DOI: 10.20998/2079-0023.2024.02.14
UDC 004.9

V. O. SHAROV, Postgraduate of Department Information Systems and Technologies National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; e mail: wyctpiy@gmail.com; ORCID: https://orcid.org/0000-0003-3152-0650
O. M. NIKULINA, Doctor of Technical Sciences, Professor, Head of Department Information Systems and Technologies National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; e mail: elniknik02@gmail.com; ORCID: https://orcid.org/0000-0003-2938-4215

STUDY OF COMPATIBILITY OF METHODS AND TECHNOLOGIES OF HIGH-LEVEL PROTOCOLS AND ERROR-CORRECTING CODES

Since the year 2000, the fields of error-correction codes and Virtual Private Networks (VPNs) have undergone significant advancements driven by technological demands for higher reliability and security in communication systems. In error-correction codes, the development of turbo codes and Low-Density Parity-Check (LDPC) codes reached new heights, with LDPC codes being adopted in standards like 5G and Wi-Fi 6 for their near-Shannon-limit performance. This period saw groundbreaking contributions from researchers like David MacKay and Radford Neal, who refined LDPC algorithms, and Erdal Arıkan, who introduced polar codes in 2008. Polar codes have since been integrated into 5G systems due to their efficiency and low complexity, marking a milestone in modern coding theory. Advances in decoding methods, such as belief propagation and successive cancellation, further enhanced the utility of these codes in practical applications. Parallel to these developments, VPN technology evolved in response to the growing need for secure and private communication in an increasingly interconnected world. Enhanced encryption protocols such as IPsec and OpenVPN became widespread, supported by innovations in cryptography. Researchers like Hugo Krawczyk contributed to robust authentication mechanisms, such as the HMAC and IKEv2 protocols, ensuring the integrity and confidentiality of VPN tunnels. Meanwhile, the development of WireGuard in the mid-2010s, spearheaded by Jason A. Donenfeld, introduced a lightweight and highly secure VPN protocol, revolutionizing the way modern VPNs operate. These advancements addressed the escalating cyber threats and facilitated the secure exchange of data across global networks. The importance of studying error-correction codes and VPNs in the modern era cannot be overstated. Error-correction codes are integral to overcoming the challenges of high-noise environments, enabling reliable communication in technologies ranging from space exploration to massive IoT networks. Simultaneously, VPNs remain critical for preserving user privacy, securing corporate networks, and protecting sensitive data in the face of sophisticated cyberattacks. Emerging technologies like quantum computing and artificial intelligence introduce both opportunities and threats, necessitating continuous innovation in these fields. Exploring quantum error-correction codes and post-quantum cryptographic protocols represents a vital area for future research. By addressing these challenges, scientists and engineers can ensure the resilience and security of communication systems in an increasingly digital and interconnected world.

Keywords: VPN, FEC, ECC, CIA triad, common security model, cascade codes, data transmission channel

Introduction. In In the modern era of digital communication, the demand for high-speed, reliable data transmission has never been greater. High-level protocols, error-correcting codes (ECC), also known as forward error correcting codes (FEC), are fundamental components of this ecosystem, enabling efficient and secure information exchange across diverse networks. However, the growing complexity of communication systems, driven by the proliferation of IoT devices, 5G networks, and emerging technologies like quantum computing, has highlighted the critical need for compatibility between these methods and technologies [1].

Studying the compatibility of methods and technologies of high-level protocols, among which VPN protocols are set, and error-correcting codes is highly valuable and relevant for several reasons:

- ensuring interoperability: modern communication systems are built on heterogeneous networks that integrate a wide range of devices and technologies. Ensuring compatibility between high-level protocols and ECCs is essential for seamless interoperability, reducing latency, and preventing data loss;
- optimizing network efficiency: compatibility directly impacts the efficiency of data transmission. By aligning protocols with the most suitable error-correcting codes, it is possible to reduce overhead, enhance throughput, and optimize bandwidth utilization, which is critical for applications requiring high data rates such as streaming services, online gaming, and real-time communications;
- enhancing security and reliability: error-correcting codes are crucial for mitigating data corruption, especially in noisy channels or environments with high interference. Compatibility with high-level protocols ensures that ECC mechanisms are effectively implemented, safeguarding data integrity and improving the reliability of communication systems;
- supporting emerging technologies: the evolution of new communication paradigms, such as 5G, 6G, and edge computing, introduces new challenges in protocol design and error correction. A thorough understanding of compatibility between these components allows for better adaptation to these innovations, supporting the development of robust and scalable network architectures;
- reducing implementation costs: mismatched or incompatible protocol and ECC implementations can lead to inefficiencies, increased error rates, and costly redesigns. By studying and ensuring compatibility early in the design process, organizations can reduce implementation [2].

The integration of VPN technologies with advanced error-correcting methods, such as FEC, is not just about improving individual components but about creating a holistic, resilient system capable of meeting the challenges of modern communication networks. By enhancing the compatibility and performance of these technologies, we can achieve more secure, efficient, and reliable data transmission across diverse and demanding environments. It becomes crucial when trying to deal with CIA triad and it’s prerequisites [3].

The purpose and the objectives of study. The purpose of study is in assessing the modern ways of connection between high-level OSI protocols and ECC, clarifying potential and options of unifying them in a concept of one technology.

Objectives can be defined as following:

- consider the possibilities of combining the use of error-correcting codes and VPN within a single outline of a general model for secure data transmission;
- study the possibility of combining error-correcting codes with VPN protocols;
- research the impact of combining error-correcting codes with VPN protocols.

Comprehensive Overview: combining VPN and Error-Correcting Codes (FEC). In modern data transmission, especially over VPN, issues such as unstable networks, high latency, and packet loss can reduce the quality and reliability of connections. By integrating Forward Error Correction (FEC) codes with VPN technologies, we can significantly enhance the stability and security of data transfer.

FEC codes add redundant data to the transmitted information, allowing the system to detect and correct errors without needing retransmissions. This is crucial for VPN scenarios where continuous, secure connections are vital. Below is a detailed analysis of different VPN types and their potential combinations with various FEC codes.

Tunneling in VPN: detailed description. Tunneling is the method of encapsulating original network traffic within another data transfer protocol, creating a secure communication channel between the client and the server.

Main Tunneling Types in VPN are presented below.

- PPTP (Point-to-Point Tunneling Protocol). Uses Layer 2 (Data Link) of the OSI model. Simple to set up but has outdated encryption methods, making it less secure.
- L2TP (Layer 2 Tunneling Protocol). Often combined with IPsec for encryption. It uses both Layer 2 and Layer 3 (Data Link and Network) and offers better security than PPTP due to IPsec protection.
- OpenVPN. Uses SSL/TLS for encryption, providing a high level of security. It works at the Transport layer (Layer 4) and can use various ports, making it flexible and harder to block.
- WireGuard. A modern protocol focused on performance and security, using advanced encryption. It operates at the Network layer (Layer 3) and has lower latency and higher speed than traditional VPNs.

Tunneling protocols secure network connections by encrypting traffic. PPTP is fast and simple but lacks modern security. L2TP with IPsec offers stronger encryption but can be slower due to double encapsulation. OpenVPN is highly secure, flexible, and excellent for bypassing restrictions but requires technical setup. WireGuard is fast, lightweight, and secure, using modern cryptography, though it lacks some advanced features.

Sources and Justifications. I rely on information that Paul Bischoff has written regarding different types of VPN protocols [4]. Also Aleksandar Kochovski's article, which assessed and approved by Aleksander Hougen and Simona Ivanovski was taken in sight [5, 6], results in table 1.

Table 1 – Comparison Table: Tunneling Protocols

Protocol	OSI Layer	Encryption	Security level	Performance
PPTP	Data Link (2)	MPPE (128-bit)	Low	High
L2TP/IPsec	Data Link (2) & Nerwork (3)	IPsec (256-bit)	High	Moderate
OpenVPN	Transport (4)	SSL/TLS (AES-256)	Very High	Moderate to High
WireGuard	Network (3)	ChaCha20, Poly1305	Very High	Very High

1. PPTP (Point-to-Point Tunneling Protocol):

- security Level: PPTP utilizes the Microsoft Point-to-Point Encryption (MPPE) protocol with RC4 encryption, which is considered weak by modern standards. It has known vulnerabilities that can be exploited by attackers;
- performance: Due to its minimal encryption overhead, PPTP offers high performance and faster speeds.

2. L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec):

- security Level: When combined with IPsec, L2TP provides robust security features, including strong encryption and authentication mechanisms;
- performance: The double encapsulation process can introduce additional overhead, leading to moderate performance.

3. OpenVPN:

- security Level: OpenVPN employs SSL/TLS protocols with support for various encryption standards, including AES-256, offering a high level of security;
- performance: Performance can vary based on configuration but generally provides a good balance between speed and security.

4. WireGuard:

- security Level: WireGuard uses modern cryptographic primitives like ChaCha20 for encryption and Poly1305 for data authentication, providing a high level of security;
- performance: Designed for efficiency, WireGuard offers high performance with low latency and high throughput.

Performance Evaluation Metrics:

Evaluating VPN performance involves measuring:

- latency (ms): the time taken for data to travel from source to destination;
- throughput (Mbps): the rate of successful data transfer over a network;
- CPU utilization (%): the amount of processing power required to handle VPN operations;
- packet loss (%): the percentage of data packets that are lost during transmission.

These metrics can be assessed using network performance tools and monitoring systems to determine the efficiency and impact of each VPN protocol on system resources.

Further it is very important to look through all benefits of combining FEC codes and VPN. It can be done in various combinations. For article purposes, it would be better to look through a few examples, bypassing some connections, because of the amount of data. Benefits from combining FEC and VPN shall be balanced and reliable, in terms of practical usability.

Expected Results and Analysis both shown in table 2. The study established the following advantages provided by the use of FEC with various types of VPN protocols [7]. By combining strong sides from both FECs and VPNs with decreasing of influence of weaknesses it becomes possible to create stable and effective combinations.

Table 2 – Detailed Analysis of VPN and FEC Code Combinations

VPN Type	OSI Layer	Characte-ristics	Suggested FEC Code	Benefits of Combination
IPsec VPN	Network (3)	Encryption and packet integrity checks	LDPC, Reed-Solomon	Enhanced reliability and error correction for high-latency networks.
SSL VPN	Transport (4)	Protection via SSL/TLS, browser-based access	Convolutional, Reed-Solomon	Real-time error correction, improved stability in web applications.
L2TP/IPsec	Data Link (2) & Network (3)	Tunneling via L2TP with IPsec encryption	Turbo Codes, LDPC	Balanced low latency and high accuracy for remote access scenarios.
OpenVPN	Transport (4)	Open-source, supports multiple encryption protocols	Turbo Codes, Convolu-tional	Efficient hand-ling of VoIP and streaming data with mini-mal retrains-missions.

Due to table 3 low-density parity-check codes help recover lost data, reducing the need for retransmission and improving throughput, especially beneficial in high-latency environments like satellite networks. LDPC codes can be compared with other powerful coding schemes, e.g. turbo codes. From one side, bit error rate performance of turbo codes is influenced by low codes limitations. However, LDPC codes have any limitations of minimum distance that indirectly states that LDPC codes are more effective on large code rates. It is needed to highlight that LDPC codes, as well as turbo codes, are affected by error floor phenomenon and both have error floor region.

Table 3 – IPsec VPN and LDPC Codes

Metric	Without FEC	With LDPC Codes	Expected Improvement
Packet Loss (%)	20–30	10–15	Reduced by 40–50%
Average Latency (ms)	200	180	Reduced by 10%
Throughput (%)	80	90	Increased by 12%
Retransmissions	High	Low	Reduced retransmissions

Due to table 4 Reed-Solomon codes are highly effective in handling burst errors, making SSL VPN more reliable, especially for web access in mobile and satellite networks.

Table 4 – SSL VPN and Reed-Solomon Codes

Metric	Without FEC	With Reed-Solomon Codes	Expected Improvement
Packet Loss (%)	25–35	15–20	Reduced by 30–40%
Connection Establish-ment (s)	1.2	1	Reduced by 15%
Session Stability	Low	High	Increased stability
Load Errors (%)	High	Low	Reduced by 50%

Due to table 5 turbo codes use iterative decoding for high accuracy, effectively reducing packet loss and latency, improving the quality of video streams and remote access.

Table 5 – L2TP/IPsec VPN and Turbo Codes

Metric	Without FEC	With Turbo Codes	Expected Improvement
Packet Loss (%)	18–25	10–12	Reduced by 50%
Average Latency (ms)	180	160	Reduced by 11%
Video Quality	Medium	High	Improved by 20%
Throughput (%)	85	95	Increased by 12%

Due to table 6 convolutional codes correct real-time errors, ensuring stable and uninterrupted transmission for VoIP and streaming video, which is crucial for OpenVPN.

Table 6 – OpenVPN and Convolutional Codes

Metric	Without FEC	With Convolutional Codes	Expected Improvement
Packet Loss (%)	15–20	8–10	Reduced by 45%
VoIP Latency (ms)	150	130	Reduced by 13%
Audio Quality	Medium	High	Improved by 25%
Stream Stability	Low	High	Increased stability

Due to table 7 integrating FEC codes with different VPN types significantly improves the reliability and quality of data transmission, particularly in challenging network conditions such as mobile and satellite channels. The combined approach offers robust solutions for secure and stable communications, reducing packet loss, increasing throughput, and minimizing latency.

Concept. We have previously investigated the possibilities of using cascaded error-correcting codes and their impact on the triad CIA [8].

The use FEC has wide applicability, but they have long been a well-studied area of data transmission theory [9].

Table 7 – Summary Table: Advantages of Using FEC Codes with Various VPNs

VPN Type	FEC Code	Improved Metric	Expected Improvement
IPsec VPN	LDPC	Packet Loss, Throughput	–40% loss, +12% throughput
SSL VPN	Reed-Solomon	Session Stability, Latency	+30% stability, –15% latency
L2TP/IPsec	Turbo	Video Quality, Packet Loss	+20% quality, –50% loss
OpenVPN	Convolutional	VoIP Quality, Real-Time Errors	+25% VoIP quality, –45% errors

Using FEC and VPN in one algorithm aligns with the CIA triad principles (Confidentiality, Integrity, and Availability) and can be implemented effectively for secure data transmission, in more detail further:

1. Confidentiality:

- encryption at both the first and second stages ensures that data is unreadable to unauthorized entities. This aligns with the need to protect sensitive information during transmission;
- interference-resistant coding adds an extra layer of security by obfuscating the data structure, making it harder to breach.

2. Integrity:

- dual-stage coding ensures data is not tampered with during transmission. If any part of the data stream is altered, the decoding process would fail, signaling potential interference;
- cryptographic hash functions can be integrated into the algorithm to verify the integrity of transmitted data packets.

3. Availability:

- the robust structure of the VPN tunnel and error-resilient coding minimizes disruptions caused by noise or attacks, ensuring uninterrupted data access.
- implementing redundancy mechanisms within the coding process can further enhance data availability [10].

Implementation Steps:

1. Coding and Encryption:

- use state-of-the-art encryption algorithms such as AES-256 or ChaCha20, coupled with error-resilient codes like Reed-Solomon or LDPC (Low-Density Parity-Check);
- incorporate protocols like WireGuard or OpenVPN for modern, high-performance tunneling.

2. Interference Resistance:

- embed interference-resistant coding at both the first and second stages to mitigate the risk of errors caused by noisy channels or external interference.

3. Physical Transmission:

- utilize secure physical and virtual communication channels. Employ Secure Socket Layer (SSL)/Transport Layer Security (TLS) to safeguard data at the transport layer.

4. Error Handling and Decoding:

- implement mechanisms to identify and correct errors during the decoding process, ensuring data reliability.

5. Decryption:

- after verifying data integrity, decrypt the data at the recipient's end using secure cryptographic keys.

Detailed algorithm is presented in fig.1 [11].

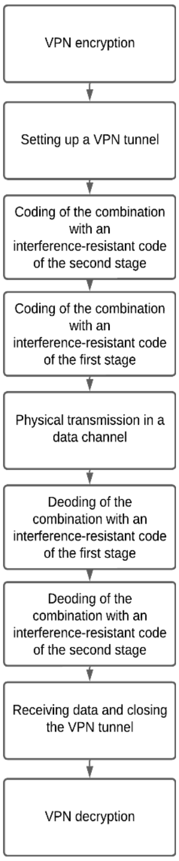
VPN encryption
Setting up a VPN tunnel
Coding of the combination with an interference-resistant code of the second stage
Coding of the combination with an interference-resistant code of the first stage
Physical transmission in a data channel
Deoding of the combination with an interference-resistant code of the first stage
Deoding of the combination with an interference-resistant code of the second stage
Receiving data and closing the VPN tunnel
VPN decryption

Fig. 1. Algorithm of using cascade codes with this model

As said, different types of ECC codes can be used, more on fig. 2 [12, 13].

Conclusions. We have already explored and analyzed several approaches to integrating Error Correction Codes (ECC) with VPN technology, uncovering their potential to enhance data transmission reliability and security. These studies have demonstrated how ECC, combined with Forward Error Correction (FEC) methods, can address critical challenges like packet loss, interference, and noise in modern communication systems. By embedding error-resilience directly into the transmission process, ECC and FEC reduce the dependency on retransmissions, ensuring smoother and faster communication over VPNs, even in adverse network conditions.

VPNs are essential for creating encrypted tunnels that protect data from eavesdropping and tampering. When combined with robust error-correction mechanisms, they provide an additional layer of reliability, ensuring that transmitted information remains accurate and undistorted. This is especially valuable in high-demand applications such as real-time video streaming, telemedicine, and remote work environments, where even minor transmission errors can disrupt critical processes.

Continued research in this domain is vital for the evolution of IT technologies. As networks become increasingly complex with the rise of 5G, IoT, and quantum

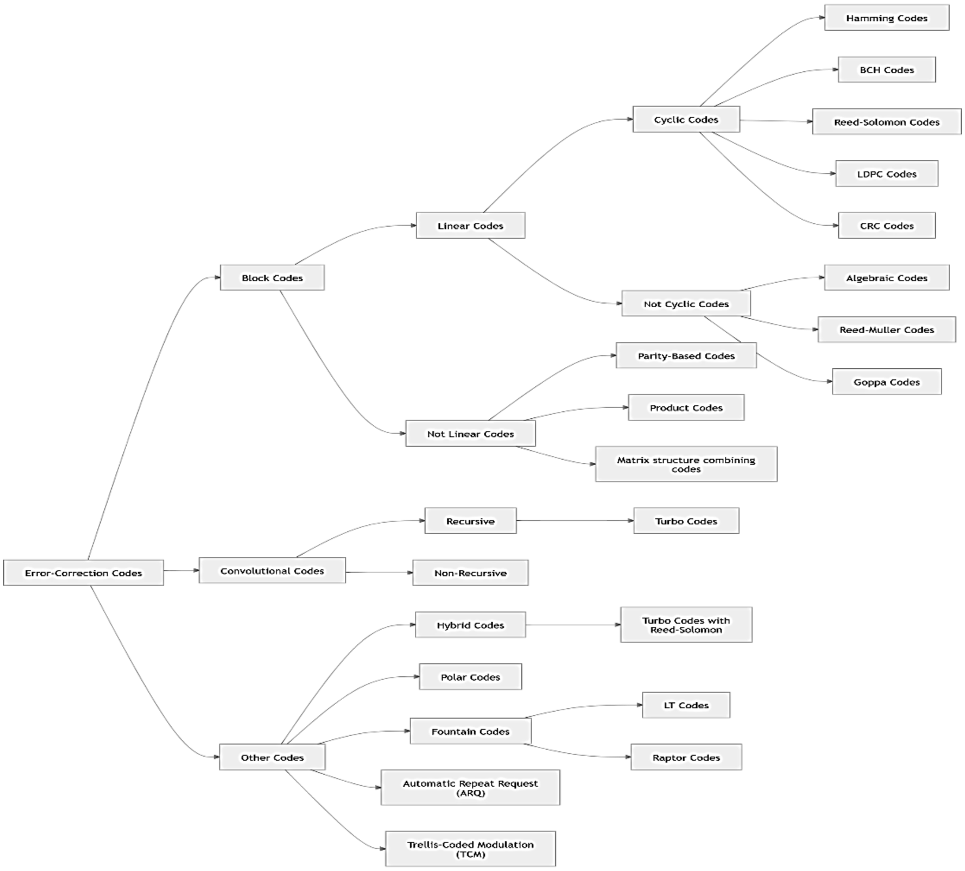

Fig. 2. ECC common types

computing, the demand for secure and efficient data transmission methods will grow exponentially. By studying ECC and its integration with VPNs, we can pave the way for innovative communication protocols that are not only faster and more reliable but also resilient against emerging cybersecurity threats. These advancements will lay the groundwork for the next generation of digital infrastructure, driving progress across industries and ensuring the seamless connectivity required in an interconnected world.

References

1. Stallings W. *Data and Computer Communications. 10th ed*. Pearson, 2013. 912 p.
2. Tanenbaum A. S., Wetherall D. J. *Computer Networks. 5th ed*. Pearson, 2010, 960 p.
3. Nieles M., Dempsey K., Pillitteri V. Y. *An Introduction to Information Security. National Institute of Standards and Technology, Special Publication 800 – 12 Revision 1*, June 2017. 101 p. URL: https://nsarchive.gwu.edu/document/22632-document-07-michaelnieles-kelley-dempsey-and (accessed 02.11.2024).
4. Bischoff P., *VPN protocols explained and compared*. Available at: https://www.comparitech.com/vpn/protocols. (accessed 02.11.2024).
5. Kochovski A., Hougen A., Ivanovski S. *A Full VPN Protocols List in 2024: Explained and Compared*. URL: https://www.cloudwards.net/vpn-protocol-breakdown/ (accessed 02.11.2024).
6. Kochovski A., Hougen A., Ivanovski S. *PPTP vs OpenVPN: Differences, Advantages & Disadvantages in 2024*. URL: https://www.cloudwards.net/pptp-vs-openvpn/ (accessed 02.11.2024).
7. Vincent R., Belkacem T., Christophe B., Tuan T. Cédric T. Less latency and better protection with AL-FEC sliding window codes: A robust multimedia CBR broadcast case study. *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, October 2017, Italy. 9 p.
8. Шаров В. О., Нікуліна О. М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. *Вісник Національного технічного університету «Харківський політехнічний інститут»: зб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології*. Харків: НТУ «ХПІ», 2024. № 1 (11).. С. 70–75.
9. Шаров В. О., Нікуліна О. М., Северин В. П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник Національного технічного університету «Харківський політехнічний інститут»: зб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології*. Харків: НТУ "ХПІ", 2023. № 1 (9). С. 60–69.
10. Stallings W., Brown L. *Computer Security: Principles and Practice*. New York, Prentice Hall, 2008. 817 p..
11. Pfleeger C. P., Pfleeger S. L. Security in Computing. New Jersey, Prentice Hall, 2003. 746 p.
12. Tiller J. S. *The Ethical Hack: A Framework for Business Value Penetration Testing*. Auerbach Publications, 2005. 352 p.
13. Банкет В. Л., Іващенко В. Л., Іващенко М. О. *Завадостійке кодування в телекомунікаційних системах*. Одеса, ОНАЗ ім. О. С. Попова, 2011. 100 с.

References (transliterated)

1. Stallings W. *Data and Computer Communications. 10th ed*. Pearson, 2013. 912 p.
2. Tanenbaum A. S., Wetherall D. J. *Computer Networks. 5th ed*. Pearson, 2010. 960 p.
3. Nieles M., Dempsey K., Pillitteri V. Y. *An Introduction to Information Security. National Institute of Standards and Technology, Special Publication 800 – 12 Revision 1*, June 2017. 101 p. URL: https://nsarchive.gwu.edu/document/22632-document-07-michaelnieles-kelley-dempsey-and (accessed 02.11.2024).

4. Bischoff P., VPN protocols explained and compared. Available at: https://www.comparitech.com/vpn/protocols. (accessed 02.11.2024).
5. Kochovski A., Hougen A., Ivanovski S. *A Full VPN Protocols List in 2024: Explained and Compared*. Available at: https://www.cloudwards.net/vpn-protocol-breakdown/. (accessed 02.11.2024).
6. Kochovski A., Hougen A., Ivanovski S. *PPTP vs OpenVPN: Differences, Advantages & Disadvantages in 2024*. Available at: https://www.cloudwards.net/pptp-vs-openvpn/ (accessed 02.11.2024).
7. Vincent R., Belkacem T., Christophe B., Tuan T. Cédric T. Less latency and better protection with AL-FEC sliding window codes: A robust multimedia CBR broadcast case study. *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, October 2017, Italy. 9 p.
8. Sharov V. O., Nikulina O. M. Dvorivneva kontseptsiya dlya modelyuvannya yedynoyi zavadostiykoyi peredachi tsyfrovykh danykh [A two-level concept for simulating a single interference-resistant digital data transmission] *Bulletin of the National Technical University "KhPI". Series: System analysis, management and information technologies*. Kharkiv, NTU "KhPI" Publ., 2024, no. 1 (11), pp. 70–75. (In Ukr.).
9. Sharov V. O., Nikulina O. M., Severyn V. P. Modelyuvannya ta analiz koderiv zavadostiykykh kaskadnykh kodiv dlya dynamichnykh system [Modeling and analysis of encoders of interference-tolerant cascade codes for dynamic systems]. *Bulletin of the National Technical University "KhPI". Series: System analysis, management and information technologies*. Kharkiv, NTU "KhPI" Publ., 2023, no. 1 (9), pp. 60–69. (In Ukr.).
10. Stallings W., Brown L. *Computer Security: Principles and Practice*. New York, Prentice Hall, 2008. 817 p..
11. Pfleeger C. P., Pfleeger S. L. *Security in Computing*. New Jersey, Prentice Hall, 2003. 746 p.
12. Tiller J. S. *The Ethical Hack: A Framework for Business Value Penetration Testing*. Auerbach Publications, 2005. 352 p.
13. Banket V. L., Ivashchenko P. V., Ishchenko M. O. *Zavadostijke koduvannja v telekomunatsijnyh systemah* [Interference-resistant coding in telecommunication systems]. Odesa, ONAZ named O. S. Popova Publ., 2011. 100 p. (In Ukr.).

Received 05.11.2024

УДК 004.9

В. О. ШАРОВ, аспірант кафедри інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; e-mail: wyctpiy@gmail.com; ORCID: https://orcid.org/ 0000-0003-3152-0650

О. М. НІКУЛІНА, д-р техн. наук, професор, завідувачка кафедри інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; e-mail: elniknik02@gmail.com; ORCID: https://orcid.org/0000-0003-2938-4215

ДОСЛІДЖЕННЯ СУМІСНОСТІ МЕТОДІВ І ТЕХНОЛОГІЙ ПРОТОКОЛІВ ВИСОКОГО РІВНЯ ТА КОДІВ ВИПРАВЛЕННЯ ПОМИЛОК

Починаючи з 2000 року, галузі кодів для виправлення помилок і віртуальних приватних мереж (VPN) зазнали значних успіхів, зумовлених технологічними вимогами до вищої надійності та безпеки систем зв’язку. У кодах для виправлення помилок розробка турбо-кодів і кодів перевірки парності з низькою щільністю (LDPC) досягла нових висот, коли коди LDPC були прийняті в таких стандартах, як 5G і Wi-Fi 6, через їхню продуктивність, близьку до меж Шеннона. У цей період були внесені новаторські внески таких дослідників, як Девід Маккей і Редфорд Ніл, які вдосконалили алгоритми LDPC, і Ердал Арикан, який представив полярні коди в 2008 році. Відтоді полярні коди були інтегровані в системи 5G завдяки їх ефективності та низькій складності, що стало важливою віхою в сучасній теорії кодування. Досягнення в методах декодування, таких як поширення переконань і послідовне скасування, ще більше підвищили корисність цих кодів у практичних застосуваннях. Паралельно з цими розробками технологія VPN розвивалася у відповідь на зростаючу потребу в безпечному та приватному спілкуванні у все більш взаємопов’язаному світі. Удосконалені протоколи шифрування, такі як IPsec і OpenVPN, отримали широке поширення, підтримані інноваціями в криптографії. Такі дослідники, як Хьюго Кравчик, зробили внесок у створення надійних механізмів автентифікації, таких як протоколи HMAC і IKEv2, які забезпечують цілісність і конфіденційність тунелів VPN. Тим часом розробка WireGuard у середині 2010-х років, яку очолив Джейсон А. Доненфельд, представила легкий і високозахищений протокол VPN, який революціонізував роботу сучасних VPN. Ці досягнення спрямовані на вирішення ескалації кіберзагроз і сприяють безпечному обміну даними в глобальних мережах. Важливість вивчення кодів виправлення помилок і VPN у сучасну епоху неможливо переоцінити. Коди виправлення помилок є невід’ємною частиною подолання проблем середовищ із високим рівнем шуму, забезпечуючи надійний зв’язок у різних технологіях, від дослідження космосу до масивних мереж Інтернету речей. Водночас VPN залишаються критично важливими для збереження конфіденційності користувачів, безпеки корпоративних мереж і захисту конфіденційних даних перед обличчям складних кібератак. Нові технології, такі як квантові обчислення та штучний інтелект, створюють як можливості, так і загрози, що вимагає постійних інновацій у цих сферах. Вивчення квантових кодів корекції помилок і постквантових криптографічних протоколів є життєво важливою областю для майбутніх досліджень. Вирішуючи ці виклики, вчені та інженери можуть забезпечити стійкість і безпеку комунікаційних систем у все більш цифровому та взаємопов’язаному світі.

Ключові слова: VPN, FEC, ECC, тріада CIA, єдина модель безпеки, каскадні коди, канал передачі даних.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Шаров Владислав Олегович / Sharov Vladyslav Olegovich
Автор 2 / Author 2: Нікуліна Олена Миколаївна / Nikulina Olena Mykolaivna