

КИБЕРСИГУРНОСТ В ЦЕНТРОВЕ ЗА ДАННИ БАЗИРАНА НА ИЗКУСТВЕН ИНТЕЛЕКТ

Росен Пасарелски

CYBERSECURITY IN DATA CENTERS BASED ON ARTIFICIAL INTELLIGENCE

Rosen Pasarelski

Резюме: Настоящата статия разглежда проблемите и решенията, свързани с киберсигурността в центрове за данни, базирана на изкуствен интелект. С нарастващата роля на цифровите технологии и увеличаването на обема от обработвани данни, центрове за данни се превръщат в критична инфраструктура, изискваща висока степен на защита. Интеграцията на изкуствен интелект в управлението на киберсигурността на тези системи дава възможност за автоматизирано откриване на заплахи, анализ на мрежовия трафик в реално време и адаптивна реакция при инциденти. Целта на статията е да представи систематичен анализ на основните киберзаплахи, засягащи съвременните центрове за данни, да оцени съществуващите методи за защита и да изследва ролята на изкуствения интелект като инструмент за повишаване на тяхната сигурност и автономност. Допълнително се цели идентифициране на проблеми, свързани с внедряването на интелигентни системи, както и очертаване на тенденциите в развитието на сигурни и самоуправляващи се инфраструктури. Постигнатите резултати включват класификация на основните типове киберзаплахи, оценка на ефективността на традиционните защитни механизми и анализ на предимствата на AI базирани подходи, включително алгоритми за машинно обучение, дълбоко обучение и поведенчески анализ. Изследването показва, че използването на интелигентни системи значително подобрява способността за ранно откриване на аномалии, намалява времето за реакция при инциденти и повишава устойчивостта на инфраструктурата срещу сложни и непознати атаки.

Ключови думи: киберсигурност, център за данни, изкуствен интелект, защита, мрежова сигурност, автоматизация.

Abstract: This article examines the problems and solutions related to cybersecurity in data centers based on artificial intelligence. With the growing role of digital technologies and the increase in the volume of processed data, data centers are becoming critical infrastructure requiring a high level of protection. The integration of artificial intelligence into the cybersecurity management of these systems enables automated threat detection, real-time network traffic analysis, and adaptive incident response. The aim of the article is to present a systematic analysis of the main cyber threats affecting modern data centers, to evaluate existing protection methods, and to explore the role of artificial intelligence as a tool for increasing their security and autonomy. Additionally, it aims to identify problems related to the implementation of intelligent systems, as well as outline trends in the development of secure and self-governing infrastructures. The results achieved include a classification of the main types of cyber threats, an assessment of the effectiveness of traditional defense mechanisms, and an analysis of the advantages of AI-based approaches, including machine learning algorithms, deep learning, and behavioral analysis. The study shows that the use of intelligent systems significantly improves the ability to detect anomalies early, reduces incident response time, and increases the resilience of the infrastructure against complex and unknown attacks.

Keywords: cybersecurity, data center, AI, protection, network security, automation.

1. ВЪВЕДЕНИЕ

Съвременното развитие на комуникационните и информационните технологии води до експоненциално нарастване на обема от генерирани и обработвани данни. Центровете за данни се утвърждават като основна инфраструктура, осигуряваща

съхранение, обработка и разпределение на информация в глобален мащаб. С разширяването на облачните услуги, Интернет на нещата (IoT) и дигиталните платформи, значението на сигурността в тези среди нараства съществено. Паралелно с това, внедряването на изкуствен интелект (AI) в управлението на центровете за данни предоставя нови възможности за автоматизация, оптимизация на ресурсите и анализ на големи масиви от данни в реално време. Интелигентните системи могат да откриват аномалии, да предсказват потенциални инциденти и да реагират динамично на възникващи заплахи, което значително повишава ефективността на защитните механизми. Въпреки тези предимства, интеграцията на AI технологии въвежда и нови предизвикателства, свързани със сигурността. Увеличава се сложността на системите, разширява се повърхността на атака, а зависимостта от алгоритми за машинно обучение създава рискове от манипулиране на данните и неправилни решения. Това налага разработването на нови подходи и стратегии за защита, които комбинират традиционни методи за киберсигурност с интелигентни технологии. Съществена роля в този процес имат специалистите по кибертехнологии и инженерите по киберсигурност, които проектират, внедряват и управляват защитните механизми в AI-базираните среди. Те отговарят за конфигурирането на интелигентните системи, анализа на събраните данни, оценката на риска и вземането на крайни решения при възникване на инциденти. Освен това, тяхната експертиза е ключова при обучението и валидирането на AI моделите, за да се обезпечи тяхната надеждност и ефективност срещу кибератаки. В условията на нарастваща автоматизация, човешкият фактор остава критичен за стратегическото управление на сигурността, интерпретацията на резултатите от алгоритмите и адаптирането на системите към нововъзникващи заплахи. Това налага интегриран подход, при който интелигентните технологии и експертните знания на инженерите работят съвместно за осигуряване на надеждна и устойчива киберсигурност. Целта на настоящата статия е да анализира ролята на изкуствения интелект в осигуряването на киберсигурност в центровете за данни, като разгледа основните заплахи, механизми за защита и бъдещи тенденции в развитието на сигурни и автономни инфраструктури.

2. Архитектура на център за данни базирана на изкуствен интелект

Архитектурата на център за данни базирана на изкуствен интелект, се основава на интеграцията на физическа инфраструктура, виртуализирани ресурси и интелигентни софтуерни системи, които работят съвместно за осигуряване на ефективност, надеждност и високо ниво на сигурност. Основните компоненти включват изчислителни ресурси - сървъри, системи за съхранение на данни, мрежова инфраструктура и платформи за управление, върху които се изграждат AI модули за анализ и автоматизация. Тези модули използват алгоритми за машинно обучение и дълбоко обучение за обработка на големи обеми от данни в реално време, като дават възможност за динамично разпределение на ресурсите, откриване на аномалии и оптимизация на работните процеси. Ключов елемент в архитектурата е слой за сигурност, който обединява традиционни механизми за защита като защитни стени, системи за откриване и предотвратяване на прониквания (IDS/IPS), криптиране и контрол на достъпа, с AI-базирани решения за интелигентен мониторинг и анализ. Архитектурата често включва и разпределени компоненти като „edge“ и „cloud“ среди, които позволяват обработка на данни близо до източника и намаляване на латентността. Взаимодействието между тези слоеве се управлява чрез централизирани или децентрализирани платформи, които осигуряват координация, автоматизация и устойчивост на системата.

2.1. Слой за сигурност базиран на AI

Слоят за сигурност в подобна архитектура комбинира традиционни механизми за защита - защитни стени, система за откриване на прониквания (IDS - Intrusion Detection System), система за предотвратяване на прониквания (IPS - Intrusion Prevention System), криптиране, контрол на достъпа и сегментация на мрежата - с AI-базирани решения, които осигуряват:

- **Интелигентен мониторинг** - непрекъснат анализ на мрежовия трафик, логове и системни събития чрез модели за поведенческа аналитика (UEBA - User and Entity Behavior Analytics).
- **Автоматично откриване на заплахи** - ML модели, обучени да разпознават zero-day атаки, ботнет активности, вътрешни злоупотреби и сложни многослойни атаки.
- **Автономен отговор** - системи, които могат да изолират компрометирани ресурси, да блокират подозрителни връзки или да задействат политики за ограничаване на щетите без човешка намеса.
- **Предиктивна сигурност** - анализ на исторически данни за прогнозиране на бъдещи атаки и уязвимости.

Този интелигентен слой се интегрира, както в централната инфраструктура, така и в разпределените компоненти – периферни (edge) устройства, облачни среди и хибридни платформи. Това осигурява обработка и защита на данни близо до източника, намалявайки латентността и риска от компрометиране по пътя.

2.2. Управление и координация

Взаимодействието между физическите, виртуалните и AI компонентите се управлява чрез централизирани или децентрализирани платформи за оркестрация. Те осигуряват:

- автоматизация на процесите по сигурност (SOAR - Security Orchestration, Automation and Response);
- управление на политики за достъп;
- интеграция между AI системи и традиционни защитни механизми;
- устойчивост при атаки чрез разпределени архитектури и резервираност.

2.3. Ролята на инженерите по кибертехнологии

Инженерите по кибертехнологии имат ключова роля в изграждането на тази архитектура. Те извършват операции, както следва:

- проектират структурния модел на центъра за данни с фокус върху сигурността;
- избират подходящи AI инструменти за мониторинг, анализ и автоматизация;
- конфигурират защитни механизми и политики за достъп;
- интегрират AI моделите в инфраструктурата, като обезпечават тяхната надеждност, прозрачност и устойчивост срещу манипулации;
- осигуряват непрекъснат мониторинг, оценка на риска и адаптация към нови заплахи.

Чрез постоянен анализ и оптимизация специалистите потвърждават, че архитектурата остава гъвкава, адаптивна и ефективна срещу еволюиращите киберзаплахи. Така центърът за данни не просто функционира сигурно, а се превръща в самозащитаваща се система, способна да реагира и да се развива в динамична дигитална среда.

3. Киберсигурност в център за данни базирана на изкуствен интелект

Моделите за киберсигурност, управлявани от изкуствен интелект, се основават на използването на алгоритми за машинно обучение и дълбоко обучение за анализ, откриване и предотвратяване на киберзаплахи в реално време. Тези модели обработват големи обеми от мрежови данни, логове и поведенчески характеристики на системите, като идентифицират отклонения от нормалното функциониране и сигнализируют за потенциални атаки. Основните подходи включват контролирано обучение (SL-Supervised Learning) за класификация на известни заплахи, самостоятелно обучение (UL-Unsupervised Learning) за откриване на аномалии и обучение с подсилване (RL-Reinforcement Learning) за адаптивно управление на защитните механизми. Съществен модел в съвременната киберсигурност е поведенческият анализ, при който се изграждат профили на нормално поведение на потребители и системи, а всяко отклонение се разглежда като потенциална заплаха. Друг важен подход е предиктивният модел, който използва исторически данни за прогнозиране на бъдещи атаки и уязвимости. Освен това, се прилагат модели за автоматизирана реакция, които позволяват в реално време изолиране на компрометирани ресурси и ограничаване на разпространението на атаки. Интеграцията на тези модели в центрове за данни води до значително повишаване на ефективността на защитата, но също така изисква внимателно управление и контрол. Инженерите по кибертехнологии играят жизненоважна роля при избора, обучението и валидирането на AI моделите, както и при настройката на параметрите им спрямо конкретната инфраструктура. Те следят за качеството на данните, предотвратяват манипулации като „отравяне на данни“ и потвърждават, че моделите функционират надеждно и ефективно. По този начин се постига баланс между автоматизацията и човешкия контрол, който е критичен за ефективната киберсигурност в AI-базираните системи.

3.1. Основни модели и подходи при киберсигурност базирана на AI

Основните модели и подходи в киберсигурността, управлявана от изкуствен интелект, се характеризират с използването на различни методи за обучение и анализ, които позволяват ефективно откриване, прогнозиране и неутрализиране на заплахи в динамична среда. Те се прилагат върху големи обеми от мрежови данни, системни логове и поведенчески характеристики, като осигуряват многостепенна защита на инфраструктурата, както следва:

- **Контролирано обучение (Supervised Learning – SL)** - Този подход използва предварително означени етикетирани данни за обучение на модели, които могат да разпознават известни видове атаки. Алгоритмите се обучават върху исторически данни, съдържащи примери за нормално и злонамерено поведение, като впоследствие класифицират нови събития в реално време. Предимството на метода е високата точност при откриване на вече познати заплахи, но ограничението е свързано с невъзможността да идентифицира непознати или нововъзникващи атаки.
- **Самостоятелно обучение (Unsupervised Learning – UL)** - При този подход не се използват предварително означени данни, а моделите анализират структурата на входящата информация и откриват скрити зависимости и отклонения. Той е особено ефективен за идентифициране на аномалии в поведението на системите и мрежовия трафик. Самостоятелното обучение дава възможност за откриване на непознати заплахи, но изисква внимателна настройка, тъй като може да генерира фалшиви положителни резултати.

- Обучение с подсилване (Reinforcement Learning – RL) - Този модел се базира на взаимодействие със средата, при което системата се обучава чрез награди и наказания. В контекста на киберсигурността RL се използва за динамично управление на защитните механизми, като например автоматично конфигуриране на защитни стени или оптимизация на реакции при атаки. Предимството е способността за адаптация към променящи се условия, но изисква значителни изчислителни ресурси и време за обучение.
- Поведенчески анализ (Behavioral Analysis - BA) - Поведенческият модел изгражда профили на нормално поведение на потребители, устройства и приложения, използвайки исторически данни. Всяко отклонение от тези профили се счита за потенциална заплаха. Този подход е ефективен при откриване на вътрешни атаки и компрометирани акаунти, тъй като анализира не само технически параметри, но и контекста на действията.
- Предиктивни модели - Предиктивните модели използват статистически методи и машинно обучение за анализ на исторически данни с цел прогнозиране на бъдещи атаки и уязвимости. Те дават възможност за проактивен подход към сигурността, като идентифицират рискове преди тяхната реализация. Това осигурява предварително предприемане на защитни мерки и намаляване на потенциалните щети.
- Модели за автоматизирана реакция - Тези модели осигуряват автоматично реагиране при откриване на заплаха, като включват действия като изолиране на засегнати системи, блокиране на мрежов трафик или рестартиране на услуги. Те функционират в реално време и значително намаляват времето за реакция при инциденти. Въпреки това, изискват прецизна настройка, за да се избегнат нежелани прекъсвания на нормалната работа.

Интеграцията на всички тези модели създава многослойна и адаптивна система за защита, която комбинира предимствата на различните подходи и осигурява високо ниво на киберсигурност базирана на AI в центровете за данни.

4. Сравнителен анализ на AI-базираните модели за киберсигурност

Сравнителният анализ на моделите за киберсигурност, базирани на изкуствен интелект, се извършва по ключови критерии като ефективност на откриване, възможност за внедряване в център за данни, ниво на сигурност, адаптивност, изчислителна сложност и устойчивост на нови заплахи. Различните модели показват специфични предимства и ограничения в зависимост от средата и типа атаки.

Основните критерии за сравнение на моделите за киберсигурност, базирани на изкуствен интелект следват:

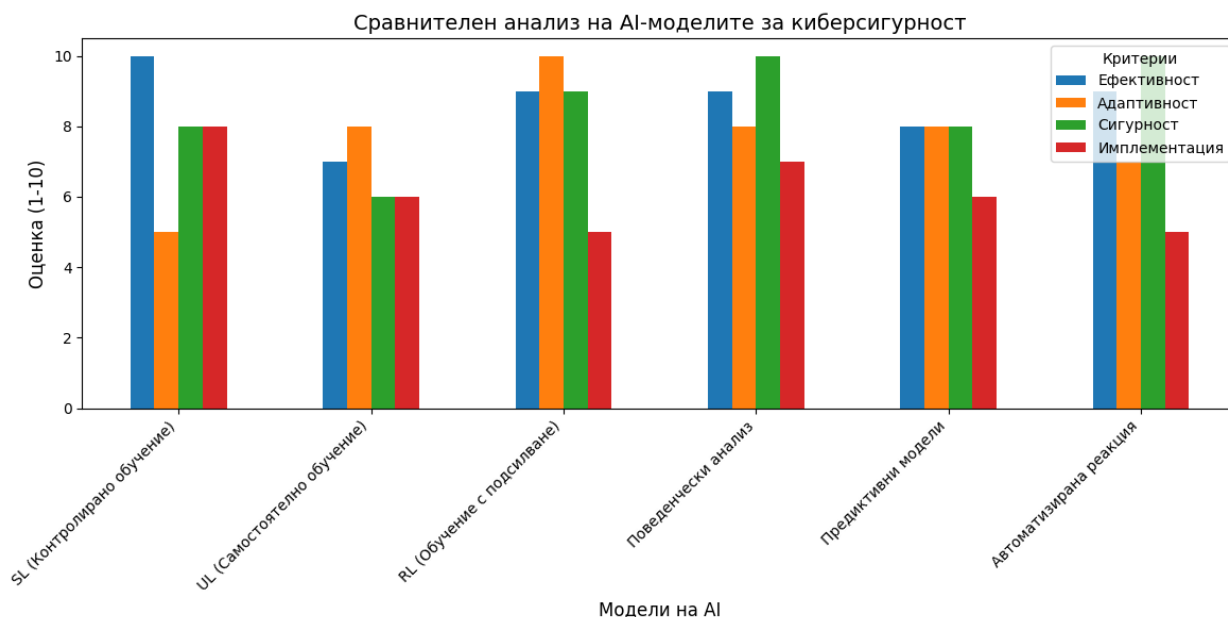
- ефективност;
- ниво на сигурност и устойчивост към атаки и фалшиви аларми;
- адаптивност и способност за работа при нови заплахи;
- сложност на имплементация в център за данни;
- изчислителни ресурси;
- време за реакция.

В таблица 1 е представено сравнение на моделите за киберсигурност, базирани на изкуствен интелект, според основни критерии и показатели.

Таблица 1. Сравнителна таблица на AI моделите

Модел	Ефективност	Ниво на сигурност	Адаптивност	Имплементация в Data Center	Изчислителна сложност	Основни предимства	Основни недостатъци
Supervised Learning (SL)	Много висока	Високо (за познати атаки)	Ниска	Лесна (при налични данни)	Средна	Висока точност и нисък процент грешки	Не открива нови атаки
Unsupervised Learning (UL)	Средна	Средно	Висока	Средна	Висока	Открива аномалии и zero-day атаки	Повече фалшиви аларми
Reinforcement Learning (RL)	Висока	Високо	Много висока	Трудна	Много висока	Адаптивност и автоматизация	Дълго обучение
Поведенчески анализ	Висока	Много високо	Висока	Средна	Средна	Открива insider threats	Зависи от качеството на данните
Предиктивни модели	Средна-висока	Високо	Висока	Средна	Висока	Проактивна защита	Риск от неточни прогнози
Автоматизирана реакция	Висока	Много високо	Висока	Трудна	Средна	Бърза реакция в реално време	Риск от грешни действия

Ефективността на различните модели може да бъде представена графично, чрез фигура 1, за по-добра илюстрация на основни критерии като – ефективност, ниво на сигурност, адаптивност и сложност при имплементация в център за данни, за сравнение на моделите за киберсигурност, базирани на изкуствен интелект.



Фиг.1. Сравнителен анализ на AI-моделите за киберсигурност

Показателите от сравнителният анализ на AI-моделите за киберсигурност се обобщават в таблица 2.

Таблица 2. Показатели от сравнителен анализ на AI-моделите за киберсигурност

Модел	Ефективност	Адаптивност	Ниво на сигурност	Имплементация
SL (Контролирано обучение)	10	5	8	8
UL (Самостоятелно обучение)	7	8	6	6
RL (Обучение с подсилване)	9	10	9	5
Поведенчески анализ	9	8	10	7
Предиктивни модели	8	8	8	6
Автоматизирана реакция	9	7	10	5

- Ефективност – точност при откриване на заплахи (от 1 до 10)
- Адаптивност – способност за справяне с нови заплахи (от 1 до 10)
- Ниво на сигурност – устойчивост на атаки и фалшиви аларми (от 1 до 10)
- Имплементация – сложност при внедряване в център за данни (от 1 до 10)

Сравнителния анализ показва, че няма универсален модел, който да осигурява оптимална защита във всички случаи.

- Контролираното обучение е най-ефективно при известни заплахи.
- Самостоятелното обучение е критично за откриване на нови атаки.
- Обучението с подсилване предлага най-добра адаптивност, но с висока цена.
- Поведенческите и предиктивните модели добавят проактивност.
- Автоматизираните системи намаляват времето за реакция.

В практиката в центровете за данни се прилага хибриден подход, който комбинира всички модели, за да се постигне максимално ниво на сигурност, ефективност и устойчивост срещу съвременните киберзаплахи.

5. Заключение

Развитието на центровете за данни с имплементиран изкуствен интелект, очертава нов етап в еволюцията на комуникационните и информационните инфраструктури, при който автоматизацията, интелигентната обработка на данни и киберсигурността се превръщат във взаимозависими и стратегически значими компоненти. Интеграцията на алгоритми за машинно обучение и дълбоко обучение в архитектурата на центровете за данни осигурява не само оптимизация на ресурсите и повишаване на оперативната ефективност, но и създаване на адаптивни механизми за защита, способни да реагират на динамичния характер на съвременните киберзаплахи. Комбинацията от традиционни защитни технологии, като *IDS* и *IPS системите*, с AI-базирани аналитични модели формира многослоен подход към сигурността, който надхвърля възможностите на класическите системи. Чрез непрекъснат мониторинг, поведенчески анализ и автоматизирани реакции архитектурата придобива способност за ранно откриване на аномалии, прогнозиране на рискове и автономно ограничаване на потенциални атаки. Това превръща сигурността в интегрална характеристика на системата, а не в допълнителен защитен механизъм. В този контекст ролята на инженерите по кибертехнологии е жизненоважна. Те осигуряват структурната и функционална цялост на архитектурата, обезпечават надеждната интеграция на AI моделите и поддържат устойчивостта на системата спрямо нововъзникващи заплахи. Чрез систематичен анализ,

оптимизация и управление на риска специалистите допринасят за изграждането на центрове за данни, които са не само високоефективни, но и безотказни, самонаблюдаващи се и способни да поддържат високо ниво на сигурност в условията на непрекъснато променяща се дигитална среда.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

REFERENCES

- [1] BASTA, A. and W. HALTON. *Computer security and penetration testing*. Cengage Learning, 2013. ISBN 978-0840020932.
- [2] GOODFELLOW, I., BENGIO, Y., and A. COURVILLE. *Deep learning*. MIT Press, 2016. ISBN 978-0262035613.
- [3] HWANG, K. and J. DONGARRA. *Distributed and cloud computing: From parallel processing to the Internet of things*. Morg an Kaufmann, 2013. ISBN 978-0123858801.
- [4] BUCZAK, A. L. and E. GUVEN. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorial* [online]. 2016, vol. 18(2), pp. 1153–1176 [viewed 11.06.2026]. ISSN 1553-877X. Available from: <https://doi.org/10.1109/COMST.2015.2494502>
- [5] KHAN, M. A. and K. SALAH. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* [online]. 2018, (82), pp. 395–411 [viewed 11.06.2026]. eISSN 1872-7115. Available from: <https://doi.org/10.1016/j.future.2017.11.022>
- [6] SHONE, N., NGOC, T. N., PHAI, V. D., and Q. Shi. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence* [online]. 2018, vol. 2(1), pp. 41-50 [viewed 11.06.2026]. eISSN 2471-285X. Available from: <https://doi.org/10.1109/TETCI.2017.2772792>
- [7] ZHANG, Lejun, et. all. Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing. *Transactions on Emerging Telecommunications Technologies* [online]. 2021, vol. 32(10), e4315 [viewed 11.06.2026]. Available from: <https://doi.org/10.1002/ett.4315>
- [8] PASARELSKA, T. Research of the implementation of modern wireless broadband electronic communication services. *Yearbook Telecommunications* [online]. 2024, vol. 11, pp. 69-79 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://ojs.nbu.bg/index.php/YT/issue/view/84>
- [9] DOBREVA, A. Impact of new technologies and artificial intelligence in brand management. *Yearbook Telecommunications* [online]. 2024, vol. 11, pp. 107-117 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.24.11.11>
- [10] АНГЕЛОВ, К. Анализ на сигурността в комуникационни мрежи за интернет на нещата. *Годишник Телекомуникации* [онлайн]. 2024, год. 11, с. 131-141 [прегледан 11.06.2026]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.24.11.13> [ANGELOV, K. Analiz na sigurnostta v komunikatsionni mrezhi za internet na neshtata. *Godishnik Telekomunikatsii* [onlayn]. 2024, god. 11, s. 131-141 [pregledan 11.06.2026]. eISSN 2534-854X. Dostapen na: <https://doi.org/10.33919/YTelecomm.24.11.13>]
- [11] PASARELSKA, T. Analysis of radio frequency spectrum planning and allocation for the deployment of new modern broadband networks and technologies. *Yearbook Telecommunications* [online]. 2023, vol. 10, pp. 79-88. [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.23.10.8>
- [12] IVANOVA, Y. A methodology for empirical research and analysis in the field of cybersecurity. *Yearbook Telecommunications* [online]. 2022, vol. 9, pp. 45-52 [viewed 11.06.2026]. eISSN 2534-854X. Available from: <https://doi.org/10.33919/YTelecomm.22.9.4>
- [13] IVANOVA, Y. Trends in the use of high technology solutions for cybersecurity of critical infrastructure. *Yearbook Telecommunication*. [online]. 2019, vol. 6, pp. 37-44 [viewed 11.06.2026]. eISSN 2534-854X. Available from: [10.33919/YTelecomm.19.6.4](https://doi.org/10.33919/YTelecomm.19.6.4)
- [14] СИМЕОНОВА, Цв. Подход за анализ и моделиране на надеждността на мрежовата свързаност от гледна точка на ефективност и неговата приложимост. *Годишник Телекомуникации* [онлайн]. 2020, год. 7, с. 57-63. [прегледан 11.06.2026]. eISSN 2534-854X. Достъпен на: <https://doi.org/10.33919/YTelecomm.20.7.7> [SIMEONOVA, Tsv. Podhod za analiz i modelirane na nadezhdnostta na mrezhovata svarzanost ot gledna tochka na effektivnost i negovata prilozhimost. *Godishnik Telekomunikatsii* [onlayn]. 2020, god. 7, s. 57-63. [pregledan 11.06.2026]. eISSN 2534-854X. Dostapen na: <https://doi.org/10.33919/YTelecomm.20.7.7>]
- [15] PASARELSKI, R., G. PETROV, T. PASARELSKA, K. ANGELOV. Neural Network Architecture to Predict Radio Wave Attenuation in a 5G Network. In: *31st National Conference with International Participation „Telecom 2023“, November 16 - 17, 2023, Sofia, Bulgaria* [online]. 2023, pp. 1-5 [viewed 21.03.2025]. ISSN 2837-5246. Available from: <https://ieeexplore.ieee.org/xpl/conhome/10409594/proceeding>

- [16] PASARELSKI, Rosen, Krasen ANGELOV, Kristian POSTAGIAN, and Stanimir SADINOV. Implementation and Analysis of a Customized Encryption Algorithm in 5G Networks for Educational Purposes. In: *4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, 23 - 25 November, 2023, Plovdiv, Bulgaria [online]. 2023, pp. 1-5 [viewed 25.03.2025]. eISBN 979-8-3503-3691-7. Available from: 10.1109/CIEES58940.2023.10378834
- [17] СТЕФАНОВА, Тереза. *Новите технологии: приложения, професии, умения: монография*. София: Аскони-издат, 2024. ISBN 978-954-383-151-7. [STEFANOVA, Tereza. *Novite tehnologii: prilozhenia, profesii, umenia: monografia*. Sofia: Askoni-izdat, 2024. ISBN 978-954-383-151-7.]

Информация за автора:

проф. д-р Росен Пасарелски, НБУ департамент „Телекомуникации“, rpasarelski@nbu.bg

Contacts:

Prof. Rosen Pasarelski, PhD, New Bulgarian University, Department „Telecommunications“, rpasarelski@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 25.06.2025

Дата на приемане за публикуване (Date of adoption for publication): 30.09.2025