сред основните причини за използването на криптиране в съвременните комуникационни мрежи. Потребителите ежедневно споделят чувствителна информация, която трябва да бъде защитена от неправомерен достъп. Електронната търговия е пример за сфера, в която криптирането играе критична роля. Данните за банкови карти и финансови транзакции се предават чрез защитени канали, което намалява риска от измами и кражба на информация.

В здравеопазването криптирането защитава медицинските досиета и резултатите от изследванията. Това е особено важно предвид високата чувствителност на медицинската информация и законовите изисквания за нейното съхранение. Облачните услуги също разчитат на криптографска защита, за да гарантират поверителността на съхраняваните данни. Чрез криптиране преди качване на информацията се ограничава възможността тя да бъде достъпна за неоторизирани лица. Поверителността на данните има не само техническо, но и социално значение. Загубата на контрол върху личната информация може да доведе до финансови щети, нарушаване на личното пространство и загуба на доверие в цифровите услуги. Друг подход за поверително предаване на информация е стеганографията, при която се прикрива наличието на съобщение [13]. Откриването на скрита информация чрез визуална стеганализа е разгледано в [6]. Данните в таблица 2 показват същественото значение на криптирането за осигуряване на поверителността на информацията в комуникационните мрежи. При използване на криптографска защита вероятността за неоторизиран достъп и изтичане на чувствителни данни намалява многократно, докато нивото на защита и доверието на потребителите значително се повишават. Същевременно времето, необходимо за компрометиране на защитената информация, нараства драстично, което затруднява потенциалните нападатели и повишава цялостната сигурност на комуникационната среда.

Таблица 2. Влияние на криптирането върху сигурността на данните

Показател	Без криптиране	С криптиране
Вероятност за успешен неоторизиран достъп (%)	85	10
Риск от изтичане на чувствителни данни (%)	80	15
Време за компрометиране на информацията (минути)	5	> 10 000
Ниво на защита на личните данни (%)	20	95
Доверие на потребителите (%)	45	90

5 Осигуряване на цялостност и автентичност на информацията

Освен поверителност, криптографските технологии осигуряват и цялостност на данните. Чрез използването на хеш-функции и цифрови подписи може да се установи дали информацията е била променяна по време на предаването. Цифровите подписи също така позволяват удостоверяване на самоличността на изпращача, като гарантират, че съобщението действително произхожда от посочения източник. Това е особено важно при електронните плащания, електронното управление и бизнес комуникациите. Цялостността на данните гарантира, че информацията не е била променяна по време на предаването или съхранението ѝ. Това е особено важно при обмен на финансови документи и критична бизнес информация. Хеш-функциите са ключов инструмент за проверка на цялостността на данните. Те генерират уникална стойност, която се променя дори при минимална промяна на съдържанието на съобщението. Цифровите подписи предоставят възможност за удостоверяване на автора на дадено съобщение или документ. Те създават механизъм за доказване на произхода на информацията и предотвратяват отричането на извършени действия. На фиг. 3 са показани механизми за осигуряване на цялостност и автентичност [1].

В електронното управление цифровите подписи позволяват извършването на административни услуги по електронен път. Това улеснява комуникацията между гражданите и институциите и намалява необходимостта от физическо присъствие. Съвременните системи за електронно банкиране използват множество криптографски механизми за гарантиране на автентичността на потребителите. Това включва сертификати, еднократни пароли и други средства за силно удостоверяване.



Фиг. 3. Механизми за осигуряване на цялостност и автентичност

6 Предизвикателства и бъдещо развитие на криптирането

Въпреки високата степен на защита, която криптирането предоставя, съществуват редица предизвикателства пред неговото развитие. Нарастващата изчислителна мощност на компютрите и развитието на квантовите технологии поставят под въпрос сигурността на някои от съществуващите криптографски алгоритми. Поради тази причина научната общност активно разработва нови криптографски решения, известни като постквантова криптография, които да осигурят надеждна защита и в бъдеще. Развитието на квантовите компютри представлява едно от най-сериозните предизвикателства пред съществуващите криптографски системи. Очаква се бъдещите квантови технологии да могат да извършват изчисления, които днес са практически невъзможни. Постквантовата криптография се разработва с цел създаване на алгоритми, устойчиви на атаки от квантови компютри. Тези решения са обект на активни научни изследвания и международна стандартизация. Нарастващият брой свързани устройства увеличава сложността на управлението на криптографските ключове. Това налага разработването на автоматизирани системи за управление и обновяване на защитните механизми. Друг проблем е балансът между сигурност и производителност. По-високите нива на криптографска защита често изискват повече изчислителни ресурси, което може да повлияе на скоростта на комуникациите. Забавянето при криптиране и декриптиране на глас, предаван през VPN мрежи, е предмет на аналитично изследване в [7]. Бъдещето на криптирането е свързано с интегрирането на нови технологии, включително изкуствен интелект и машинно обучение. Тези технологии могат да подпомогнат откриването на уязвимости и подобряването на криптографските системи в условията на непрекъснато развиващи се киберзаплахи. Свързани направления

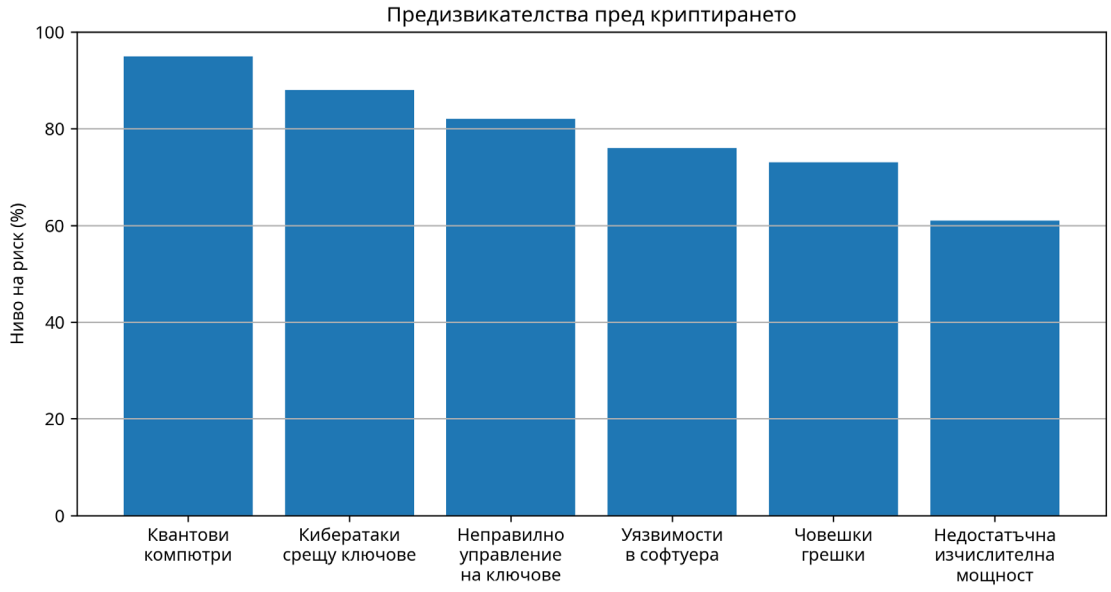
са моделирането на сигурността при мрежово кодиране [8], анализът на комуникациите с Wireshark [9], компютърната сигурност и управлението на мрежовия трафик [10], както и киберсигурността в мултимедийните мрежи на автоматизирани системи [11].

Таблица 3 представя основните предизвикателства пред развитието на съвременните криптографски системи. Най-сериозен потенциален риск представлява развитието на квантовите компютри, които могат да компрометират част от използваните днес алгоритми за криптиране. Значително влияние оказват също атаките срещу криптографските ключове и грешките при тяхното управление, тъй като дори надеждните алгоритми могат да бъдат компрометирани при неправилно използване. Данните показват необходимостта от разработване на нови постквантови решения и усъвършенстване на механизмите за управление на сигурността, които да гарантират надеждна защита на информацията в бъдеще.

Таблица 3. Основни предизвикателства пред криптирането и тяхното влияние

Предизвикателство	Ниво на риск (%)
Квантови компютри	95
Кибератаки срещу ключове	88
Неправилно управление на ключове	82
Уязвимости в софтуера	76
Недостатъчна изчислителна мощност	61
Човешки грешки	73

Анализът на данните, представени на фиг. 4, потвърждава, че бъдещото развитие на криптографията ще бъде силно повлияно от технологичния напредък и еволюцията на киберзаплахите.



Фиг. 4. Ниво на риск при основните предизвикателства пред съвременните криптографски системи

Наблюдава се значителна разлика между отделните рискови фактори, като най-високи стойности са отчетени при квантовите компютри и атаките срещу криптографските ключове. Това показва, че научните изследвания и инвестициите в областта на информационната сигурност трябва да бъдат насочени към разработването на по-устойчиви алгоритми и усъвършенствани механизми за защита. Същевременно наличието на рискове, свързани с човешкия фактор и софтуерните уязвимости, подчертава необходимостта от комплексен подход, който съчетава технологични решения, организационни мерки и повишаване на квалификацията на потребителите и специалистите по киберсигурност.

7 Заключение

Криптирането играе ключова роля за сигурността на комуникационните мрежи и е основен елемент от съвременната киберсигурност. То осигурява поверителност, цялостност и автентичност на информацията, като защитава потребителите и организациите от множество заплахи. С развитието на технологиите необходимостта от усъвършенстване на криптографските методи ще продължи да нараства. Ефективното прилагане на криптирането остава критичен фактор за сигурното функциониране на цифровото общество и защитата на информационните ресурси. Анализът на криптографските технологии показва, че те са сред най-ефективните средства за противодействие на заплахите в комуникационните мрежи. Независимо от непрекъснатото развитие на методите за атака, криптирането продължава да осигурява високо ниво на защита и остава основен компонент на съвременните системи за информационна сигурност. Практическото приложение на криптирането обхваща почти всички области на обществения и икономическия живот. От личната комуникация между потребителите до защитата на национални информационни ресурси, криптографските механизми допринасят за създаването на по-надеждна и сигурна цифрова среда. Успешното прилагане на криптографски решения изисква не само подходящи технологии, но и правилна организация на процесите по управление на сигурността. Обучението на потребителите, поддръжката на системите и редовното актуализиране на защитните механизми са също толкова важни, колкото и самите алгоритми за криптиране. В бъдеще значението на криптографията вероятно ще нараства успоредно с увеличаването на количеството цифрова информация и броя на свързаните устройства. Това ще наложи разработването на нови стандарти и подходи, способни да осигурят адекватна защита срещу все по-сложни киберзаплахи. Следователно криптирането не трябва да се разглежда единствено като технически инструмент, а като стратегически фактор за гарантиране на доверието, сигурността и устойчивото развитие на съвременните комуникационни мрежи.

ЛИТЕРАТУРА:

[1] Цанков Ц. С. Приложения на нелинейните функции за защита на информацията в комуникационните системи. Университетско издателство „Епископ К. Преславски“, Шумен, 2018, 204 с., ISBN 978-619-201-212-0.

[2] Denev D., Tsankov Ts., Use in Internet of Protocols Transport Layer Security and its Now-Deprecated Predecessor Secure Sockets Layer, 2018, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 94-101.

[3] Denev D., Konstantinova E., Cybersecurity – International and National Dimensions, 2019, Cadet-Students Scientific Conference, Collection of Papers, National Military University „Vasil Levski”, Veliko Tarnovo, ISSN 2367-7481, pp. 300-310.

[4] 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.

[5] Denev D., Tsankov Ts., Development of a Virtual Private Network in Computer Networks and Communication Environments, 2020, International scientific refereed online journal SocioBrains – Sofia: Smart ideas - wise decisions Ltd, Issue 71, ISSN 2367-5721, pp. 11-19.

[6] Terziev H., Denev D., Analysis of the Possibilities for Discovery of Information in the Communication Information Systems Through the use of Visual Steganalysis, 2020, Annual of Konstantin Preslavski University of Shumen, Vol. X E, Faculty of technical sciences, ISSN 1311-834X, pp. 229-233.

[7] Denev D., Analytical Study of the Delay Introduced as a Result of Encryption/Decryption of Voice Transmitted over a VPN Networks, 2021, Journal scientific and applied research, vol. 20, International Journal, ISSN 1314-6289, pp. 73-77.

[8] 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.

[9] 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.

[10] Iliev D., Denev D., Computer Security and Traffic Management in Communication Networks, Conference with international participation MATTEH 2024, Conference Proceedings, vol. 2 Communication and Computer Technologies, ISSN 1314-3921, pp. 161-169.

[11] Denev D., Petrov I., Cybersecurity in Multimedia Networks of Automated Systems, 2025, Annual of Konstantin Preslavski University of Shumen, Vol. XV E, Faculty of technical sciences, ISSN 1314-8818, pp. 61-73.

[12] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144. ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[13] Stoyanova, V. Steganography as a Means to Solve the Problem whit Transmitting Confidential Information. Proceedings of the International Conference on Technics, Technologies and Education ICTTE 2014, Yambol, 2014, pp. 496–502. ISSN 1314-9474.

STATE-BASED CYBERSECURITY MODEL FOR AUTOMATED AND ELECTRIC VEHICLES AND CHARGING INFRASTRUCTURE*

EMILI K. DIMITROVA, KOSTADIN D. KOSTADINOV

ABSTRACT: *The increasing connectivity of automated and electric vehicles integrates in-vehicle networks, charging equipment, backend management systems and cloud services into a common cyber-physical environment. This paper reviews the applicable communication standards and documented attack surfaces and proposes a state-based protection model for three operating conditions: driving, stationary software maintenance and charging. The model isolates safety-critical control functions from public networks while driving, permits firmware installation only in a verified stationary state, and requires signed update metadata, cryptographic integrity verification, secure boot and rollback protection. For charging infrastructure, the model combines authenticated communication with independent electrical safety interlocks. The proposal provides a traceable set of security requirements; experimental validation remains a subject of subsequent work.*

KEYWORDS: *automated vehicles, electric vehicles, charging infrastructure, secure software update, cybersecurity*

DOI: https://doi.org/10.46687/MT26EKD

МОДЕЛ ЗА КИБЕРСИГУРНОСТ СПОРЕД РЕЖИМА НА РАБОТА ПРИ АВТОМАТИЗИРАНИ И ЕЛЕКТРИЧЕСКИ ПРЕВОЗНИ СРЕДСТВА И ЗАРЯДНА ИНФРАСТРУКТУРА

ЕМИЛИ К. ДИМИТРОВА, КОСТАДИН Д. КОСТАДИНОВ

АБСТРАКТ: *Нарастващата свързаност на автоматизираните и електрическите превозни средства обединява бордовите мрежи, зарядното оборудване, системите за централно управление и облачните услуги в обща киберфизична среда. В доклада са анализирани приложимите комуникационни стандарти и документираните повърхности за атака и е предложен защитен модел за три режима: движение, софтуерно обслужване в покой и зареждане. При движение моделът изолира функциите за управление, свързани с безопасността, от публични мрежи; актуализиране на фърмуера се допуска само в проверено неподвижно състояние и след удостоверяване на източника, проверка с криптографски хеш и цифров подпис, защитено стартиране и защита срещу връщане към уязвима версия. За зарядната инфраструктура моделът съчетава удостоверена комуникация с независими електрически защити. Предложението формулира проследими изисквания, чието експериментално валидиране е предмет на последваща работа.*

1 Въведение

В научната и нормативната литература се разграничават електрически, свързани и автоматизирани превозни средства. Електрическото задвижване не предполага автоматизирано управление, а свързаността не е равнозначна на автономност. Съгласно SAE J3016 степента на автоматизация се определя чрез нива от 0 до 5, като термините следва да се използват според конкретните функции и разпределението на отговорностите между човека и системата [16]. В настоящия доклад „автоматизирано превозно средство“ се използва като обобщаващ термин за автомобил с функции за автоматизирано динамично

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

управление. Съвременните превозни средства съдържат електронни блокове за управление, сензори, вътрешни комуникационни мрежи и външни интерфейси. Тяхната свързаност с мобилни приложения, облачни услуги, зарядни станции и системи за управление на трафика разширява повърхността за атака. Общият контекст на съвременните киберзаплахи е разгледан в [11]. Успешното компрометиране на отделен интерфейс може да засегне поверителността и целостта на данните, наличността на услуги и при определени условия безопасността на движението. Поради това защитата трябва да обхваща едновременно бордовата електроника, комуникационните канали, системите за централно управление и зарядната инфраструктура и да се прилага през целия жизнен цикъл на системата [4, 7, 17]. Целта на изследването е да се разработи концептуален модел за защита според режима на работа на превозното средство и зарядната инфраструктура. Използван е сравнителен анализ на стандарти, нормативни документи и публикувани експериментални изследвания. Авторският принос се състои в формализиране на правила за мрежова изолация при движение, защитена актуализация само в неподвижно състояние и независимо ограничаване на опасните режими при зареждане.

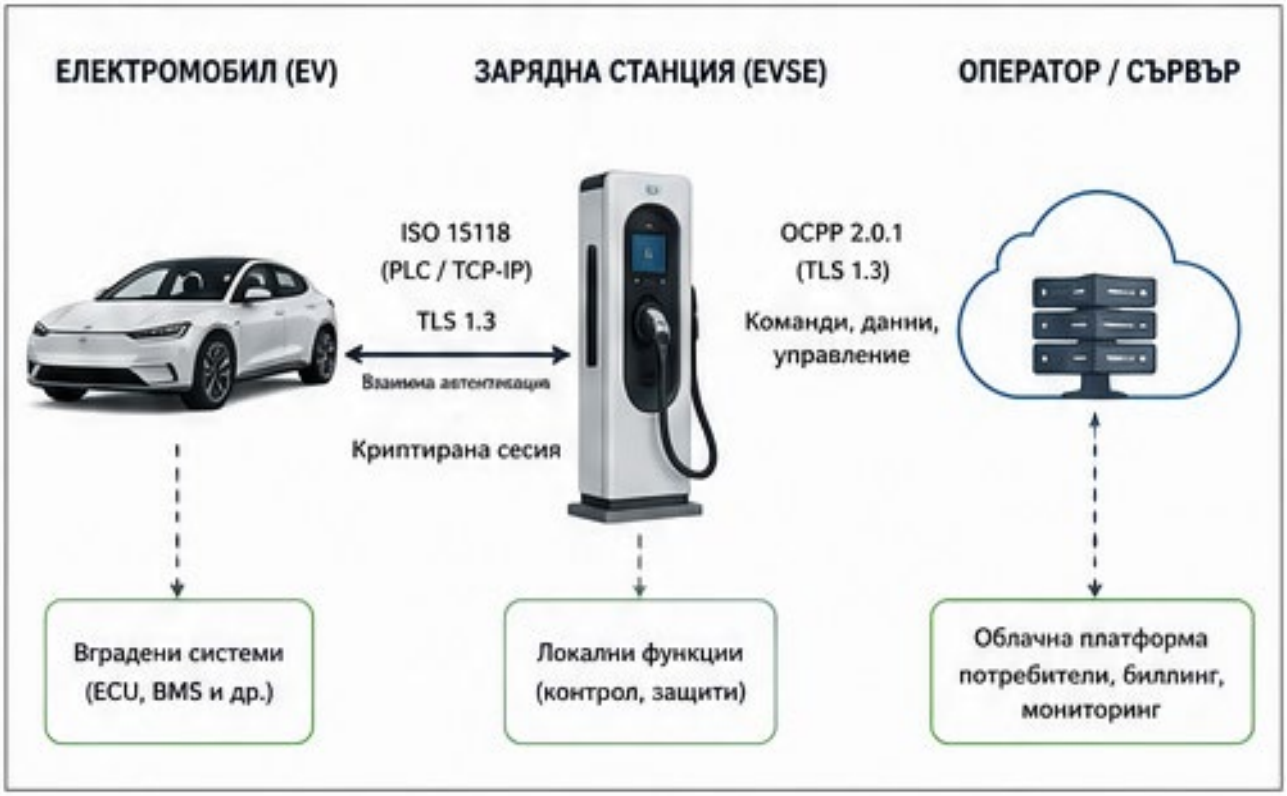


Фиг. 1. Концептуален модел на многослойна защита на автоматизирано превозно средство

2 Същност и принципи на комуникацията между автомобил и зарядна станция

Комуникацията между електрическото превозно средство и зарядната точка включва обмен на данни за установяване на връзката, договаряне на параметрите на зареждане, удостоверяване и управление на сесията. Основни участници са превозното средство,

зарядното оборудване (EVSE), операторът и системата за централно управление. ISO 15118 определя комуникацията между контролера в превозното средство (EVCC) и контролера в зарядното оборудване (SECC) [21]. OCPP определя обмена между зарядната станция и системата за централно управление, а IEC 63110 разглежда архитектурата и случаите на употреба при управлението на инфраструктура за зареждане и разреждане [2], [3]. Тези стандарти и протоколи имат различен обхват и не бива да се представят като взаимозаменяеми. Защитата на комуникацията изисква надеждно управление на цифрови сертификати и ключове, удостоверяване на участниците, защита на целостта и контрол на достъпа. Приложението на TLS и неговия предшественик SSL за защита на интернет комуникациите е разгледано в [1].



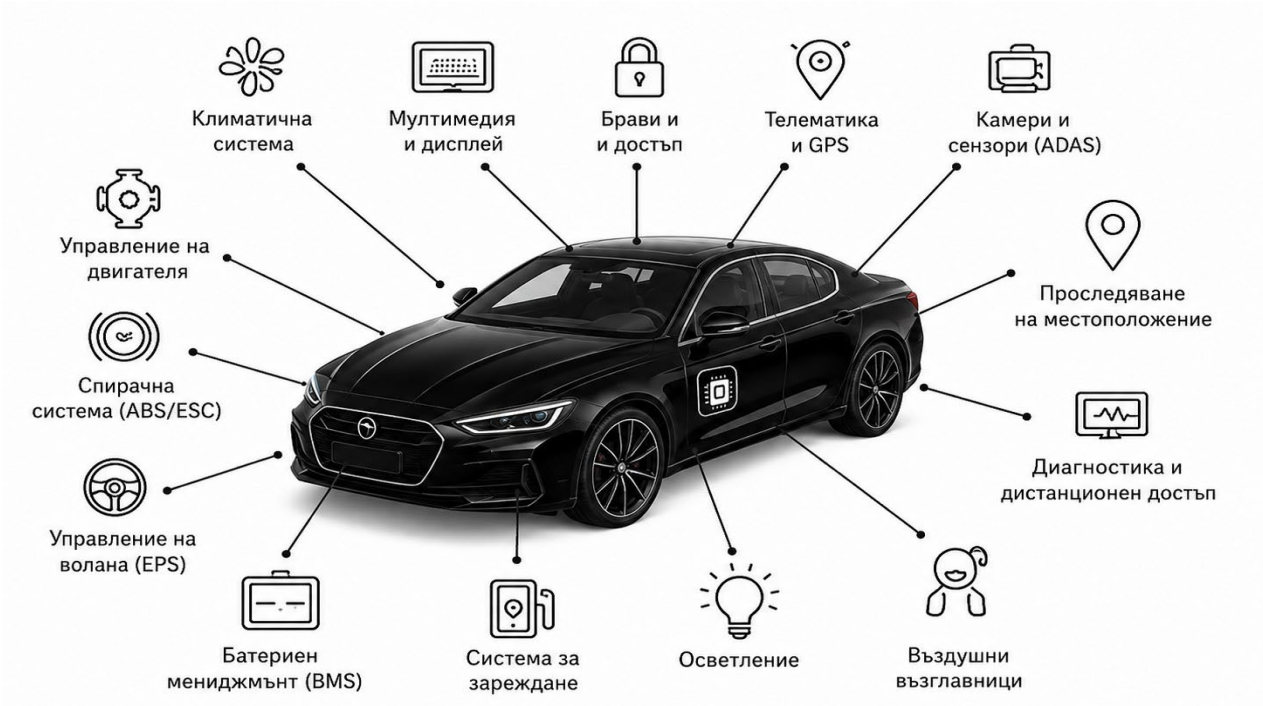
Фиг. 2. Основни комуникационни връзки в екосистемата за зареждане на електрически превозни средства

ISO 15118 е серия международни стандарти за комуникационния интерфейс между електрическо превозно средство и зарядно оборудване. Отделните части определят физическия и каналния слой, мрежовите и приложните изисквания и изпитванията за съответствие. ISO 15118-20:2022 описва второто поколение мрежови и приложни изисквания и поддържа услуги за двупосочен енергиен обмен [21]. OCPP е отворен приложен протокол, разработван от Open Charge Alliance, за комуникация между зарядна станция и система за централно управление. Версия 2.0.1 включва функционалности за управление на устройства, интелигентно зареждане, актуализация на софтуер и профили за сигурност; наличието на такива механизми обаче не гарантира защитена реализация без правилна конфигурация и управление на сертификатите [2]. IEC 63110-1:2022 определя основни понятия, случаи на употреба и архитектура за управление на инфраструктурата за

зареждане и разреждане [3]. Следователно оценката на сигурността трябва да отчита цялата комуникационна верига, а не само отделен протокол.

3 Основни комуникационни протоколи и технологии

Вътрешната комуникация в автомобила се реализира чрез различни мрежови технологии според изискванията за скорост, детерминираност, цена и функционална безопасност. CAN се използва широко за обмен между електронни блокове за управление. Класическият протокол не осигурява самостоятелно удостоверяване на източника и криптографска защита на всяко съобщение, поради което защитата разчита на архитектурни мерки като сегментиране, защитени шлюзове, филтриране и наблюдение на трафика [6], [9]. LIN се използва предимно за по-нискоскоростни периферни функции, а FlexRay е разработен за детерминирана комуникация и резервираност. Automotive Ethernet се прилага при функции с по-високи изисквания към пропускателната способност. Изборът на шина не отменя необходимостта от анализ на заплахите и управление на риска съгласно ISO/SAE 21434 [4].



Фиг. 3. Основни компоненти и комуникационни интерфейси в съвременно превозно средство

Външните интерфейси включват клетъчни мрежи, Wi-Fi, Bluetooth, системи за глобална навигация, диагностични портове, мобилни приложения и комуникация със зарядната инфраструктура. Всеки интерфейс има различен модел на заплахите. При взаимодействието с мобилни приложения значение имат и проблемите на информационната сигурност на мобилните устройства [15]. Рискът зависи не само от технологията, а и от конкретната реализация, конфигурацията, възможностите за отдалечен достъп и връзките с критични бордови функции. Поради това общи твърдения от типа „безжичната връзка е несигурна“ са недостатъчни; необходим е систематичен анализ на активите, заплахите, уязвимостите и възможните последствия [4], [8].

4 Заплахи и уязвимости при свързаните и автоматизираните превозни средства

Основните категории заплахи включват неоторизиран достъп, подправяне или повторно изпращане на съобщения, отказ на услуга, компрометиране на софтуерни актуализации и идентификационни данни, както и атаки срещу сензори и външни услуги [7], [8]. Атака „посредник“ (man-in-the-middle) е възможна, когато нападателят може да прихваща и изменя обмена между две страни, а използваните механизми не осигуряват надеждно взаимно удостоверяване и защита на целостта. При зарядната инфраструктура обект на защита са зарядното оборудване, системата за централно управление, потребителските приложения, платежните услуги и връзките с електроенергийната система. Потенциалните последствия включват прекъсване на зареждането, неправомерен достъп до данни и акаунти, манипулиране на сесии и използване на компрометиран компонент като отправна точка към други системи. Конкретната вероятност и тежест не могат да бъдат определени без описана методика, контекст и емпирични данни.

Сензорните системи на автоматизираното превозно средство могат да бъдат повлияни чрез заслепяване, подправяне или подаване на подвеждащи входни данни. Камерите, радарите, лидарите и системите за глобална навигация имат различни физически принципи и съответно различни уязвимости. Анализите на автоматизирани превозни средства подчертават необходимостта от сензорна излишност, проверка за съгласуваност на данните, откриване на аномалии и безопасно преминаване към ограничен режим при недостоверни входни данни [7], [8]. Не всяка демонстрирана лабораторна атака е непосредствено приложима към серийно превозно средство; условията и ограниченията на експеримента трябва да бъдат посочвани.

Компрометирането на електронен блок за управление или на външен интерфейс може да осигури път към вътрешната автомобилна мрежа. Експериментални изследвания показват, че при недостатъчна изолация между домейните е възможно преминаване от некритичен интерфейс към функции с по-висока критичност [6], [9]. Подходящите противодействия включват защитени шлюзове, мрежово сегментиране, принцип на минималните привилегии, сигурно стартиране, проверка на целостта на софтуера, защитено управление на ключове и наблюдение на необичайно поведение. Тези мерки трябва да бъдат определени чрез проследим процес за анализ и управление на киберриска [4].

Таблица 1. Основни повърхности за атака и мерки за защита

Повърхност за атака	Примерен механизъм	Възможен ефект	Основна мярка
Външни безжични интерфейси	Неоторизиран достъп или подправяне на трафик	Достъп до данни или функции	Удостоверяване, актуализации, сегментиране
Вътрешна автомобилна мрежа	Инжектиране или повторение на съобщения	Нарушаване на комуникацията между ECU	Защитен шлюз, филтриране, наблюдение
Сензори и навигация	Заслепяване или подаване на подвеждащи данни	Неправилна оценка на средата	Излишност и проверка за съгласуваност
Зарядна инфраструктура	Компрометиране на EVSE, CSMS или идентичности	Прекъсване на услуга или достъп до данни	Сертификати, контрол на достъпа, мониторинг
Софтуерни актуализации	Подмяна или връщане към уязвима версия	Изпълнение на неоторизиран код	Цифров подпис, защита срещу rollback

5 Документирани експериментални атаки и уязвимости

Научната литература съдържа експериментални демонстрации, които доказват техническата възможност за компрометиране на определени автомобилни и зарядни системи при конкретни условия. Koscher и съавтори демонстрират атаки срещу вътрешна автомобилна мрежа при лабораторен достъп [9]. Checkoway и съавтори разширяват анализа към отдалечени повърхности за атака и показват значението на разделянето между външните интерфейси и критичните функции [6]. Petit и Shladover систематизират потенциални атаки срещу автоматизирани превозни средства и подчертават ролята на излишността и проверката на данните [7]. При зарядната инфраструктура атаката Brokenwire демонстрира безжично прекъсване на управляващата комуникация при CCS бързо зареждане и предизвиква прекратяване на зарядната сесия [10]. Тези резултати не следва да се представят като статистика за реални инциденти или като доказателство, че всички превозни средства са уязвими по един и същ начин.

Документираните изследвания показват, че сигурността е системно свойство, което зависи от архитектурата, реализацията и експлоатационните процеси. Отделна защитна функция не е достатъчна, когато липсват сегментиране, управление на идентичности и ключове, сигурни актуализации, регистриране на събития и процедура за реакция при инциденти. Принципът „сигурност още при проектирането“ трябва да се прилага към превозното средство, зарядното оборудване и системите за централно управление [4, 5, 17].

Таблица 2. Примери за публикувани изследователски демонстрации

Година	Изследване	Документиран резултат
2010	Koscher et al. [9]	Експериментални атаки срещу вътрешна автомобилна мрежа
2011	Checkoway et al. [6]	Анализ и демонстрация на отдалечени автомобилни повърхности за атака
2015	Petit и Shladover [7]	Систематизация на потенциални атаки срещу автоматизирани превозни средства
2023	Köhler et al. [10]	Безжично прекъсване на CCS зарядна комуникация (Brokenwire)

6 Предложен модел за защита според режима на работа

Предложеният модел разделя системата на домейни с различна критичност и определя разрешените действия според текущия режим. При движение функциите за управление, свързани с безопасността, не трябва да имат пряк маршрутизируем достъп до интернет или друга публична мрежа. Външната свързаност се прекратява на защитен телематичен шлюз, а към управляващия домейн се пропускат само предварително определени и проверени съобщения. Така се запазват необходимите свързани услуги, без да се създава пряк входящ път към управлението на спирането, ускорението и направлението [4], [6], [9].

Актуализиране на фърмуера на критичните електронни блокове се разрешава само когато превозното средство е неподвижно, трансмисията е в режим за паркиране, задвижването е деактивирано, зарядната сесия не е в активна силова фаза и е установено достатъчно енергийно ниво. Процедурата включва: (1) взаимно удостоверяване на участниците; (2) проверка на цифровия подпис и версията на пакета преди инсталиране; (3) изчисляване и сравняване на криптографски хеш след записването; (4) защитено стартиране и самопроверка; (5) автоматично връщане към последната валидна версия при неуспех. Обикновена контролна сума открива случайна повреда, но не доказва произхода на пакета; затова тя не може да замени цифровия подпис и защитеното управление на ключовете [19, 20].

Таблица 3. Правила на предложения модел според режима на работа

Режим	Мрежова политика	Разрешени действия	Независима защита
Движение	Без пряк достъп от публична мрежа до критичния управляващ домейн	Телеметрия и външни услуги през филтриран шлюз; актуализацията е забранена	Локални контролери и безопасно деградиране
Покой и обслужване	Удостоверена сервизна или OTA сесия	Инсталиране само на подписан пакет; хеш, версия, secure boot и rollback	Имобилизация и прекъсване при отпадане на условията
Зареждане	Разделяне на EVSE, CSMS, платежни услуги и силова електроника	Само удостоверени и ограничени команди за зарядна сесия	Защити по ток, напрежение, изолация и температура
Авария или несъответствие	Прекратяване на недостоверната комуникация	Отказ на актуализацията или контролирано прекратяване на зареждането	Отваряне на контакторите, ограничаване на мощността и регистриране на събитието

За зарядната инфраструктура същият принцип се прилага чрез разделяне на комуникационния, платежния и силовия домейн. Команда, получена от система за централно управление, не трябва непосредствено да отменя локалните ограничения за ток, напрежение, изолационно състояние и температура. При загуба на комуникация, невалидна идентичност, несъответствие между договорените и измерените параметри или превишена температура зарядната станция трябва да ограничи мощността или контролирано да прекрати сесията. Независимите хардуерни защити и контактори намаляват вероятността една кибератака да доведе до прегряване, повреда на батерията или пожар. Експлозия не следва да се посочва като пряка и неизбежна последица от мрежова атака, а като краен сценарий при едновременно компрометиране или отказ на няколко защитни слоя [2, 3, 21].

Моделът има концептуален характер. Неговата проверка изисква прототипна реализация и изпитвания с инжектиране на откази и невалидни команди, измерване на времето за откриване и реакция и доказване, че преходът към безопасно състояние не нарушава функционалната безопасност. За оценката на последствията върху движението са относими изследванията на безопасното разстояние между превозно средство и пешеходец [12], спирачното забавяне и ефективността на спирачните системи [13], както и вероятностната оценка на риска от сблъсък на пешеходна пътека [14].

7 Предизвикателства и бъдещо развитие на киберсигурността

Актуализациите по въздуха (over-the-air, OTA) позволяват отстраняване на уязвимости и добавяне на функционалности без физическо посещение в сервиз. Те създават и критична верига на доверие: пакетът трябва да бъде автентичен, целостта му да бъде проверена, инсталацията да е защитена срещу прекъсване и връщане към уязвима версия, а събитията да се регистрират. Компрометиран процес за актуализация може да разпространи неоторизиран софтуер до множество превозни средства. Затова управлението на актуализациите трябва да бъде част от системата за управление на киберсигурността и да се поддържа през целия жизнен цикъл [4], [5]. Методи за машинно обучение могат да подпомагат откриването на аномалии, но ефективността им зависи от качеството и представителността на данните, избраните показатели и устойчивостта срещу заобикаляне; те не заменят основните архитектурни мерки.

Нормативната рамка поставя изисквания към организационните процеси, а не само към отделни технически механизми. UN Regulation No. 155 изисква система за управление

на киберсигурността и доказване, че рисковете се управляват за съответния тип превозно средство [5]. ISO/SAE 21434 определя инженерни дейности за управление на киберриска през жизнения цикъл [4]. При зарядната инфраструктура сигурността трябва да обхваща комуникацията EV–EVSE, връзката между зарядната станция и системата за централно управление, обслужващите приложения и интеграцията с електроенергийната система. Двупосочният енергиен обмен увеличава взаимната зависимост между транспортната и енергийната инфраструктура и налага координирано управление на риска [2, 3, 21].

Бъдещото развитие следва да се насочи към проверима идентичност на устройствата, надеждно управление на сертификати и ключове, сегментирана архитектура, защитени диагностични и сервизни интерфейси, непрекъснато наблюдение и координирано разкриване на уязвимости [18]. За автоматизираните функции са необходими и механизми за откриване на недостоверни сензорни данни, излишност и безопасно деградиране. Оценката на ефективността трябва да се основава на измерими показатели и възпроизводими изпитвания, а не на недокументирани проценти за вероятност или пазарни прогнози.

8 Заключение

Свързаните, автоматизираните и електрическите превозни средства формират обща киберфизична екосистема с бордови мрежи, външни комуникационни интерфейси, зарядно оборудване, системи за централно управление и облачни услуги. ISO 15118, OCPP и IEC 63110 имат различен, взаимно допълващ се обхват в комуникационната архитектура за зареждане [2, 3, 21]. Публикуваните експериментални изследвания показват реалистични пътища за атака към автомобилни мрежи, сензорни системи и комуникацията при зареждане, но резултатите им са валидни при конкретно описани условия и не трябва да се превръщат в неподкрепени обобщения [6]–[10]. Основният принос на доклада е предложеният модел за режимно-зависима защита, който свързва мрежовата изолация при движение, удостоверената актуализация в покой и независимите електрически ограничения при зареждане.

Ефективната защита изисква управление на риска през целия жизнен цикъл, включително защитена архитектура, удостоверяване, криптографска защита, управление на ключове, сигурни софтуерни актуализации, сегментиране, мониторинг и реакция при инциденти. ISO/SAE 21434 и UN Regulation No. 155 поставят основата за систематичен организационен и инженерен подход [4], [5]. Следователно киберсигурността не е допълнителна функция, а условие за безопасната и надеждна експлоатация на съвременните превозни средства и зарядната инфраструктура. Моделът не се представя като експериментално доказано решение; следващ етап е неговата прототипна реализация и количествена оценка.

ЛИТЕРАТУРА:

[1] Denev D. R., Tsankov Ts. S. Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, Faculty of Technical Sciences, 2018, ISSN 1311-834X, pp. 94–101.

[2] Open Charge Alliance, Open Charge Point Protocol 2.0.1, Edition 3, 2024.

[3] IEC 63110-1:2022, Protocol for management of electric vehicles charging and discharging infrastructures – Part 1: Basic definitions, use cases and architectures, IEC, 2022.

[4] ISO/SAE 21434:2021, Road vehicles – Cybersecurity engineering, ISO/SAE, 2021.

[5] United Nations Economic Commission for Europe, UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, consolidated version, 2025.

[6] Checkoway S. et al., Comprehensive Experimental Analyses of Automotive Attack Surfaces, 20th USENIX Security Symposium, 2011.

[7] Petit J., Shladover S. E., Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems, Vol. 16, No. 2, 2015, pp. 546–556, DOI: 10.1109/TITS.2014.2342271.

[8] Thing V. L. L., Wu J., Autonomous Vehicle Security: A Taxonomy of Attacks and Defences, 2016 IEEE iThings/GreenCom/CPSCom/SmartData, 2016, pp. 164–170, DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[9] Koscher K. et al., Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447–462, DOI: 10.1109/SP.2010.34.

[10] Köhler S., Baker R., Strohmeier M., Martinovic I., Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging, Network and Distributed System Security Symposium, 2023, DOI: 10.14722/ndss.2023.23251.

[11] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144. ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[12] Petrov, Y., Staneva, L. Mathematical Modeling of Safe Vehicle–Pedestrian Distance with Interactive Visualization. Proceedings of the International Conference on Secure Systems Design and Technology Development, Vol. 2, 2026.

[13] Petrov, Y., Staneva, L. Analysis of Braking Deceleration and the Efficiency of Automotive Braking Systems Using MATLAB. Proceedings of the International Conference on Secure Systems Design and Technology Development, Vol. 2, 2026.

[14] Petrov, Y. Probabilistic Assessment of Vehicle–Pedestrian Collision Risk at a Crosswalk Using the Monte Carlo Method. Black Sea Journal of Engineering and Transport, Vol. 2, 2026, pp. 8–11. ISSN 3033-2885.

[15] Stoyanova, V. Problems with Information Security on Mobile Devices. Industry 4.0, 2019, p. 200. https://stumejournals.com/journals/i4/2019/4/200

[16] SAE International, SAE J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, 2021.

[17] ENISA, Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations, European Union Agency for Cybersecurity, 2016.

[18] NIST, The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, 2024, DOI: 10.6028/NIST.CSWP.29.

[19] United Nations Economic Commission for Europe, UN Regulation No. 156 – Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system, E/ECE/TRANS/505/Rev.3/Add.155, 2021.

[20] Uptane Standards Committee, Uptane Standard for Design and Implementation, Version 2.1.0, 2023.

[21] ISO 15118-20:2022, Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements, ISO, 2022.

MODEL OF A WEB-BASED STEGANOGRAPHIC SYSTEM*

ALEKS YA. DANEV, VALENTIN T. ATANASOV

ABSTRACT: *This paper presents a model of a Web-based steganographic system designed for hiding and extracting textual information in static digital images. The proposed model is based on the Least Significant Bit (LSB) method for data embedding and operates entirely within a Web browser using modern Web technologies. The system architecture includes modules for text processing, image loading, data embedding, information extraction, and result visualization. The proposed approach enables local image processing without transmitting image data outside the browser environment. The developed model demonstrates the practical applicability of Web technologies for the implementation of experimental steganographic systems.*

KEYWORDS: *web-based steganographic system, steganography, LSB method, digital image, information hiding, data extraction*

DOI: https://doi.org/10.46687/MT26AYV

МОДЕЛ НА WEB-БАЗИРАНА СТЕГАНОГРАФСКА СИСТЕМА

АЛЕКС Я. ДАНЕВ, ВАЛЕНТИН Т. АТАНАСОВ

АБСТРАКТ: *Настоящата публикация представя модел на Web-базирана стеганографска система, предназначена за скриване и извличане на текстова информация в статични цифрови изображения. Предложеният модел е базиран на метода Least Significant Bit (LSB) за вграждане на данни и функционира изцяло в средата на Web браузъра чрез използване на съвременни Web технологии. Архитектурата на системата включва модули за обработка на текст, зареждане на изображения, вграждане на данни, извличане на информация и визуализиране на резултатите. Предложеният подход позволява локална обработка на изображенията без предаване на графичните данни извън браузърната среда. Разработеният модел демонстрира практическата приложимост на Web технологиите за реализиране на експериментални стеганографски системи.*

1 Въведение

Развитието на цифровите комуникации и широкото използване на Web технологиите създават необходимост от ефективни средства за защита на информацията при нейния обмен и съхранение. Стеганографската защита на текстови документи е разгледана чрез разработване на алгоритъм и програма в [7]. По-широкият контекст на скритите интернет среди и киберсигурността е обсъден в [12]. Наред с криптографските методи, които осигуряват защита на съдържанието на съобщението, стеганографията предлага различен подход, насочен към прикриване на самия факт, че съществува скрита информация [1, 2, 5, 6, 13, 15]. По този начин двата подхода могат да бъдат използвани съвместно при изграждането на многослойни механизми за информационна сигурност [3]. Съвременните Web технологии предоставят възможност за разработване на приложения, които обработват цифрови изображения изцяло в средата на Web браузъра. Това ограничава необходимостта от предаване на обработваната информация извън браузърната среда и позволява реализиране на функционални прототипи, достъпни чрез стандартен Web браузър. Настоящата публикация представя модел на Web-базирана стеганографска система за

* Докладът е частично финансиран по проект РД-08-94/03.02.2026 г. „Експериментална и изследователска среда за моделиране, анализ и оптимизация на производствени процеси и технологии“

скриване и последващо извличане на текстова информация от статични цифрови изображения. Предложеният модел използва метода Least Significant Bit (LSB) за вграждане на текстова информация чрез модификация на най-малко значимите битове на пикселните компоненти [4, 11, 14, 17], като разглежда архитектурната структура на системата, основните функционални модули, последователността на процесите по обработка и взаимодействието между отделните компоненти.

2 Архитектурен модел на Web-базираната стеганографска система

Предложеният архитектурен модел описва концептуалната организация на функционалните компоненти, участващи в процесите по подготовка, вграждане, извличане и визуализиране на текстова информация в статични цифрови изображения. При проектирането е възприет модулен принцип, при който всеки функционален модул изпълнява ясно дефинирана задача в общия процес на стеганографска обработка. Подобен подход позволява разделяне на алгоритмичната логика от механизмите за визуализация и потребителското взаимодействие, което улеснява разработването, поддръжката и последващото разширяване на системата при необходимост от интегриране на нови алгоритми или допълнителни функционални възможности. В рамките на предложения модел статичното цифрово изображение изпълнява ролята на изображение носител, а текстовото съобщение представлява информацията, предназначена за вграждане. При изграждането на архитектурния модел са отчетени основни принципи на стеганографската обработка, свързани с ограничаване на визуалното въздействие върху изображението носител, контролиране на капацитета за вграждане и осигуряване на възможност за последващо коректно извличане на информацията [2].

При LSB метода измененията се извършват в най-малко значимите битове на избрани пикселни компоненти, което позволява модификациите да бъдат ограничени до нискоразрядните равнища на цифровото представяне на изображението [4]. Същевременно процесите по вграждане и извличане трябва да бъдат логически съгласувани, така че разположената в пикселната структура информация да може да бъде възстановена при последващата обработка на стегоизображението. Капацитетът определя количеството информация, което може да бъде разположено в достъпните пикселни компоненти, а степента на изменение характеризира въздействието на извършените модификации върху цифровото представяне на изображението [5, 8].

Съществено значение има запазването на модифицираните пикселни стойности, тъй като изменения, породени от загубна компресия, могат да нарушат последващото възстановяване на вградената информация [1, 5]. Архитектурният модел е реализиран чрез съвременни Web технологии, като всички операции по обработка на изображението се изпълняват локално в средата на Web браузъра. Използването на HTML5, JavaScript, FileReader API и HTML5 Canvas API осигурява локално зареждане, визуализиране и обработка на пикселната информация в цифровите изображения, както и непосредствен достъп до техните графични данни. При реализацията следва да се отчита и сигурността на JavaScript кода, чиито проблеми са разгледани в [16]. Това позволява реализиране на стеганографската обработка в средата на Web браузъра без използване на допълнителни програмни среди, специализиран софтуер или външна инфраструктура. По този начин обработката на изображенията и текстовата информация се извършва изцяло в рамките на Web-базираното приложение, без необходимост от предаването им извън браузърната среда. Функционалната организация на предложения модел включва последователно изпълнение на процесите по избор на изображение носител, подготовка на текстовото

съобщение, преобразуване на информацията в двоично представяне, реализиране на стеганографското вграждане чрез LSB метода, генериране на стегоизображение и последващо извличане на вграденото съдържание. Логическата последователност на тези процеси позволява ясно проследяване на взаимодействието между отделните функционални модули и създава предпоставки за коректно възстановяване на първоначалното текстово съобщение.

3 Алгоритмичен модел на процесите по вграждане и извличане на текстова информация

Алгоритмичният модел на LSB вграждането формализира последователността от операции, чрез които входното текстово съобщение се подготвя, преобразува в двоично представяне и се разполага в цифровата структура на избрано статично изображение. Структурирането на тези операции определя логическите зависимости и условията за преминаване между отделните етапи на стеганографската обработка.

В рамките на модела са синтезирани взаимно съгласувани алгоритмични последователности за вграждане и извличане, при които процесът по извличане реализира обратната обработка чрез прочитане на съответните позиции, формиране на двоична последователност и възстановяване на текстовото съдържание. В разглеждания модел принципът на LSB вграждането е приложен чрез контролирана модификация на най-малко значимите битове на избраните RGB компоненти. В научната литература LSB заместването се разглежда като подход, позволяващ постигането на висок капацитет за вграждане, като съществено значение има ограничаването на изменението на пикселните стойности при формирането на стегоизображението [4].

В предложения алгоритмичен модел тази зависимост се отчита чрез предварителна оценка на наличния капацитет и последващо контролирано използване на избраните пикселни компоненти. По този начин проверката на условията за допустимо вграждане се отделя логически от непосредствената модификация на данните, което позволява по-ясно формализиране на последователността между входната информация и формираното стегоизображение. Подобна организация на LSB вграждането позволява използването на нискоразрядните позиции на пикселните данни при ограничена промяна на цифровото представяне на изображението [6]. Тази характеристика допълнително обосновава необходимостта алгоритмичната последователност да отчита условията за формиране и последваща обработка на стегоизображението. Алгоритмичната организация може да бъде представена като предварително определена последователност с условни преходи, при която изпълнението на следващия етап зависи от резултата на предходните контролно-проверочни операции.

Разработената алгоритмична процедура включва проверка на входните данни, оценка на необходимия капацитет, подготовка на данните за вграждане, модификация на избраните RGB компоненти и формиране на стегоизображение като краен резултат от процеса. На фиг. 1 е представена диаграма, обобщаваща основните етапи на процеса по LSB вграждане на текстова информация в статично цифрово изображение, включително подготовката и проверката на входните данни, оценката на капацитета, модификацията на най-малко значимите битове на RGB компонентите и формирането на стегоизображение.

При положителна оценка на входните данни текстовото съобщение се преобразува в двоично представяне, след което се определя наличният капацитет на избраното изображение носител. Проверката на капацитета установява дали пикселната структура разполага с достатъчен брой позиции за вграждане на подготвената информация. При

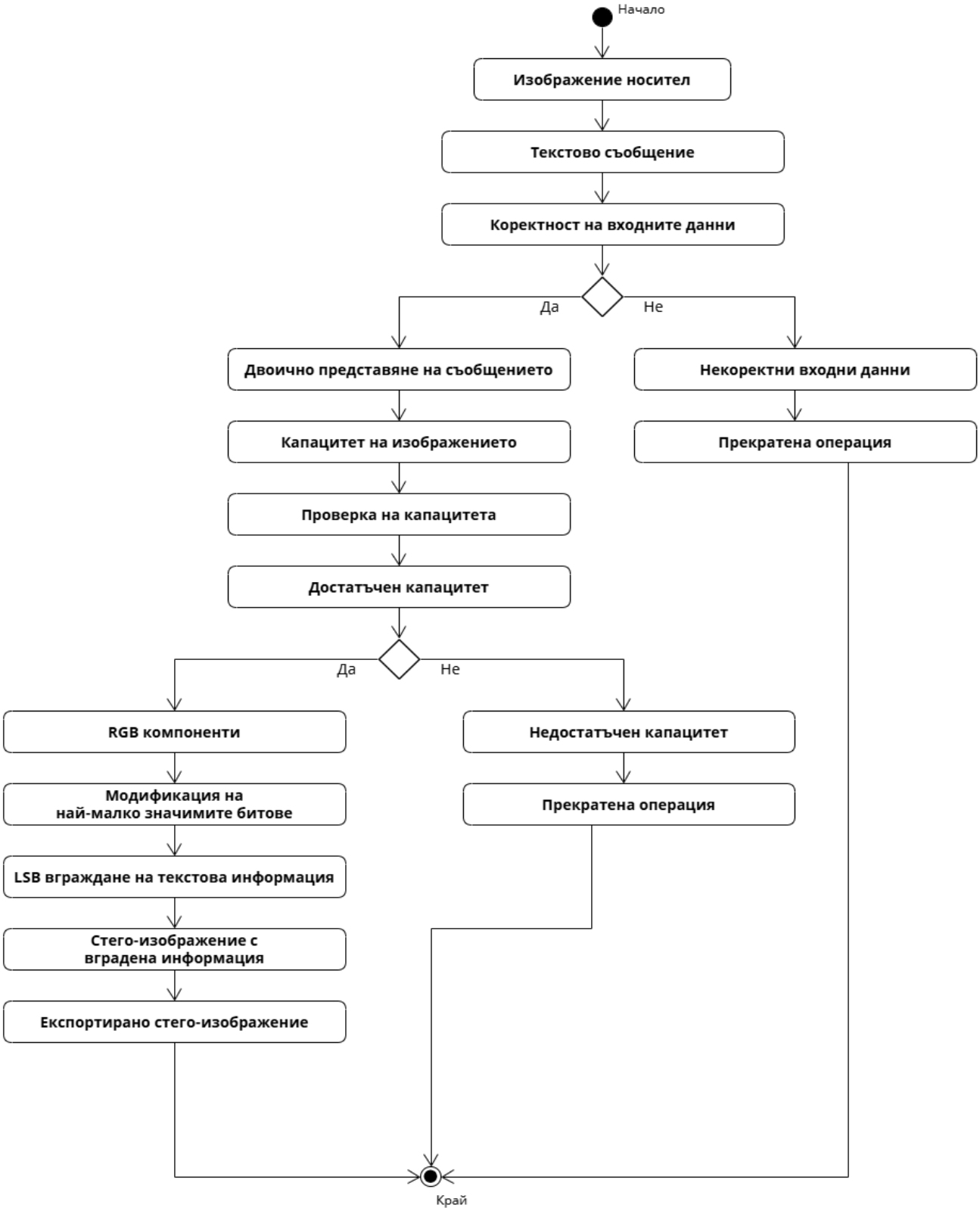
недостатъчен капацитет операцията се прекратява, докато при изпълнение на необходимото условие процесът продължава с достъп до RGB компонентите и модификация на техните най-малко значими битове.

Чрез LSB вграждането текстовата информация се разполага в избраните пикселни компоненти, в резултат на което се формира стегоизображение с вградено съдържание, което впоследствие може да бъде експортирано. Представеният алгоритмичен модел разглежда LSB вграждането като структуриран процес, включващ подготвителни, контролно-проверочни и изпълнителни етапи. Условните разклонения осигуряват разграничаване между допустимите и недопустимите условия за изпълнение, а последователността между двоичното представяне на съобщението, оценката на капацитета и модификацията на RGB компонентите позволява ясно проследяване на процеса по формиране на стегоизображението. По този начин диаграмата представя функционалната връзка между входните данни, наличния ресурс на изображението носител и крайния резултат от стеганографското вграждане. Структурирането на процеса в отделни етапи позволява ясно съпоставяне между алгоритмичните операции и съответните функционални модули на системата.

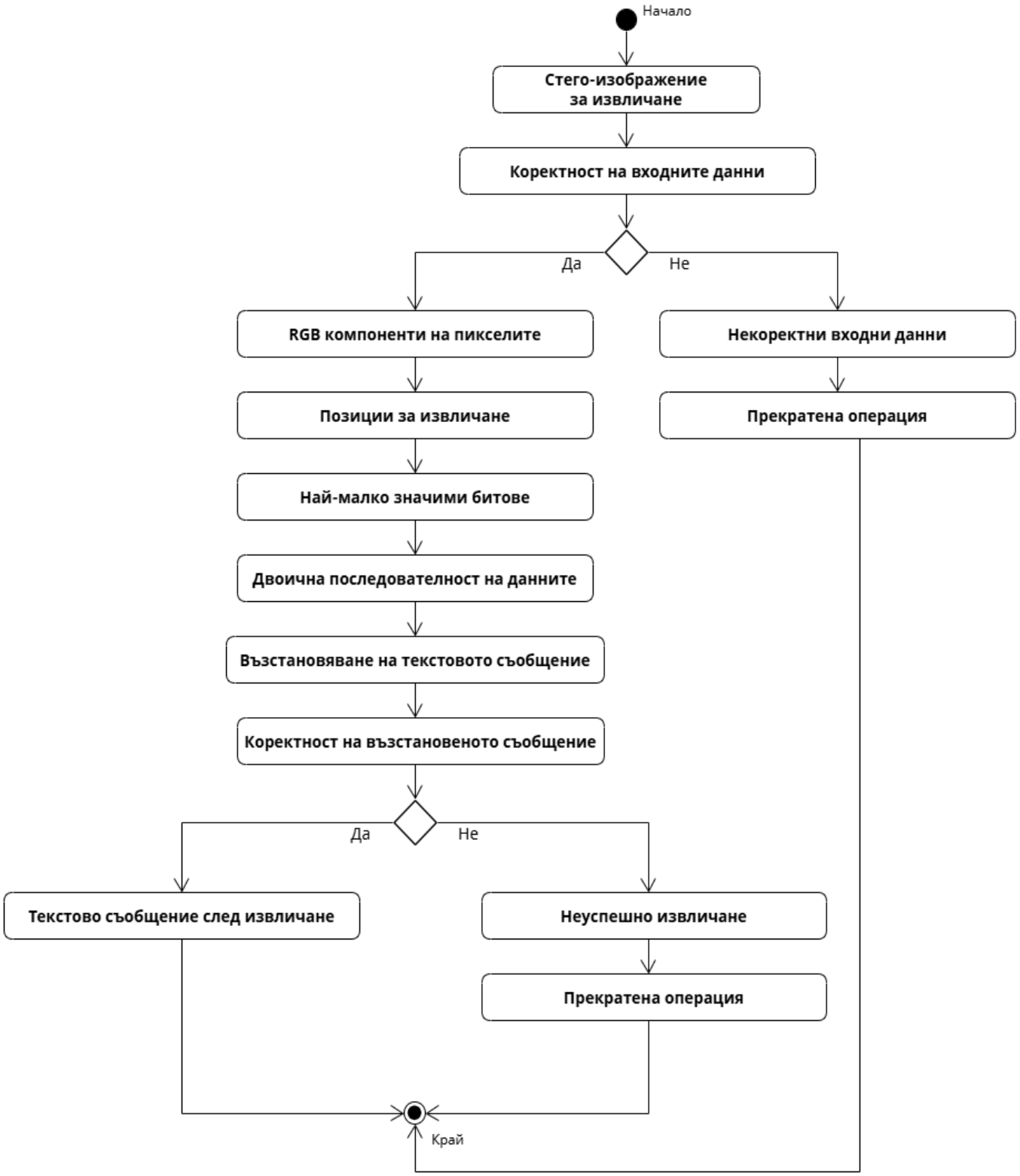
Блоково-базираното индексиране и LSB заместването са разгледани като подход за стеганографско вграждане в изображения [14]. Показателите за оценка на качеството при стеганографията с изображения са анализирани в [8]. Така дефинираната последователност формира детерминирана алгоритмична зависимост между валидирането на входните данни, оценката на наличния капацитет и последващата модификация на избраните пикселни компоненти, което позволява формално проследяване на условията за коректно формиране на стегоизображението. Формирането на стегоизображението завършва процеса по вграждане, след което функционалният модел може да бъде разгледан и в обратна посока чрез последователността за извличане и възстановяване на вградената текстова информация.

Процесът по извличане на текстова информация представлява обратна алгоритмична последователност спрямо процеса на вграждане, при която от пикселната структура на стегоизображението се възстановява предварително разположеното съдържание. В разглеждания модел извличането включва проверка на коректността на входните данни, определяне на съответните RGB компоненти и позиции за извличане, формиране на двоична последователност от най-малко значимите битове и възстановяване на текстовото съобщение. Допълнителната проверка на коректността на възстановеното съобщение позволява разграничаване между успешно и неуспешно извличане и определя крайния резултат от алгоритмичната последователност. На фиг. 2 е представена диаграма, обобщаваща основните етапи на процеса по извличане и проверка на възстановената текстова информация от стегоизображението.

Анализът на процеса по извличане показва, че възстановяването на текстовото съдържание е пряко свързано със съгласуваността между позициите, използвани при вграждането, и последователността за прочитане на най-малко значимите битове от RGB компонентите. Включването на проверки за коректност на входните данни и на възстановеното съобщение позволява разграничаване между успешните и неуспешните сценарии на обработка и контролирано приключване на съответния процес. Взаимното допълване на алгоритмичните последователности по вграждане и извличане формира завършен функционален цикъл, при който текстовата информация се преобразува, разполага в пикселната структура на изображението носител и впоследствие се възстановява от формираното стегоизображение.



Фиг. 1. Основни етапи на процеса по LSB вграждане на текстова информация в статично цифрово изображение



Фиг. 2. Основни етапи на процеса по извличане на текстова информация от стегоизображение

4 Функционални характеристики и ограничения на предложения модел

Предложеният модел се характеризира с модулна организация, локално изпълнение на операциите в средата на Web браузъра и логическа съгласуваност между процесите по вграждане и извличане на текстова информация. Коректното му функциониране е обвързано с наличния капацитет на изображението носител, правилното определяне на позициите за обработка и запазването на модифицираните пикселни стойности. Поради използването на LSB метода изменения на пикселната информация вследствие на загубна компресия или друга преобразуваща обработка могат да нарушат последващото възстановяване на вграденото съдържание. Това определя необходимостта от използване на формат за съхранение без загубна компресия и от контролиране на условията, при които се формира и обработва стегоизображението. Въпреки тези ограничения, модулната структура на модела създава предпоставки за последващо разширяване чрез включване на допълнителни алгоритмични подходи и механизми за проверка на коректността на обработваната информация. Сред разглежданите в научната литература направления за подобно развитие са оптимизираното LSB заместване с използване на генетичен алгоритъм [11] и блоково-базираните методи за индексиране и LSB заместване [14]. Други разглеждани направления са използването на повече най-малко значими битове [10] и стеганографията в сегменти на изображения с генетичен алгоритъм [18]. Характеристиките на стеганографски алгоритъм при използване на различни азбуки са предмет на изследване в [9].

5 Заключение

В настоящата публикация е разработен модел на Web-базирана стеганографска система за вграждане и последващо извличане на текстова информация от статични цифрови изображения. Предложеният модел структурира основните функционални компоненти и алгоритмични зависимости в последователна организация, която обединява подготовката на входните данни, оценката на капацитета на изображението носител, модификацията на най-малко значимите битове на избраните RGB компоненти, формирането на стегоизображение и последващото възстановяване на вграденото съдържание. Формализирането на процесите по вграждане и извличане като взаимно съгласувани алгоритмични последователности позволява ясно разграничаване на подготвителните, контролно-проверочните и изпълнителните етапи на стеганографската обработка и създава основа за проследяване на зависимостите между отделните функционални модули. Използването на HTML5, JavaScript, FileReader API и HTML5 Canvas API позволява обработката на изображенията и текстовата информация да бъде реализирана локално в средата на Web браузъра, като достъпът до пикселните данни осигурява необходимата основа за прилагане на LSB метода. Разработеният модел може да бъде разглеждан като концептуална и алгоритмична основа за последващо разширяване на Web-базираната стеганографска система чрез включване на допълнителни методи за скриване на информация, механизми за проверка на коректността на обработваната информация и експериментални процедури за оценяване на капацитета и степента на изменение на цифровото изображение. По този начин предложеният модел създава предпоставки за последващо изследване и усъвършенстване на стеганографската обработка в рамките на съвременни Web технологии.

ЛИТЕРАТУРА:

[1] Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding. IBM Systems Journal, Vol. 35, Nos. 3–4, 1996, pp. 313–336, DOI: 10.1147/sj.353.0313.

[2] Katzenbeisser S., Petitcolas F. A. P. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 1999, ISBN 978-1-58053-035-4.

[3] Цанков Ц. С. Приложения на нелинейните функции за защита на информацията в комуникационните системи. Университетско издателство „Епископ Константин Преславски“, Шумен, 2018, ISBN 978-619-201-212-0, 204 с.

[4] Chan C.-K., Cheng L. M. Hiding Data in Images by Simple LSB Substitution. Pattern Recognition, Vol. 37, No. 3, 2004, pp. 469–474, DOI: 10.1016/j.patcog.2003.08.007.

[5] Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. Digital Watermarking and Steganography. 2nd ed., Morgan Kaufmann, 2008, ISBN 978-0-12-372585-1, DOI: 10.1016/B978-0-12-372585-1.X5001-3.

[6] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009, ISBN 978-0-521-19019-0.

[7] Параскевов Х. И., Железов С. К., Цанков Ц. С., Станев С. С. Алгоритъм и програма за стеганографска защита на текстови документи. Международна научна конференция, посветена на 105-годишнината от рождението на Джон Атанасов и Джон фон Нойман, Шумен, 2008, ISBN 978-954-577-540-6.

[8] Стоянова, В., Кулев, Н. Анализ на показателите за качеството в стеганографията с изображения. Proceedings of the International Scientific Conference “Defense Technologies”, Shumen, 2017, с. 414–419. ISSN 2367-7902.

[9] Stoyanova, V. Research of the Characteristics of a Steganography Algorithm in Images When Using Different Alphabet. Proceedings of the 15th International Scientific and Practical Conference, Vol. IV, 2024, p. 259.

[10] Stoyanova, V. T. Steganography System Using More LSBs. ENTRENOVA – ENTerprise REsearch InNOVAtion, Vol. 4, No. 1, 2018, pp. 168–174.

[11] Wang R.-Z., Lin C.-F., Lin J.-C. Image Hiding by Optimal LSB Substitution and Genetic Algorithm. Pattern Recognition, Vol. 34, No. 3, 2001, pp. 671–683, DOI: 10.1016/S0031-3203(00)00015-7.

[12] Konstantinova E., Karadocheva M., Tsankov Ts. The Invisible Internet and Cyber Security. Proceedings of the International Scientific Conference 2019, “Vasil Levski” National Military University, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, 2019, ISSN 2367-7902, pp. 519–524.

[13] Johnson N. F., Jajodia S. Exploring Steganography: Seeing the Unseen. Computer, Vol. 31, No. 2, 1998, pp. 26–34, DOI: 10.1109/MC.1998.4655281.

[14] Patel A., Vekariya D. An Efficient Image Steganography Method Using Block-Based Indexing and LSB Substitution. Journal of Innovative Image Processing, Vol. 8, No. 2, 2026, pp. 536–557, DOI: 10.36548/jiip.2026.2.006.

[15] Диманова Д., Илиев Св. Стеганография – изкуството да скриваме информация. Годишник на Шуменския университет „Епископ Константин Преславски“, Том IV Е, 2014, с. 147–152, ISSN 1311-834X.

[16] Nikolov, L. G., Fetfov, O. M., Borisova, A. R. Security Concerns in JavaScript Coding. Proceedings of the Scientific Conference MATTEH 2018, Vol. 2, Part 2, Communication and Computer Technologies, Shumen, 2018, pp. 27–31, ISSN 1314-3921.

[17] Stoyanova, V. Steganography System that Uses the LSB Method of Embedding Information in Images. Proceedings of the International Scientific Conference “Defense Technology Forum 2015”, Shumen, 2015, pp. 186–193. ISSN 2367-7902.

[18] Stoyanova, V., Stoyanova, St. Steganography in Image Segments Using Genetic Algorithm. Proceedings of the International Scientific Conference “High Technologies. Business. Society”, Vol. I “High Technologies”, 2019, pp. 44–48. ISSN 2535-0005 (Print), ISSN 2535-0013 (Online).

INTELLIGENT SYSTEM FOR EARLY INCIDENT DETECTION THROUGH AI VIDEO ANALYSIS AND IoDT SENSORS*

SILVIA H. NIKOLOVA

ABSTRACT: *Early detection of critical events is a fundamental requirement for modern monitoring, control and protection systems in industrial facilities, critical infrastructure, warehouse complexes and public spaces. Conventional solutions typically use standalone video cameras or specialized physical sensors, which limits reliability under adverse conditions, partial failures and complex emergency scenarios. This paper presents an architecture and algorithmic model of an intelligent system for early detection of fires, unauthorized intrusion and industrial accidents through the combined analysis of video streams and data from IoDT (Internet of Digital Things) sensors. The proposed system integrates AI video cameras, thermal imaging devices, and temperature, smoke, gas, vibration, motion and access-control sensors. Data are processed through computer vision, time-series analysis and multisensor fusion algorithms. The solution uses dynamic reliability assessment of individual channels, probabilistic incident estimation and multilevel alarm confirmation. Simulation results show that the combined AI + IoDT approach achieves an average accuracy of 98.1%, compared with 91.8% for video-only analysis. The integrated model reaches an AUC of 0.988, demonstrating that heterogeneous sensor fusion improves detection reliability and enables automated response to critical events.*

KEYWORDS: *artificial intelligence, video analytics, IoDT, sensor fusion, early detection, fire, intrusion, industrial accident, Edge AI*

DOI: https://doi.org/10.46687/MT26SHK

ИНТЕЛИГЕНТНА СИСТЕМА ЗА РАННО ОТКРИВАНЕ НА ИНЦИДЕНТИ ЧРЕЗ AI АНАЛИЗ НА ВИДЕО И IoDT СЕНЗОРИ

СИЛВИЯ Х. НИКОЛОВА

АБСТРАКТ: *Ранното откриване на критични събития е основно изискване към съвременните системи за наблюдение, контрол и защита на индустриални обекти, критична инфраструктура, складови комплекси и обществени пространства. Традиционните решения обикновено използват самостоятелни видеокамери или специализирани физически сензори, което ограничава надеждността им при неблагоприятни условия, частични откази и сложни аварийни сценарии. Настоящият доклад представя архитектура и алгоритмичен модел на интелигентна система за ранно откриване на пожари, нерегламентирано проникване и индустриални аварии чрез комбиниран анализ на видеопотоци и данни от IoDT (Internet of Digital Things) сензори. Предложената система включва AI видеокамери, термовизионни устройства, температурни, димни, газови, вибрационни и сензори за движение и контрол на достъпа. Данните се обработват чрез алгоритми за компютърно зрение, анализ на времеви редове и мултисензорно обединяване (Sensor Fusion). Решението използва динамична оценка на надеждността на отделните канали, вероятностна оценка на инцидента и многостепенен механизъм за потвърждаване на алармите. Основната цел е намаляване на времето за откриване, повишаване на точността и ограничаване на фалшивите аларми. Симулационната оценка на разработения модел показва, че комбинираният подход AI + IoDT достига средна точност 98,1%, докато моделът, използващ само видеоанализ, достига 91,8%. Площта под ROC кривата на интегрирания модел е 0,988. Резултатите показват, че обединяването на хетерогенни сензорни източници повишава надеждността на детекцията и създава предпоставки за автоматизирана реакция при критични събития.*

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

1 Въведение

Развитието на изкуствения интелект, компютърното зрение, разпределените сензорни мрежи и Edge изчисленията създава предпоставки за преминаване от пасивно видеонаблюдение към интелигентни системи, които не само регистрират събития, но и извършват автоматична интерпретация на наблюдаваната среда. Особено важна е възможността за ранно разпознаване на опасни процеси, преди те да достигнат критична фаза.

Съвременните индустриални и инфраструктурни обекти се характеризират с висока степен на автоматизация, разпределени технологични процеси и значителен брой взаимосвързани устройства. Възникването на пожар, изтичане на опасни вещества, повреда на оборудване или нерегламентиран достъп може да доведе до човешки жертви, материални загуби, прекъсване на производствени процеси и отрицателно въздействие върху околната среда. Състоянието на критичната инфраструктура за район Шумен е анализирано в [1], а управлението на риска за обекти и съоръжения от критичната инфраструктура е разгледано в [29].

Ефективността на защитните системи зависи не само от способността им да разпознават вече настъпил инцидент, но и от възможността да откриват неговите ранни признаци. При пожар например началните индикатори могат да бъдат локално повишаване на температурата, наличие на дим, промяна в инфрачервения спектър или поява на характерни визуални структури. При индустриална авария ранните признаци могат да включват увеличени вибрации, необичайна температура, промяна в концентрацията на газове или отклонение в движението на механични компоненти.

Класическите системи за наблюдение често работят с един тип информация. Видеосистемите зависят от осветеността, атмосферните условия, положението на камерата и наличието на препятствия. Сензорните системи могат да регистрират физическа промяна, но често не осигуряват достатъчно информация за пространственото положение и причината за събитието. Това може да доведе до фалшиви аларми, пропуснати инциденти или забавена реакция.

Интегрирането на видеоанализ и IoDT сензори позволява формиране на по-пълна и устойчива оценка на наблюдаваната среда. В настоящото изследване IoDT се разглежда като разширена екосистема от интелигентни цифрови устройства, физически сензори, комуникационни модули и изчислителни възли, които обменят данни и участват в автоматизираното вземане на решения.

Основната цел е разработването на интелигентна архитектура за ранно откриване и класифициране на три основни категории инциденти: пожари и начални признаци на възпламеняване; нерегламентирано проникване; индустриални аварии и опасни технологични отклонения. Работната хипотеза е, че комбинирането на вероятностните оценки от видеоанализа и физическите сензори може да повиши точността на детекцията и да намали броя на фалшивите аларми.

2 Анализ на проблема и свързани изследвания

Съвременните методи за визуално откриване на пожар и дим използват конволюционни невронни мрежи, едноетапни детектори, трансформър архитектури и времеви модели [3, 4, 23]. При тях основно предимство е възможността за ранно визуално разпознаване на дим и пламък преди задействане на конвенционални точкови датчици.

Въпреки това точността остава зависима от контекста, осветлението и качеството на видеопотока.

При индустриалните приложения все по-широко се използват модели за анализ на многомерни времеви редове и графови невронни мрежи, които могат да моделират взаимозависимостите между температура, налягане, вибрации и други технологични параметри [5, 11–17]. Тези подходи са подходящи за откриване на ранни аномалии, тъй като оценяват не само абсолютните стойности, но и времевите и структурните зависимости между каналите.

В областта на системите за проникване и киберфизическата сигурност се използват хибридни модели, които съчетават CNN, LSTM, GRU и feature fusion [6–10]. Макар част от тези изследвания да са насочени към мрежови прониквания, принципът за обединяване на независими признаци е приложим и при физическа защита на периметър, където видео, движение и контрол на достъпа трябва да бъдат съпоставяни.

Съвременните разработки за ранно откриване на пожар все по-често комбинират интелигентни сензори, Edge обработка и IoT комуникация [19–22]. Тази тенденция показва, че надеждността на системата може да бъде увеличена, когато локалните AI алгоритми и сензорните данни се използват съвместно, а критичните решения не зависят изцяло от централен облачен ресурс.

2.1 Ограничения на системите, базирани само на видео

Алгоритмите за компютърно зрение могат да разпознават хора, превозни средства, дим, пламък, защитно оборудване и опасни действия. Тяхната ефективност обаче се влияе от редица фактори: недостатъчна или променлива осветеност; дим, мъгла и прах; частично закриване на обектите; отражения и сенки; ниска разделителна способност; вибрации на камерата; промени във фона; непознати обекти, които не са представени в обучаващата извадка. Откриването на обекти с военно предназначение в оптични изображения е разгледано в [34], а разпознаването на частично видими обекти и използването на трансфер на знания в MATLAB са теми на [2, 33].

2.2 Ограничения на системите, базирани само на сензори

Физическите сензори осигуряват надеждно измерване на температура, дим, газова концентрация, движение и вибрации, но обикновено предоставят локална информация. Един температурен сензор може да отчете повишение, без да е възможно автоматично да се установи дали причината е пожар, работещо оборудване или външен топлинен източник. Основните ограничения включват локален обхват на измерване; необходимост от подходящо разположение; дрейф на измервателните характеристики; прекъсване на комуникацията; повреда или замърсяване на сензора; невъзможност за визуална идентификация на причината.

2.3 Необходимост от мултисензорен подход

Мултисензорното обединяване позволява информацията от различни източници да се използва взаимно за потвърждаване или отхвърляне на предполагаемо събитие. Ако видеоалгоритъмът разпознае дим, а температурният и газовият сензор едновременно регистрират отклонение, вероятността за реален пожар е значително по-висока. При нерегламентирано проникване видеоразпознаването може да бъде комбинирано с инфрачервена бариера, сензор за движение и система за контрол на достъпа. При индустриална авария вибрационните и температурните данни могат да бъдат съпоставени с визуалното състояние на оборудването.

3 Архитектура на предложената система

Предложената архитектура е организирана в четири основни слоя: слой за събиране на данни; комуникационен слой; AI аналитичен слой; слой за управление, известяване и реакция. Между сензорния и аналитичния слой е предвидена Edge обработка, която намалява латентността и позволява локално функциониране при временна загуба на връзка с централния сървър.

3.1 Слой за събиране на данни

Първият слой включва всички устройства, които наблюдават физическата среда. Видеосистемата може да съдържа стационарни AI камери, PTZ камери, термовизионни и инфрачервени устройства, както и мобилни камери върху UAV или UGV платформи. Те осигуряват информация за форма, движение, позиция, поведение и визуални признаци на възникващи инциденти. Развитието и тенденциите при интелигентните камери за машинно зрение са разгледани в [18].

IoDT подсистемата използва температурни, димни, газови, вибрационни, акустични, инфрачервени, сензори за налягане и влажност, както и RFID устройства за контрол на достъпа. Всеки възел съдържа измервателен компонент, комуникационен модул, локална логика и уникален идентификатор. Като отделно направление при сензорните приложения е предложен модел на интерактивна система, базирана на ултрашироколентови сензори [24].

3.2 Комуникационен слой

Комуникационният слой осигурява обмен на данни между сензорите, камерите, Edge устройствата и централната платформа. В зависимост от приложението могат да се използват Ethernet, Wi-Fi, 4G/5G, LoRaWAN, MQTT и индустриални комуникационни протоколи. Видеопотоците се предават чрез подходящи протоколи за мултимедийни данни, а телеметрията от сензорите може да използва publish/subscribe механизъм.

За критични системи комуникационната инфраструктура трябва да осигурява автентикация, криптиране, контрол на достъпа, регистриране на събития, резервирани маршрути и синхронизация на времето. Времевата синхронизация е съществена, защото видео- и сензорните данни трябва да бъдат съпоставени за един и същ времеви интервал.

3.3 Edge обработка

Edge устройствата се разполагат близо до източниците на данни и изпълняват част от анализа локално. Това намалява латентността и комуникационното натоварване. На Edge ниво могат да се изпълняват филтриране на шум, компресиране, откриване на движение, базова AI класификация и локално съхраняване.

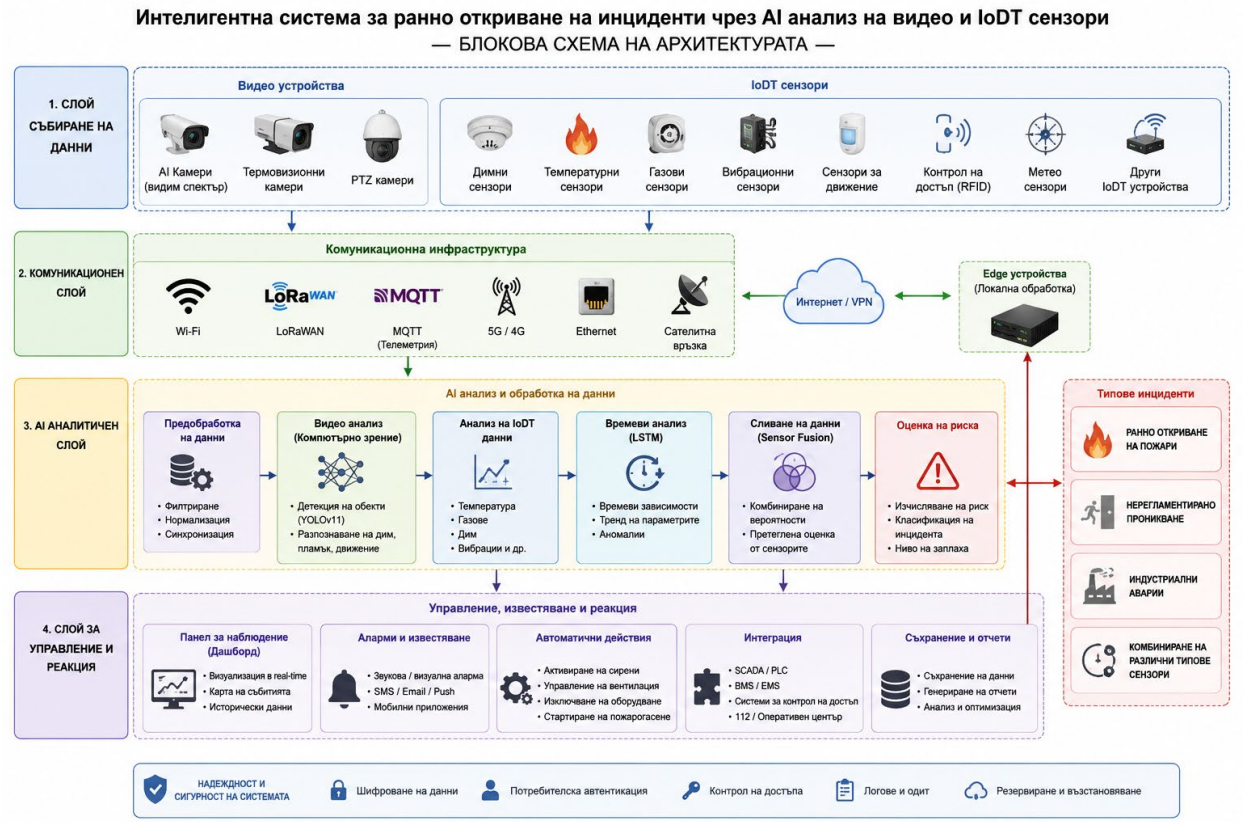
При критични приложения Edge обработката позволява системата да продължи да функционира дори при временно отпадане на интернет или облачната платформа. При достигане на предварително зададен критичен праг локалният възел може да генерира автономна аларма.

3.4 AI аналитичен слой

AI аналитичният слой обединява алгоритмите за видеообработка, анализ на IoDT данни, времеви анализ, Sensor Fusion и оценка на риска. Основните му функционални блокове са предварителна обработка, видео детекция, анализ на времеви редове, оценка на качеството на данните, динамично определяне на теглата, класификация на инцидента и оценка на риска.

3.5 Слой за управление и реакция

Последният слой включва операторски панел, визуализация на събитията, алармена система, мобилни известия, архивиране, автоматизирани защитни действия и интеграция със SCADA, PLC, BMS или други системи за управление. В зависимост от нивото на риск системата може да активира сирена, да управлява вентилацията, да изключи оборудване, да стартира пожарогасителна система или да блокира достъпа до опасна зона.



Фиг. 1. Блокова схема на архитектурата на интелигентната система за ранно откриване на инциденти

4 Предварителна обработка на данните

4.1 Предварителна обработка на видео

Видеопотоците преминават през последователност от операции: извличане на кадри, промяна на размерите, нормализация, корекция на яркостта и контраста, намаляване на шума, компенсиране на движението и отделяне на области на интерес. При термовизионните изображения се извършва температурна калибрация и определяне на области с необичайно висока температура.

4.2 Предварителна обработка на сензорни данни

За всеки сензор се извършват премахване на очевидно невалидни стойности, филтриране на импулсен шум, интерполация на липсващи стойности, нормализация, калибрационна корекция, изчисляване на плъзгаща средна и определяне на скоростта на изменение.

Нормализираната стойност на измервания параметър може да се изчисли чрез:

$$x_i^{norm} = (x_i - x_i^{min}) / (x_i^{max} - x_i^{min}) \quad (1)$$

където x_i е измерената стойност, а x_i^{min} и x_i^{max} са минималната и максималната допустима стойност за съответния параметър. За ранно откриване е важно не само абсолютното ниво на сигнала, но и неговата скорост на изменение:

$$\Delta x_i(t) = x_i(t) - x_i(t-1) \quad (2)$$

Бързото нарастване на температурата или концентрацията на газ може да бъде по-силен индикатор за опасност от единична висока стойност, поради което времевата производна се използва като допълнителен признак в аналитичния модел.

5 AI видеоанализ

5.1 Детекция и проследяване на обекти

За откриване на хора, превозни средства, машини и защитно оборудване може да се използва модел от семейството YOLO. За всеки открит обект се формират клас, координати на ограничителната рамка, вероятност на класификацията, времеви идентификатор, посока и скорост на движение. Наличието на човек в забранена зона се определя чрез пространствено пресичане между траекторията на обекта и предварително дефиниран полигон.

Проследяването във времето позволява разграничаване на краткотрайни шумови детекции от устойчиво присъствие и дава възможност за откриване на преминаване през виртуална линия, престой в защитена зона или движение в забранена посока.

5.2 Ранно откриване на пожар

Откриването на пожар включва анализ на цветови характеристики, форма, движение, текстура, промени между последователни кадри и термична информация. Визуалното разпознаване на дим и пламък е особено полезно в открити пространства, където класическите точкови датчици могат да реагират по-бавно.

За намаляване на фалшивите аларми визуалното разпознаване се комбинира с температура, дим и газови показатели. По този начин ярко отражение или заваръчна дейност не водят автоматично до критична аларма, ако липсва потвърждение от независими физически измервания.

5.3 Откриване на нерегламентирано проникване

Системата анализира преминаване през виртуална линия, престой в забранена зона, движение в необичайно време, нетипична траектория, движение в посока, противоположна на разрешената, и опит за манипулиране на оборудване. Видеоинформацията се съпоставя с RFID/идентификационни данни, инфрачервени бариери и сензори за движение.

Комбинирането на тези източници позволява разграничаване на разрешен служител от външно лице и намалява фалшивите аларми, причинени от животни, растителност или краткотрайни движения във фона.

5.4 Откриване на индустриални аварии

Видеоанализът може да идентифицира паднал човек, липса на защитна каска, разливане на течност, искрене, видима деформация, блокиране на производствена линия,

опасно приближаване до машина или необичайно движение на механичен компонент. Тези визуални признаци се използват съвместно със сензорни данни, тъй като част от най-ранните аварийни признаци не са видими в оптичния спектър.

6 Анализ на IoDT данни

Сензорните данни се обработват като многомерни времеви редове. За даден момент t входният вектор може да бъде дефиниран като:

$$x(t) = [T(t), S(t), G(t), V(t), M(t), H(t)] \quad (3)$$

където T(t) е температурата, S(t) е концентрацията на дим, G(t) е концентрацията на газ, V(t) е нивото на вибрации, M(t) е индикаторът за движение, а H(t) е влажността. За всеки параметър се определят нормално, предупредително и критично ниво.

Една възможна вероятностна оценка за отделен сензорен канал се получава чрез логистична функция:

$$P_i(t) = 1 / (1 + e\hat{}(-a_i(x_i(t) - \theta_i))) \quad (4)$$

където θ_i е прагът, а a_i определя чувствителността на прехода между нормално и опасно състояние. За откриване на времеви зависимости могат да се използват LSTM или GRU мрежи, които анализират последователност от измервания и могат да разпознават постепенно развиващи се отклонения.

7 Мултисензорно обединяване (Sensor Fusion)

7.1 Претеглено обединяване

За всеки източник се формира вероятност P_i за наличие на инцидент. Общата оценка се определя като претеглена комбинация:

$$P_incident = \Sigma_{i=1}^{n} w_i P_i \quad (5)$$

$$\Sigma_{i=1}^{n} w_i = 1 \quad (6)$$

Теглата отразяват базовата надеждност, точността и текущото качество на съответния сензорен канал. По-високо тегло се задава на източници, които са стабилни и релевантни за конкретния тип инцидент.

7.2 Динамично определяне на теглата

Статичните тегла не отчитат моментното състояние на устройствата. Поради това се предлага динамична корекция:

$$w_i(t) = r_i q_i(t) / \Sigma_{j=1}^{n} r_j q_j(t) \quad (7)$$

където r_i е базовата надеждност на i-тия източник, а $q_i(t)$ е показател за качеството на текущите данни. При замърсена камера или загуба на видеокадри теглото на оптичния

канал се намалява. При стабилна термовизионна информация и бързо повишаване на температурата относителното влияние на термичния канал се увеличава.

7.3 Правила за потвърждение на събития

Вероятностният модел се допълва с логически правила за потвърждение. За пожар могат да се използват комбинации от визуално открит пламък и висока температура; визуално открит дим и активен димен сензор; повишена температура, CO и термична аномалия. За проникване се използват човек в забранена зона и активиран сензор за движение; прекъсната инфрачервена бариера без валиден RFID достъп; движение в защитена зона извън разрешен интервал. За индустриална авария се комбинират високи вибрации и визуална деформация; повишена температура и необичайно движение на машина; газова концентрация над прага и визуални признаци за изтичане.

8 Оценка на риска и многостепенна реакция

Самата вероятност за инцидент не е достатъчна за определяне на приоритет. Необходимо е да се отчете и възможното въздействие. Оценката на риска се определя като:

$$R(t) = P_incident(t) \cdot C(t) \quad (8)$$

където C(t) е оценка на тежестта на последствията. Тя може да зависи от типа на обекта, наличието на хора, опасни вещества, критично оборудване и възможността за разпространение на инцидента. Анализът на причините и последствията като метод за управление на риска е разгледан в [26], а рискът от големи аварии с опасни вещества е обсъден в [28].

Ниво	Риск	Препоръчано действие
1	Много нисък	Архивиране и стандартно наблюдение
2	Нисък	Повишено наблюдение
3	Среден	Предупреждение към оператор
4	Висок	Автоматична аларма и локална реакция
5	Критичен	Незабавни защитни действия и уведомяване на аварийни екипи

9 Алгоритъм за функциониране на системата

Основният алгоритъм включва инициализация на камерите и IoDT устройствата, проверка на комуникационните канали, получаване на синхронизирани видеокадри и сензорни данни, предварителна обработка, AI анализ на видеото, анализ на сензорните времеви редове, оценка на качеството, динамично определяне на теглата, мултисензорно обединяване, класификация на инцидента, оценка на риска и задействане на подходяща реакция.

```
INPUT: video streams V, sensor streams S, thresholds Θ
INITIALIZE devices and AI models
WHILE system is active:
 acquire synchronized video and sensor data
 evaluate data quality
 preprocess video and sensor streams
 P_video ← video_AI_analysis()
 P_sensor ← temporal_sensor_analysis()
 weights ← calculate_dynamic_weights()
 P_incident ← sensor_fusion(P_video, P_sensor, weights)
 incident_class ← classify_incident(P_incident)
 risk ← P_incident × consequence
 IF risk ≥ critical threshold: activate emergency actions
 ELSE IF risk ≥ alarm threshold: notify operator
 ELSE IF risk ≥ warning threshold: increase monitoring
 store results
END WHILE
```

10 Експериментална постановка

За оценка на системата е дефиниран симулационен експериментален набор, съдържащ синхронизирани видеопоследователности и сензорни измервания. Изследвани са три основни категории: пожар, нерегламентирано проникване и индустриална авария. За всяка категория са моделирани както нормални, така и аварийни състояния.

10.1 Сценарии за пожар

Сценариите за пожар обхващат малък локален пламък; постепенно образуване на дим; прегряване без открит пламък; отражение, наподобяващо пламък; заваръчна дейност; дим от безопасен технологичен процес.

10.2 Сценарии за проникване

При проникване са моделирани следните ситуации: човек в забранена зона; преминаване през виртуална линия; движение на животно; разрешен служител с RFID идентификация; неразрешен достъп извън работно време; престой до защитено оборудване.

10.3 Сценарии за индустриални аварии

Сценариите за индустриални аварии включват повишени вибрации; прегряване на електродвигател; газово изтичане; разливане на течност; блокиране на механизъм; падане на работник; частична деформация на конструкция.

10.4 Сравнявани методи и метрики

Сравнени са три варианта: само AI видеоанализ, само IoDT сензори и комбиниран AI + IoDT модел. Оценката се извършва чрез Accuracy, Precision, Recall, F1-score, False Alarm Rate, Missed Detection Rate, ROC, AUC и матрица на объркване. Основните метрики се определят чрез:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (9)$$

$$Precision = TP / (TP + FP) \quad (10)$$

$$Recall = TP / (TP + FN) \quad (11)$$

$$F1 = 2 \cdot Precision \cdot Recall / (Precision + Recall) \quad (12)$$

11 Експериментални резултати

11.1 Обща точност

Метод	Точност
AI видеоанализ	91,8%
IoDT сензори	89,6%
AI + IoDT Sensor Fusion	98,1%

Комбинираният подход показва подобрение от 6,3 процентни пункта спрямо видеоанализа и 8,5 процентни пункта спрямо сензорния модел. Това потвърждава, че независимите информационни канали компенсират взаимно ограниченията си.

11.2 Резултати по вид инцидент

Вид инцидент	Само видео	AI + IoDT
Пожар	91,4%	98,1%
Проникване	93,2%	98,7%
Индустриална авария	88,6%	97,4%

Най-голямото подобрение се наблюдава при индустриалните аварии. Причината е, че ранни признаци като вибрации, газова концентрация и прегряване не могат да бъдат надеждно установени само чрез визуален анализ.

11.3 Матрица на объркване за видеоанализа

Реален клас	Предсказан инцидент	Предсказано нормално
Инцидент	458	42
Нормално състояние	39	461

При 1000 тестови наблюдения видеоаналитичният модел формира 458 истински положителни, 461 истински отрицателни, 39 фалшиво положителни и 42 фалшиво отрицателни решения. От тях се получават приблизително Accuracy = 91,9%, Precision = 92,2%, Recall = 91,6% и F1-score = 91,9%.

11.4 Матрица на объркване за AI + IoDT

Реален клас	Предсказан инцидент	Предсказано нормално
Инцидент	490	10
Нормално състояние	9	491

При интегрирания модел броят на пропуснатите инциденти е намален от 42 на 10, а фалшиво положителните решения – от 39 на 9. Получените показатели са Accuracy 98,1%, Precision 98,2%, Recall 98,0% и F1-score 98,1%.

11.5 ROC анализ

Метод	AUC
IoDT	0,913
AI видео	0,942
AI + IoDT	0,988

Стойността AUC = 0,988 показва много висока способност на комбинирания модел да разделя нормални и аварийни състояния. Разликата спрямо самостоятелните канали показва ефекта от мултисензорното потвърждение.

11.6 Фалшиви аларми и пропуснати детекции

Показател	Видео AI	AI + IoDT
False Alarm Rate	9,4%	6,2%
Missed Detection Rate	8,4%	2,0%

Относителното намаление на False Alarm Rate се оценява като:

$$\text{Reduction} = ((9{,}4 - 6{,}2) / 9{,}4) \cdot 100 \approx 34{,}0\% \quad (13)$$

Резултатът показва, че независимото потвърждение от няколко типа сензори ограничава неправилното активиране на алармите и едновременно с това намалява риска от пропускане на реално събитие.

12 Дискусия

Получените резултати показват, че мултисензорното обединяване има съществено значение за системите за ранно откриване. Видеоанализът предоставя пространствен контекст и идентифицира обекти и действия, докато IoDT сензорите измерват физическите характеристики на средата. Тези два типа информация са взаимно допълващи се.

При пожар термичните, димните и газовите сензори могат да потвърдят визуалното разпознаване на пламък. При неблагоприятна видимост термовизионните и температурните данни могат да компенсират намалената точност на оптичните камери. При проникване видеото позволява идентифициране и проследяване на обекта, а RFID системата и датчиците за движение дават допълнителна информация за разрешението и начина на достъп.

При индустриални аварии най-голямо значение имат времевите зависимости. Постепенното увеличаване на вибрациите или температурата може да бъде ранна индикация за неизправност, преди да се наблюдават видими повреди. Това обяснява по-голямото подобрение на комбинирания модел при този клас събития.

Основно предимство на системата е адаптивността. Динамичните тегла позволяват намаляване на влиянието на сензор, чиито данни са с ниско качество. Подходът повишава устойчивостта при частични откази, но изисква надеждна оценка на качеството на каналите и периодична калибрация.

Основните ограничения на представеното изследване са използването на симулационни данни, ограниченият брой класове инциденти, липсата на дългосрочна експлоатация в реален обект, необходимостта от обучение за конкретната среда и възможните комуникационни закъснения. Поради това числените стойности в раздел 11 следва да се разглеждат като резултати от моделна експериментална постановка, а не като универсални показатели за всички реални среди.

13 Надеждност и киберсигурност

Системата трябва да бъде проектирана така, че отказът на един компонент да не води до пълна загуба на наблюдение. Подходящи мерки са резервирани комуникационни връзки, Edge обработка, локално архивиране, самодиагностика, контрол на достоверността на сензорните данни, дублиране на критични сензори, периодична калибрация и автоматично превключване към резервен възел.

Киберсигурността включва криптиране на комуникацията, удостоверяване на устройствата, управление на сертификати, мрежова сегментация, регистриране и одит, защита срещу повторно изпращане на пакети, откриване на аномалии в трафика и контролирано актуализиране на софтуера. Особено важна е защитата срещу подмяна на сензорни данни, защото компрометиран IoDT възел може да предизвика фалшива аларма или да прикрие реален инцидент. Съвременните киберзаплахи са разгледани в [31], а сигурността на интелигентни структури в Интернет на нещата е анализирана в [32].

14 Практически приложения

Предложената система може да бъде използвана в производствени предприятия, складове за опасни вещества, енергийни обекти, транспортни терминали, пристанища, летища, логистични центрове, подземни съоръжения, минни и следминни територии, обществени сгради, интелигентни градове и други обекти от критичната инфраструктура. Архитектурата е мащабируема и позволява изграждане както на малки локални инсталации, така и на разпределени системи с множество камери и голям брой IoDT възли. При

планиране на последваща интеграция могат да се разгледат организацията на националната система за спешни повиквания [27] и геодезическите подходи и цифровите технологии за оценка и управление на риска от наводнения [30].

15 Заключение

В доклада е представена интелигентна система за ранно откриване на инциденти чрез интеграция на AI видеоанализ и IoDT сензори. Предложената архитектура комбинира пространствената и семантичната информация от видеото с физическите измервания на температура, дим, газове, вибрации и движение.

Основното предимство на подхода е възможността за взаимно потвърждаване на събитията от независими източници. Това повишава точността, намалява фалшивите аларми и съкращава времето за реакция. Симулационните резултати показват средна точност 98,1%, AUC 0,988 и значително намаляване на пропуснатите инциденти.

Бъдещата работа трябва да бъде насочена към изграждане на реален експериментален стенд, събиране на собствен набор от синхронизирани видео- и сензорни данни, оценка на латентността, проверка при частични откази и разработване на адаптивен модел за самообучение. Допълнително направление е интегрирането на FMEA [25], Fault Tree Analysis и Monte Carlo симулации за количествена оценка на надеждността и отказоустойчивостта на цялата система.

ЛИТЕРАТУРА:

[1] Диманова Д. В., Цанков Ц. С. Анализ състоянието на критичната инфраструктура за район Шумен. Годишник на Шуменския университет „Епископ К. Преславски“, Шумен, 2016, ISSN 1311-834X, с. 45–54.

[2] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[3] Essahraui S., Dini P., Saponara S. Early fire and smoke detection using deep learning: A comprehensive review of models, datasets, and challenges. Applied Sciences, Vol. 15, No. 18, 2025, Art. No. 10255, DOI: 10.3390/app151810255.

[4] Khan R. A., Alam U. I., Raza B. R. H., Anwar M. W. Beyond boundaries: Advancements in fire and smoke detection for indoor and outdoor surveillance feeds. Engineering Applications of Artificial Intelligence, Vol. 142, 2025, Art. No. 109855.

[5] Fan Y., Fu T., Listopad N. I., Liu P., Garg S., Hassan M. M. Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network. Alexandria Engineering Journal, Vol. 106, 2024, pp. 560–570, DOI: 10.1016/j.aej.2024.08.048.

[6] Ayantayo A., Kaur A., Kour A. et al. Network intrusion detection using feature fusion with deep learning. Journal of Big Data, Vol. 10, 2023, Art. No. 167, DOI: 10.1186/s40537-023-00834-0.

[7] Talukder M. A., Hasan K. F., Islam M. M. et al. A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, Vol. 72, 2023, Art. No. 103405.

[8] Henry A., Gautam S., Khanna S. et al. Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors, Vol. 23, No. 2, 2023, Art. No. 890, DOI: 10.3390/s23020890.

[9] Lilhore U. K., Manoharan P., Simaiya S. et al. Hybrid intrusion detection model for Industry 4.0 networks using an optimized CNN–LSTM with transfer learning. Sensors, Vol. 23, No. 18, 2023, Art. No. 7856, DOI: 10.3390/s23187856.

[10] Imrana Y., Xiang Y., Ali L., Abdul-Rauf Z. CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using a modified focal loss. Complex & Intelligent Systems, 2024, DOI: 10.1007/s40747-023-01313-y.

[11] Zhao M., Fink O. DyEdgeGAT: Dynamic edge via graph attention for early fault detection in IIoT systems. IEEE Internet of Things Journal, Vol. 11, No. 13, 2024, pp. 22950–22965, DOI: 10.1109/JIOT.2024.3381002.

[12] Zhao M., Peng H., Li L. Multivariate time-series anomaly detection based on dynamic graph neural networks and self-distillation in Industrial Internet of Things. IEEE Internet of Things Journal, 2024, DOI: 10.1109/JIOT.2024.3520362.

[13] Xie S., Li L., Zhu Y. Anomaly detection for multivariate time series in IoT using discrete wavelet decomposition and dual graph attention networks. Computers & Security, Vol. 146, 2024, Art. No. 104075, DOI: 10.1016/j.cose.2024.104075.

[14] Yang J., Yue Z. Learning hierarchical spatial–temporal graph representations for robust multivariate industrial anomaly detection. IEEE Transactions on Industrial Informatics, Vol. 19, No. 6, 2023, pp. 7624–7635, DOI: 10.1109/TII.2022.3216006.

[15] Zhang Z., Geng Z., Han Y. Graph structure change-based anomaly detection in multivariate time series of industrial processes. IEEE Transactions on Industrial Informatics, Vol. 20, No. 4, 2024, pp. 6457–6466.

[16] He S., Li G., Wang J., Xie K., Sharma P. K. Graph structure learning-based multivariate time-series anomaly detection in Internet of Things for human-centric consumer applications. IEEE Transactions on Consumer Electronics, Vol. 70, No. 3, 2024, pp. 5419–5431, DOI: 10.1109/TCE.2024.3409391.

[17] Wang J., Shao S., Bai Y., Deng J., Lin Y. Multiscale wavelet graph autoencoder for multivariate time-series anomaly detection. IEEE Transactions on Instrumentation and Measurement, Vol. 72, 2023, pp. 1–11, DOI: 10.1109/TIM.2022.3223142.

[18] 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.

[19] Ali M. et al. A comprehensive review of advanced sensor technologies for early fire detection and IoT integration. Chemosensors, Vol. 13, No. 7, 2025, Art. No. 230, DOI: 10.3390/chemosensors13070230.

[20] AlQahtani A. A. S. et al. A comprehensive review and bibliometric analysis of IoT-based fire detection systems. Safety, Vol. 11, No. 2, 2025, Art. No. 41, DOI: 10.3390/safety11020041.

[21] Sharobiddinov D. et al. Edge-based autonomous fire and smoke detection using deep learning and IoT devices. Sensors, Vol. 25, No. 20, 2025, Art. No. 6419, DOI: 10.3390/s25206419.

[22] Yang Y. et al. Design and research of an intelligent detection method for video fire recognition and multi-sensor data fusion based on edge computing. Applied Sciences, Vol. 15, No. 19, 2025, Art. No. 10589, DOI: 10.3390/app151910589.

[23] Hussain M. et al. A comprehensive review on deep-learning-based data-driven methods for fire and smoke detection. IEEE Access, Vol. 12, 2024.

[24] Atanasov, V., Trifonov, T. A new model of ultra wideband sensors based interactive system. International Journal on Information Technologies and Security, Vol. 16, No. 1, 2024, pp. 39–48, ISSN 1313-8251. https://doi.org/10.59035/XYCG3094

[25] Arabadzhieva-Kalcheva N., Tsankov Ts. Failure Modes and Effects Analysis – FMEA. Scientific Conference with International Participation MATTEH 2022, Conference Proceedings, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 58–62.

[26] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M. Cause-Consequence Analysis as a Risk Management Method. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, pp. 184–188. https://doi.org/10.46687/YT24NEL

[27] Диманова Д., Кузманов З. Национална система за спешни повиквания. Научна конференция MATTEX 2016, Шуменски университет „Епископ Константин Преславски“, 11–13 ноември 2016, с. 77–83, ISSN 1314-3921.

[28] Dimanova, D. Risk of major accidents with hazardous substances. SocioBrains, Issue 52, December 2018, pp. 49–53, ISSN 2367-5721.

[29] Dimanova, D. Risk management of critical infrastructure sites and facilities. SocioBrains, Issue 36, August 2017, pp. 67–73, ISSN 2367-5721.

[30] Stefanova, A. Flood risk assessment and management under directive 2007/60/EU: geodetic approaches and digital technologies for effective prevention. Environment. Technology. Resources, Proceedings of the 16th International Scientific and Practical Conference, Rezekne, Latvia, 19–20 June 2025, Vol. 4, pp. 393–397, ISSN 2256-070X. https://doi.org/10.17770/etr2025vol4.8402

[31] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144, ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[32] Стоянова, В. Интернет на нещата – анализ на сигурността при интелигентни структури. II International Scientific Conference CONFSEC, Borovets, 2018, Year 2, Issue 2 (4). ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[33] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения. DefTech 2025, 2025, с. 723–731. ISSN 2815-4282.

[34] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване на обекти с военно предназначение в оптични изображения. DefTech 2024, 2024, с. 675–682. ISSN 2815-4282.

MICROARCHITECTURAL SIDE CHANNELS AND DRAM DISTURBANCE IN MODERN COMPUTER SYSTEMS*

GALIN P. PEYCHEV, VELISLAV I. STOYANOV

ABSTRACT: *This analytical paper distinguishes cache timing channels, transient execution attacks and DRAM disturbance. The authors compare the prerequisites and observable effects of Flush+Reload, Prime+Probe, Spectre, Meltdown, microarchitectural data sampling and Rowhammer. A matrix relates each attack class to software, firmware and hardware mitigations and their remaining limitations. Performance effects are assessed qualitatively. The analysis shows why architectural permission checks alone cannot establish isolation when shared microarchitectural state or physical memory behavior remains observable.*

KEYWORDS: *processor security, side channels, cache timing, transient execution, Spectre, Meltdown, Rowhammer*

DOI: https://doi.org/10.46687/MT26GPI

МИКРОАРХИТЕКТУРНИ СТРАНИЧНИ КАНАЛИ И СМУЩЕНИЯ В DRAM ПАМЕТТА НА СЪВРЕМЕННИТЕ КОМПЮТЪРНИ СИСТЕМИ

ГАЛИН П. ПЕЙЧЕВ, ВЕЛИСЛАВ И. СТОЯНОВ

АБСТРАКТ: *Разграничават се времевите канали през кеша, атаките с преходно изпълнение и смущенията в DRAM. Авторите съпоставят предпоставките и наблюдаемите ефекти на Flush+Reload, Prime+Probe, Spectre, Meltdown, MDS и Rowhammer. Предложена е матрица на защитите на софтуерно, микрокодово и хардуерно ниво с техните ограничения. Влиянието върху производителността е оценено качествено. Анализът показва защо проверката на права за достъп не е достатъчна, когато споделено микроархитектурно състояние или физическо поведение на паметта остава наблюдаемо.*

1 Въведение

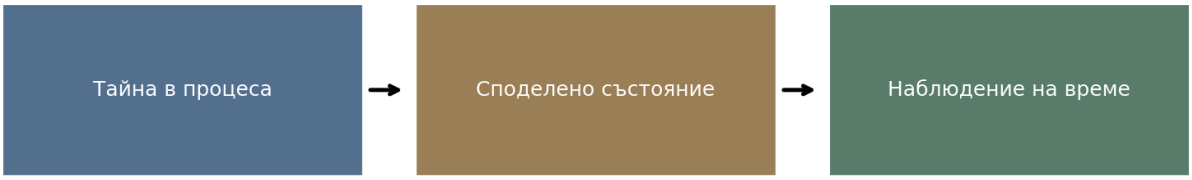
Архитектурата на набора от инструкции описва резултата, който програмата може да наблюдава чрез регистрите, паметта и изключенията. Реалният процесор пази и друго състояние: кешови линии, предсказватели на разклонения, буфери и таблици за преобразуване на адреси. Част от тези структури се споделят от процеси или нишки. Дори когато спекулативно изпълнена инструкция не промени крайния архитектурен резултат, следите от нея могат да повлияят на времето за последващ достъп [1, 2].

Целта е да се разграничат трите различни механизма, които често се смесват под общото име „хардуерни атаки“. Първият е наблюдение на споделен ресурс чрез време. Вторият е преходно изпълнение, което може да доведе чувствителни данни до такъв канал. Третият е физическо нарушаване на състоянието на DRAM. Авторският принос е сравнителната схема, матрицата на предпоставките и защитите и протоколът за оценка на остатъчния риск. Докладът е обзорно аналитично изследване, без нов експеримент върху конкретен процесор.

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

2 Канал за изтичане и преходно изпълнение

Страничният канал използва наблюдаема последица от изпълнението, например разлика във времето на достъп, вместо пряк прочит на защитения адрес. При атака с преходно изпълнение неправилно предсказана или впоследствие отказана операция може временно да обработи чувствителна стойност. След това нападателят измерва състоянието на друга структура, за да изведе информация за стойността. Тези две части имат различна роля: преходното изпълнение създава възможност за използване на данни, а измерването пренася информацията към наблюдателя [1, 2].



Фиг. 1. Обобщена последователност на микроархитектурно изтичане

Авторска схема по принципите в [1, 2]. Тя не е описание на конкретна експлоатация.

Flush+Reload измерва дали споделена кешова линия е била заредена между две наблюдения. Методът изисква подходяща споделена физическа страница, например при споделена библиотека, и възможност линията да се изхвърли или да се установи промяната в достъпа [3]. Prime+Probe работи чрез конкуренция за кешов набор и не изисква непременно споделен адрес, но зависи от съпоставянето към наборите и от шумовете в системата [4]. Нито един от тези методи сам по себе си не доказва пробив на привилегиите; те могат да бъдат каналът за наблюдение при различни уязвимости.

Spectre насочва процесора към преходно изпълнение по погрешно предсказан път. Вариант 1 използва заобикаляне на проверка на граница, а вариант 2 се отнася до отравяне на предсказването за непряк преход. Тези варианти използват различни пътища на предсказване и изискват различни мерки за защита [1]. Meltdown, наричан още Rogue Data Cache Load, използва преходно обработена стойност от достъп, който впоследствие поражда изключение на засегнати процесори. Точният момент и начин на проверката на разрешенията зависи от микроархитектурата; уязвимостта не следва от общо правило, че всяка проверка се извършва едва при приключване на инструкцията [2].

При Microarchitectural Data Sampling, включително ZombieLoad, потенциалният източник са остатъчни стойности във вътрешни буфери. Условията на експлоатация и обхватът се различават от тези на Spectre и Meltdown. На засегнати платформи микрокодови механизми за изчистване на буфери, промени в операционната система и политика за едновременна многонишковост участват в ограничаването на риска [5, 6].

3 Физическото смущение в DRAM

Rowhammer представлява многократно активиране на редове в DRAM, което може да предизвика обръщане на битове в съседни редове. Първоначалното експериментално изследване свързва явлението с електрически смущения и загуба на заряд в гъсто

разположените клетки [7]. Това е нарушаване на целостта на данни, а не просто времеви канал. Не всяка памет и конфигурация е еднакво уязвима; необходима е проверка на конкретния модул, контролер и режим на обновяване.

Целевото обновяване на редове (TRR) е една от защитите, но изследването TRRespass демонстрира шаблони на достъп, които могат да заобиколят определени реализации [8]. ECC може да открива или коригира конкретни класове грешки според кода и конфигурацията, но не е универсална гаранция срещу всички многобитови смущения. Затова коректната оценка включва режима на паметта, типа грешки, наличието на ECC и тестове за устойчивост, а не само отметка, че TRR или ECC е включен.

Таблица 1. Механизъм, предпоставка и основна граница на защитата

Клас	Необходима предпоставка	Защита и ограничение
Flush+Reload	Споделена линия и измерим достъп	Ограничаване на споделянето и код с постоянен времеви профил; остават други канали
Prime+Probe	Конкуренция за кешов набор	Изолация или партициониране на ресурса; ефектът зависи от реализацията
Spectre	Управляемо предсказване и подходящ код	Мерки според варианта, например бариери или защита на непреки преходи
Meltdown	Засегнат процесор и подходящо картографиране	KPTI или хардуерна защита; не решава автоматично Spectre
MDS	Засегнати вътрешни буфери	Микрокодово изчистване и мерки при SMT според платформата
Rowhammer	Уязвима DRAM и интензивни активации	Обновяване, ограничения на достъпа и ECC; няма универсална гаранция

Съпоставка на авторите по [1–8]. Резултатите зависят от версията на процесора, паметта и софтуера.

4 Оценка на мерките и тяхната цена

KPTI отделя потребителското от привилегированото адресно пространство на ядрото на засегнати системи и ограничава класическия Meltdown. KASLR има друга цел: затруднява предсказването на адресното разположение и не замества KPTI. Retpoline е компилаторна техника за ограничаване на определени атаки чрез отравяне на непреки преходи, но не е обща защита срещу Spectre вариант 1 или всички по-късни варианти. LFENCE може да ограничи спекулацията на избрани места, когато е поставена съгласно указанията за конкретната архитектура [2, 9, 10].

Числената оценка на забавянето изисква конкретна тестова система, натоварване и измервателен протокол. Разходът зависи от честотата на системни повиквания и превключвания на контекст, процесорния модел, активния микрокод и начина на компилиране. Дори за една и съща защита измерване на пакетна обработка и на

изчислителна задача може да даде различен резултат. Затова таблица 2 показва къде възниква разходът, без числени оценки, които не са измерени за конкретна конфигурация.

Таблица 2. Защити и условни разходи за производителността

Мярка	Основна цел	Къде възниква разход
KPTI	Meltdown на засегнати процесори	Превключване между режимите и работа с адресните таблици
Retpoline или IBRS	Някои форми на Spectre V2	Непреки преходи и управление на предсказателя
LFENCE на избрани места	Определени пътища на спекулация	Сериализиране в защитения участък
Изчистване на буфери	MDS на засегнати платформи	Преходи между контексти и режими
TRR и ECC	Грешки в DRAM	Допълнително обновяване, памет и проверки според реализацията

Качествена оценка на авторите по [6, 8–10]. Нужни са измервания за числена стойност.

Хардуерните идеи за задържане на спекулативни ефекти в отделно състояние са предмет на изследвания, например InvisiSpec [11]. Това е изследователски подход и приложимостта му зависи от конкретната реализация на процесора. Intel документира хардуерни защити за определени класове уязвимости и подчертава нуждата от анализ на конкретната платформа [6, 12]. Кешовото партициониране може да намали конкуренцията за ресурс, но ефективността срещу Prime+Probe трябва да се проверява за конкретната реализация.

5 Граници на изолацията и авторски подход

Цанков разглежда VLAN като логическо разделяне на една физическа локална мрежа с цел управление и защита [13, с. 105]. Това е пример за изолация на мрежово ниво, която не обхваща споделеното състояние вътре в процесора. Виртуална машина, контейнер или отделна мрежа могат да ограничават достъпа според своя модел, докато кешове и буфери на същия физически хост остават предмет на отделен анализ. Разграничаването на тези нива е важно при формулиране на модела на заплахите.

Авторите предлагат оценката да започва с конкретен противник и споделен ресурс. След това се проверяват процесорната и DRAM архитектура, версията на микрокода, операционната система и активните мерки. Третата стъпка е измерване на две отделни величини: дали каналът е наблюдаем и как защитата влияе върху реална задача. Така не се смесват липса на известен експлойт, липса на измерен канал и доказана липса на изтичане. Рамката е предложение за бъдеща проверка, а не резултат от проведен експеримент.

За повторяемо изследване биха били нужни описани процесор и ревизия, конфигурация на кеша и SMT, модел DRAM и ECC, версия на операционната система, микрокод и компилатор, както и статистика от многократни измервания. Резултатите следва да отделят честотата на грешните класификации в канала от забавянето на

защитеното приложение. Без тези данни твърденията за „пълна защита“ или „минимална цена“ са незащитими.

6 Заключение

Кешовите времеви канали, преходното изпълнение и Rowhammer имат различни причинни механизми и изискват различни защити. KPTI, Retpoline, бариерите, микрокодовото изчистване и защитите на DRAM трябва да се прилагат според конкретната уязвимост и платформа. Представената авторска матрица свързва предпоставките на атаката с границите на противодействието. Следваща задача е тя да се провери експериментално с повторяеми измервания на изтичането и производителността, като резултатите се отнасят към точно описаната конфигурация.

ЛИТЕРАТУРА:

[1] Kocher P. et al. Spectre Attacks: Exploiting Speculative Execution. IEEE Symposium on Security and Privacy, 2019, pp. 1–19. https://doi.org/10.1109/SP.2019.00002

[2] Lipp M. et al. Meltdown: Reading Kernel Memory from User Space. USENIX Security, 2018, pp. 973–990. https://www.usenix.org/conference/usenixsecurity18/presentation/lipp

[3] Yarom Y., Falkner K. FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. USENIX Security, 2014, pp. 719–732. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/yarom

[4] Osvik D. A., Shamir A., Tromer E. Cache Attacks and Countermeasures: the Case of AES. CT-RSA, 2006, pp. 1–20. https://doi.org/10.1007/11605805_1

[5] Schwarz M. et al. ZombieLoad: Cross-Privilege-Boundary Data Sampling. ACM CCS, 2019, pp. 753–768. https://doi.org/10.1145/3319535.3354252

[6] Intel. Microarchitectural Data Sampling, software security guidance. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/advisory-guidance/microarchitectural-data-sampling.html

[7] Kim Y. et al. Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors. ISCA, 2014, pp. 361–372. https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf

[8] Frigo P. et al. TRRespass: Exploiting the Many Sides of Target Row Refresh. IEEE Symposium on Security and Privacy, 2020. https://ieeexplore.ieee.org/document/9152631/

[9] Gruss D. et al. Kernel Isolation: From an Academic Idea to an Efficient Patch for Every Computer. USENIX ;login:, 2018. https://www.usenix.org/publications/login/winter2018/gruss

[10] Intel. Retpoline: A Branch Target Injection Mitigation. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/retpoline-branch-target-injection-mitigation.html

[11] Yan M. et al. InvisiSpec: Making Speculative Execution Invisible in the Cache Hierarchy. MICRO, 2018. https://ieeexplore.ieee.org/document/8574559/

[12] Intel. Configuring Workloads for Microarchitectural and Side Channel Security. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/best-practices/securing-workloads-against-side-channel-methods.html

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

СЪДЪРЖАНИЕ

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ: МИНАЛО, НАСТОЯЩЕ И БЪДЕЩЕ, проф. Иван Цонев, Кремен Христов 3

КЛЪСТЕРИЗАЦИЯ ПРИ АВТОНОМНИ АГЕНТИ С LLM, ВЪЗДЕЙСТВАЩИ ВЪРХУ ОБЩ ПРОЦЕС ИЛИ ПАЗАР, Николай Р. Николов, Цветослав С. Цанков 12

МОДЕЛ НА УЕБ БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА „ДИПЛОМАНТ“, Павел С. Тодоров, Валентин Т. Атанасов 24

ОБЯСНИМ ИЗКУСТВЕН ИНТЕЛЕКТ (EXPLAINABLE AI) ВЪВ ВИДЕОНАБЛЮДЕНИЕТО ЗА КРИТИЧНА ИНФРАСТРУКТУРА, Силвия Х. Николова, Симона С. Христова 30

ИЗСЛЕДВАНЕ МОДЕЛ НА ЕЛЕКТРОНЕН ПРЕОБРАЗУВАТЕЛ В SIMULINK, Васил Б. Иванов 37

ИЗСЛЕДВАНЕ НА МОДЕЛ НА ВЯТЪРНА ЕЛЕКТРОЦЕНТРАЛА СЪС СТАТИЧЕН СИНХРОНЕН КОМПЕНСАТОР STATCOM ОТ БИБЛИОТЕКАТА НА „SIMULINK“, Васил Б. Иванов 48

ВЛИЯНИЕ НА НОВИТЕ МРЕЖОВИ ТЕХНОЛОГИИ ВЪРХУ КАЧЕСТВОТО НА КОМУНИКАЦИОННИТЕ УСЛУГИ, Алекс Я. Данев, Илкер А. Хатиб 61

РОЛЯТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В СЪВРЕМЕННАТА ИНДУСТРИАЛНА АВТОМАТИЗАЦИЯ, Даниел Р. Денев 70

ИЗСЛЕДВАНЕ НА МЕХАНИЗМИТЕ ЗА УДОСТОВЕРЯВАНЕ В СЪВРЕМЕННИТЕ КОМУНИКАЦИОННИ СИСТЕМИ, Екатерина М. Христова, Стефания М. Червенкова 79

МОДЕЛ НА УЕБ-БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА „ДОКТОРАНТ“, Йовко М. Христов, Валентин Т. Атанасов 88

PLC И HMI РЕАЛИЗАЦИЯ НА АВТОМАТИЗИРАНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНДУСТРИАЛНА ПАКЕТИРАЩА ЛИНИЯ, Здравко А. Здравков 95

ИНТЕГРАЦИЯ НА ТЕХНОЛОГИИ С ИЗКУСТВЕН ИНТЕЛЕКТ В СЪВРЕМЕННИТЕ КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ, Габриела С. Маркова, Даниел Р. Денев 103

ПОТОЧНИ ИНФОРМАЦИОННИ ДАННИ И ПРИЛОЖЕНИЕТО ИМ В SMART GRID СИСТЕМИ, Милен С. Давидков, Лилия А. Станева 114

СРАВНИТЕЛЕН АНАЛИЗ НА МЕТОДИТЕ ЗА МАШИННО ОБУЧЕНИЕ, Стефан М. Казаков 125

КИБЕРСИГУРНОСТ НА ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА ВИДЕОНАБЛЮДЕНИЕ С ИЗКУСТВЕН ИНТЕЛЕКТ, Силвия Х. Николова 136

СЪДЪРЖАНИЕ

РАЗПРЕДЕЛЕНА ПАРАЛЕЛНА РЕАЛИЗАЦИЯ НА МНОГОКРИТЕРИАЛЕН МОДЕЛ ЗА ОЦЕНЯВАНЕ КАЧЕСТВОТО НА ПОТОЧНИ ДАННИ, Костадин Д. Костадинов, Милен С. Давидков 147

АДАПТИВЕН МЕХАНИЗЪМ ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО НА ПОТОЧНИ ДАННИ ПРИ КОНЦЕПТУАЛЕН ДРЕЙФ, Милен С. Давидков, Екатерина М. Христова 157

ПРОИЗВОДСТВОТО НА HBM И ВЛИЯНИЕТО МУ ВЪРХУ ПРЕДЛАГАНЕТО НА DDR5 ПАМЕТ ЗА AI ИНФРАСТРУКТУРА, Галин П. Пейчев, Велислав И. Стоянов . 164

РАЗВИТИЕ НА КОРПУСИРАНЕТО ОТ МОНОЛИТНИ КРИСТАЛИ КЪМ ЧИПЛЕТИ И 3D КЕШ, Галин П. Пейчев, Велислав И. Стоянов 169

ПРОЕКТИРАНЕ И РЕАЛИЗАЦИЯ НА ХИБРИДНА ЛАБОРАТОРНА СРЕДА ЗА ПАСИВЕН АНАЛИЗ НА МРЕЖОВ ТРАФИК, Денис И. Звезделинов, Здравко Ю. Кузманов 175

СТРАТЕГИИ ЗА ЗАЩИТА И ПРЕВЕНЦИЯ СРЕЩУ АТАКИ В СЪВРЕМЕННИ КОМУТИРУЕМИ МРЕЖИ, Денис И. Звезделинов, Здравко Ю. Кузманов..... 182

СРАВНИТЕЛЕН АНАЛИЗ НА HACKRF ONE И YARD STICK ONE ПРИ ИЗСЛЕДВАНЕ НА СУБГИГАХЕРЦОВИ БЕЗЖИЧНИ КОМУНИКАЦИИ, Димитър Н. Грешков, Здравко Ю. Кузманов 191

КОНЦЕПТУАЛЕН МОДЕЛ НА НИВАТА НА АВТОНОМНОСТ НА АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ОБРАЗОВАТЕЛНИ ПРОЦЕСИ, Десислава Н. Иванова 204

АНАЛИЗ НА ПРИНЦИПИТЕ НА РАБОТА И ЕФЕКТИВНОСТТА НА ТРАНСПОРТНИТЕ ПРОТОКОЛИ TCP И UDP, Десислав М. Христов..... 215

ПРИЛОЖЕНИЕ НА ПОЛИНОМИТЕ НА ЧЕБИШЕВ ВЪВ ФОТОВОЛТАИЧНИТЕ СИСТЕМИ, Илияна С. Иванова, Тихомир С. Трифонов 228

АРХИТЕКТУРА И МЕТОДИКА ЗА ОЦЕНКА НА НАДЕЖДНОСТТА НА РЕЗЕРВИРАНИ ИНДУСТРИАЛНИ ETHERNET МРЕЖИ, Драган С. Тончев, Цветослав С. Цанков 237

АВТОМАТИЗИРАНО ПОЗИЦИОНИРАНЕ И КЛИМАТИЧНА ЗАЩИТА НА ФОТОВОЛТАИЧЕН ПАНЕЛ СЪС SIEMENS LOGO, Сунай Х. Салим, Цветослав С. Цанков..... 247

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ НА ВРЕМЕТО ЗА РЕАКЦИЯ И ПРОИЗВОДИТЕЛНОСТТА НА WEB БАЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ПРИ ЕДНОВРЕМЕННИ ЗАЯВКИ, Йовко М. Христов, Десислав М. Христов..... 253

СРАВНИТЕЛНО ПРОЕКТИРАНЕ НА АВТОМАТИЗИРАНА ЛИНИЯ ЗА РЕЦИКЛИРАНЕ НА АЛУМИНИЕВИ КЕНОВЕ, Диян В. Марков, Цветослав С. Цанков 261

СЪДЪРЖАНИЕ

АРХИТЕКТУРЕН МОДЕЛ НА ПРОТОТИП, ИЗПОЛЗВАЩ МОДЕЛ НА КОДИРАНЕ С ПОЗИЦИОННО РЕДУВАНЕ И ПРОМЕНЛИВА ДЪЛЖИНА НА МЕТА КОДА, Валентин Т. Атанасов 269

СЕГМЕНТИРАНЕ И ИНТЕГРАЦИЯ НА IP СИСТЕМИ В МРЕЖА НА ПРОИЗВОДСТВЕН ОБЕКТ, Айкут А. Ремзиев, Цветослав С. Цанков 274

СРАВНИТЕЛЕН АНАЛИЗ МЕЖДУ Wi-Fi 7 И СИСТЕМИТЕ ОТ ПО-СТАРО ПОКОЛЕНИЕ, Николет Г. Люледжиева, Петко М. Налбантов 280

ПРИЛОЖЕНИЕ НА EDGE AI (ИЗКУСТВЕН ИНТЕЛЕКТ В КРАЙНИ/ПЕРИФЕРНИ УСТРОЙСТВА) В СЪВРЕМЕННИТЕ КОМПЮТЪРНИ СИСТЕМИ, Петко М. Налбантов, Николет Г. Люледжиева, Георги П. Илиев 288

СТЕГАНОГРАФСКО КОДИРАНЕ В ТРИИЗМЕРНИ ПОЛИГОНАЛНИ МРЕЖИ ЧРЕЗ ЦИКЛИЧНА РОТАЦИЯ НА ИНДЕКСИТЕ НА ВЪРХОВЕТЕ, Георги А. Козарев 295

ОТ КЛАСИЧЕСКИ QOS КЪМ AGE OF INFORMATION И FRESHNESS OF SERVICE В РАЗПРЕДЕЛЕНИ АСОИУ, Драгомир И. Василев, Сребрин В. Шарбанов 304

ЕКСПЕРИМЕНТАЛНО ИЗСЛЕДВАНЕ НА ВЛИЯНИЕТО НА ПРЕДВАРИТЕЛНАТА ОБРАБОТКА ВЪРХУ КАЧЕСТВОТО НА КЛЪСТЕРИЗАЦИЯТА, Нели А. Арабаджиева-Калчева 320

МЕТОДИ ЗА МАШИННО ОБУЧЕНИЕ В ЕКОЛОГИЧНИ И ГЕОПРОСТРАНСТВЕНИ ИЗСЛЕДВАНИЯ: МЕТОДОЛОГИЧНИ ПРИНЦИПИ ПРИ ИЗБОРА НА МОДЕЛ, Камен К. Калчев 324

ИМИГРАЦИОННА И МИТНИЧЕСКА СЛУЖБА (ICE) НА САЩ, Иво В. Великов 330

ЗАЩИТА НА ПОТРЕБИТЕЛСКИТЕ ДАННИ В ДИГИТАЛНИТЕ ИГРОВИ СРЕДИ, Бориславa Т. Недкова, Даниел Р. Денев 339

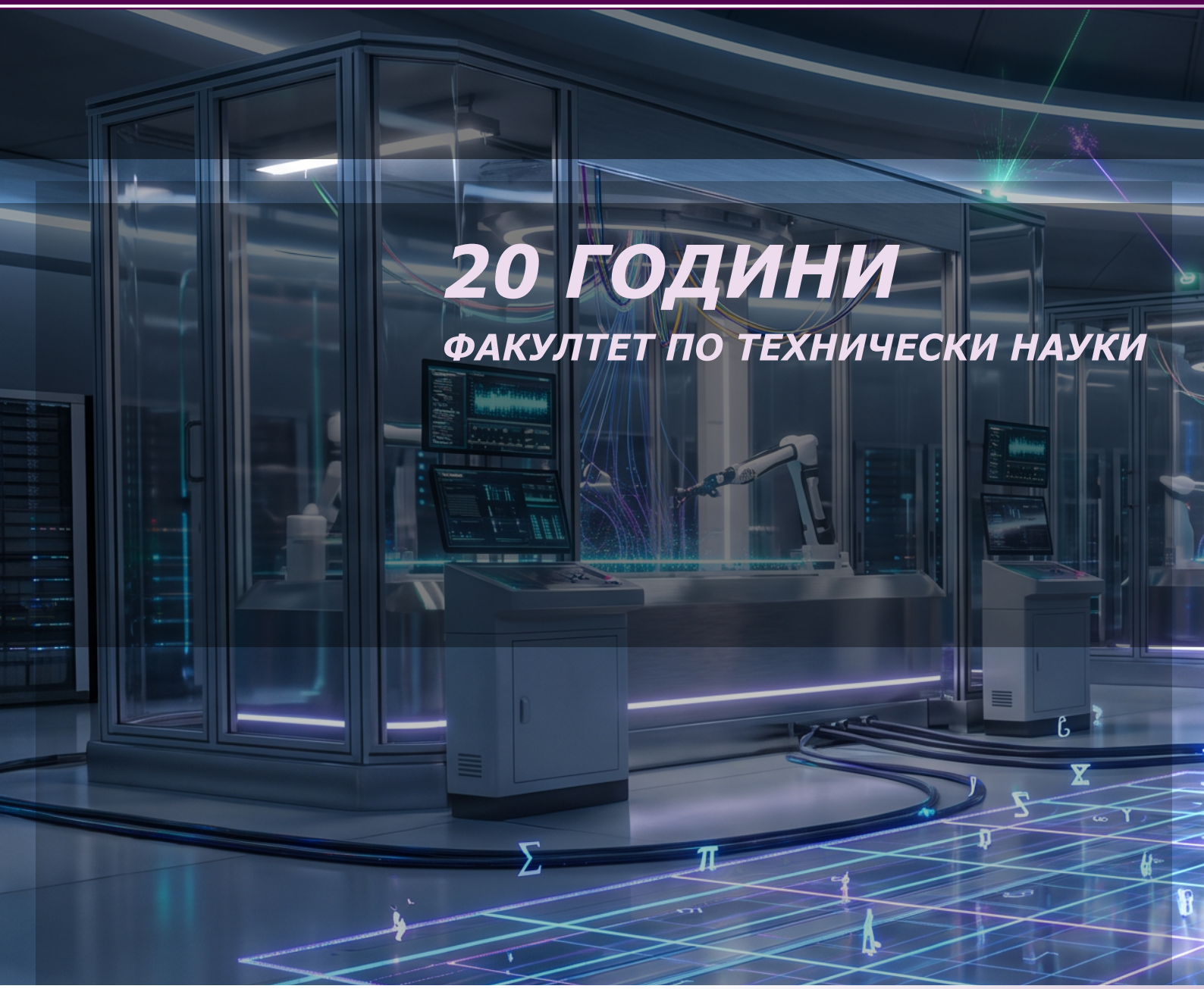
РОЛЯТА НА КРИПТИРАНЕТО ЗА СИГУРНОСТТА НА КОМУНИКАЦИОННИТЕ МРЕЖИ, Илкер А. Хатиб, Алекс Я. Данев 349

МОДЕЛ ЗА КИБЕРСИГУРНОСТ СПОРЕД РЕЖИМА НА РАБОТА ПРИ АВТОМАТИЗИРАНИ И ЕЛЕКТРИЧЕСКИ ПРЕВОЗНИ СРЕДСТВА И ЗАРЯДНА ИНФРАСТРУКТУРА, Емили К. Димитрова, Костадин Д. Костадинов 358

МОДЕЛ НА WEB-БАЗИРАНА СТЕГАНОГРАФСКА СИСТЕМА, Алекс Я. Данев, Валентин Т. Атанасов 367

ИНТЕЛИГЕНТНА СИСТЕМА ЗА РАННО ОТКРИВАНЕ НА ИНЦИДЕНТИ ЧРЕЗ AI АНАЛИЗ НА ВИДЕО И IoDT СЕНЗОРИ, Силвия Х. Николова 375

МИКРОАРХИТЕКТУРНИ СТРАНИЧНИ КАНАЛИ И СМУЩЕНИЯ В DRAM ПАМЕТТА НА СЪВРЕМЕННИТЕ КОМПЮТЪРНИ СИСТЕМИ, Галин П. Пейчев, Велислав И. Стоянов 390



20 ГОДИНИ

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ