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.*

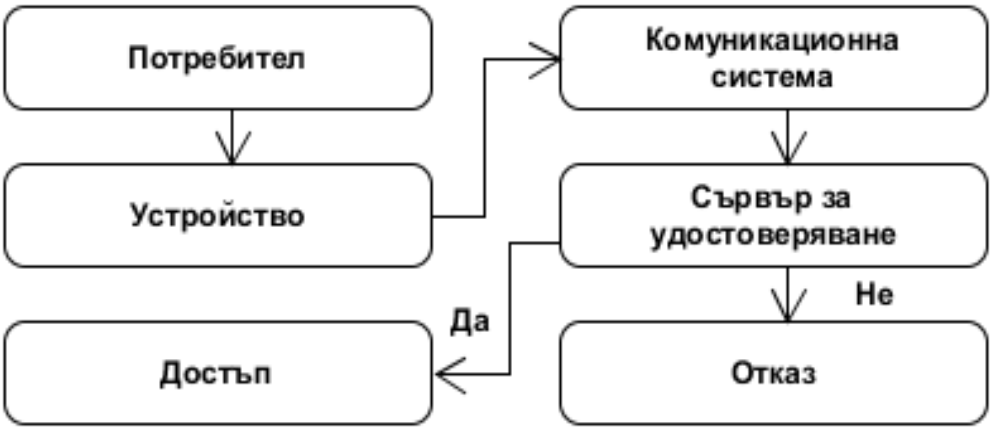
1 Въведение

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.

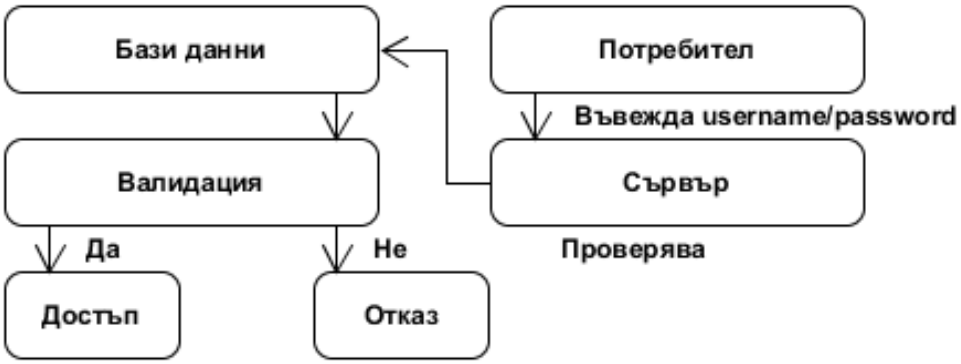
Таблица 1. Роля на удостоверяването в комуникационните системи

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.



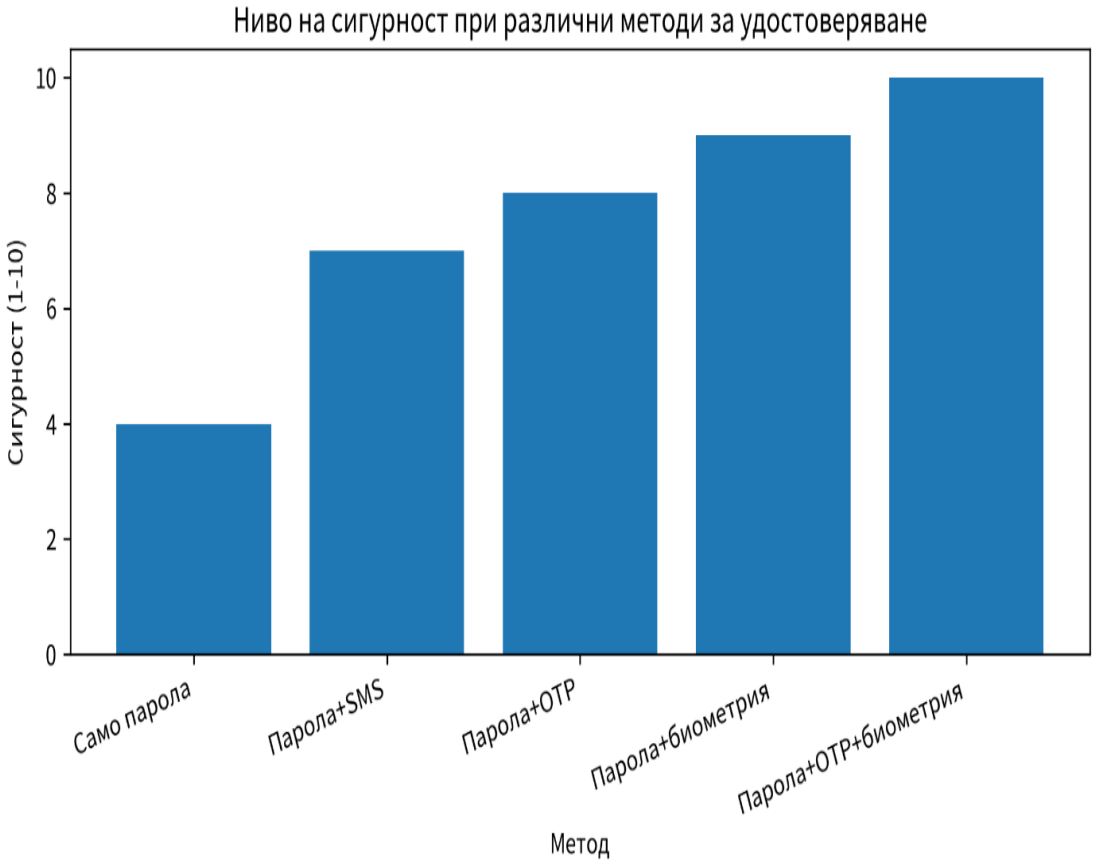
Фиг. 2. Удостоверяване чрез пароли

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

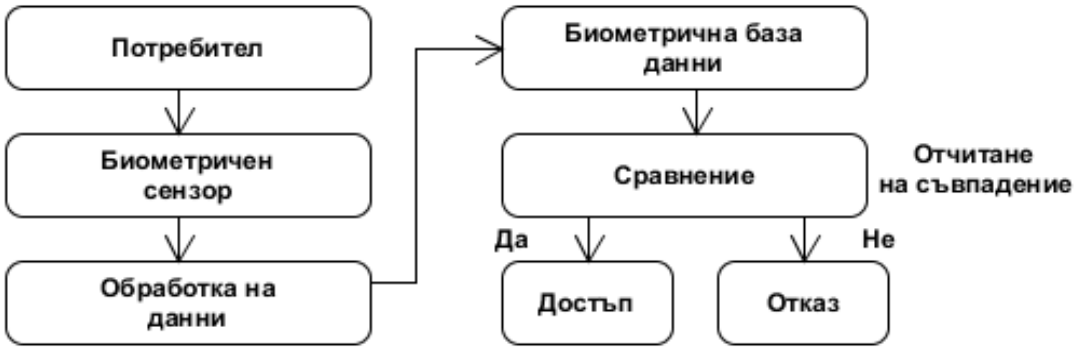
Метод	Брой фактори	Ниво на сигурност (1–10)	Време за вход (сек.)
Само парола	1	4	5
Парола + SMS код	2	7	12
Парола + OTP приложение	2	8	10
Парола + биометрия	2	9	8
Парола + OTP + биометрия	3	10	15



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

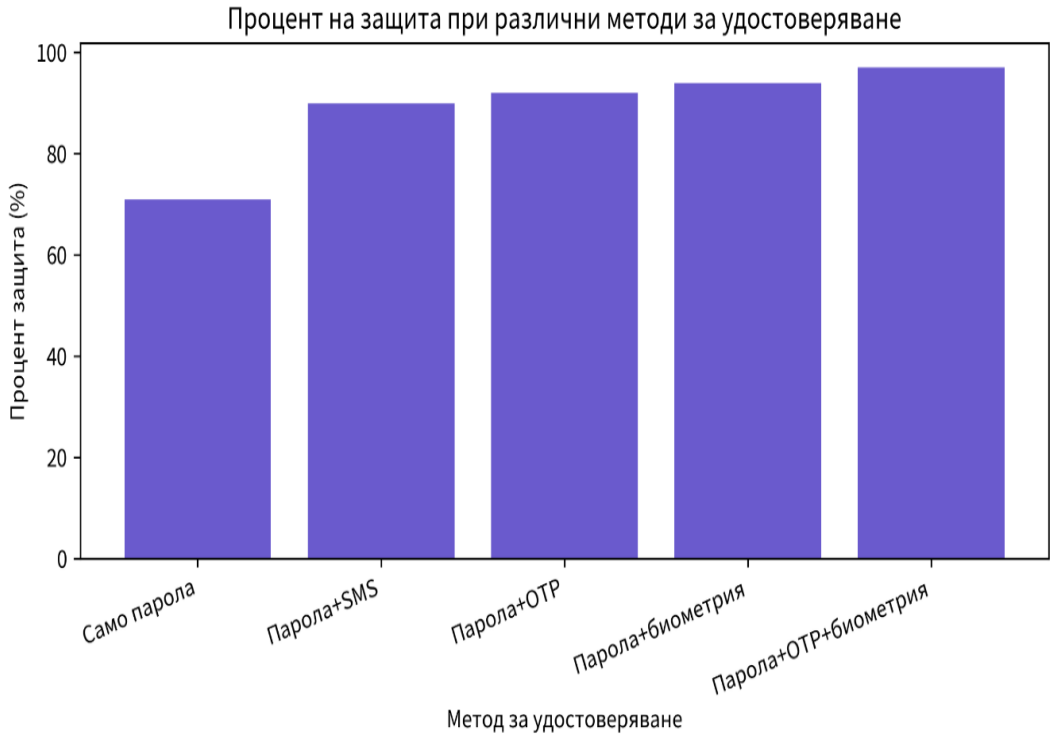
Развитието на комуникационните технологии води до появата на нови подходи за удостоверяване. Сред тях са удостоверяването без парола, използването на криптографски ключове, адаптивното удостоверяване и системите, базирани на изкуствен интелект. Тези технологии анализират поведението на потребителите 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