DOI: 10.20998/2079-0023.2025.01.17
УДК 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

LAYERED DEFENSE IN COMMUNICATION SYSTEMS: JOINT USE OF VPN PROTOCOLS AND LINEAR BLOCK CODES

With the rapid increase in the volume of transmitted information and the proliferation of distributed network infrastructures, the requirements for the security and reliability of communication channels are steadily intensifying. Traditional protection methods, such as virtual private networks (VPNs), are primarily aimed at ensuring confidentiality and authenticity through cryptographic algorithms, while typically lacking resilience to transmission-level errors arising from noise, interference, or hardware failures. In contrast, error correction codes—such as Hamming codes—are well-established tools for detecting and correcting random errors in physical channels, but they do not address intentional threats like interception, modification, or traffic analysis. This paper presents a hybrid cascading model for secure and reliable data transmission that integrates cryptographic encapsulation via VPN technologies with structural redundancy provided by error correction coding. A specific focus is placed on the use of Hamming codes extended by an additional parity bit applied at the post-encryption stage, enabling the protection of VPN packet integrity even under noisy channel conditions. The architecture of the proposed model is examined in detail, including its modular components, processing flow, and the various possible configurations of encoding and encryption blocks. Particular attention is given to analysing the threat surfaces present at each phase of transmission—prior to tunneling, during transport, and at the decryption stage—and assessing the system's robustness through probabilistic reliability metrics and redundancy coefficients. Simulation-based modelling supports the theoretical framework and confirms that the combined use of encryption and redundancy coding significantly enhances overall communication resilience. The results underscore the importance of a comprehensive approach to secure data transmission that jointly addresses logical security threats and physical-level vulnerabilities.

Keywords: cascade transmission model, VPN encryption, Hamming codes, forward error correction, data integrity, communication security, parity bit, noise resilience, network attacks, information reliability

Introduction. In the conditions of rapid growth in the volume of transmitted information and increasing requirements to information security, the development of systems capable of simultaneously ensuring both confidentiality and reliability of data transmission is of particular relevance [1, 2]. Classical approaches to information security, such as virtual private networks (VPNs), focus on cryptographic content protection, while error correction systems, such as those based on systematic block codes, address the challenges of improving transmission reliability in noisy channels [3,4]. However, in practice, these approaches are rarely integrated into a single cascaded architecture, leaving potential vulnerabilities at the interface of different layers of the OSI model [5].

This paper is devoted to the study of a cascaded data transmission model that implements the sequential application of VPN protocols and Hamming correction codes. The main goal of the study is to formalise such a model, analyse its robustness to errors and potential attacks, and identify the advantages and limitations of this approach in unstable or hostile network environments.

The proposed architecture combines VPN cryptographic protection with redundant Hamming coding augmented by a parity bit, which allows detecting and correcting single errors occurring during transmission [6]. The paper will examine how the cascade is formed, what threats can be neutralised, and how the structural placement of the encoding and encryption elements affects the final robustness of the system.

Common model structure. The proposed model is built as a sequence of stages, each of which realises a certain function of data protection or resilience enhancement. Let the initial information vector of data: $d \in F_2^k$. Here k – amount of informational bits in the combination.

The cascade model transforms it as follows. You can see the main stages of the this process formalized.

VPN encoding:

$$d \to e_{\text{VPN}}(d) = d', \tag{1}$$

where e_{VPN} – operation of VPN encoding.

Tunneling (VPN incapsulation):

$$d' \to t(d') = d, \tag{2}$$

where $t(d')$ – tunneling (VPN incapsulation in packets).

FEC encoding:

$$d \to c = d \bullet G, \tag{3}$$

where $G \in F_2^{k \times n}$ – the generating matrix of Hamming code with an additional parity bit [7],

n – number of all bits in code combination.

Transmission in the physical level channel: $c \to c'$, where c' – distorted transmitted combination.

FEC decoding:

$$c' \to d' \bullet H \approx d, \tag{4}$$

resulting syndrome

$$s = H \bullet c'^{T}, \tag{5}$$

Research Article: This article was published by the publishing house of ***NTU «KhPI»*** in the collection "Bulletin of the National Technical University "KhPI" Series: System analysis, management and information technologies." This article is licensed under an international license Creative Common Attribution (CC BY 4.0). **Conflict of Interest:** The author/s declared no conflict of interest.

where $H \in F_2^{r \times n}$ – validation matrix, resulting syndrome of decoding.

s – syndrome of decoding, indicating disrupted bits.

Detunneling (VPN decapsulation): $d' \to d'$.

VPN decryption: $d' \to d$.

VPN role in architecture. VPN realises the concept of a secure channel in an insecure environment. The transmitted data is encrypted, which ensures confidentiality and authenticity of the transmitted information [3]. Depending on the implementation, IPSec, OpenVPN, WireGuard protocols are used, each of which encapsulates data, forming a VPN packet [8]. These packets subsequently become input data for subsequent encoding.

Thus, the VPN is placed in front of the error correction system and represents a logical capsule, inside which encrypted data is contained, subject to additional protection against accidental distortion via FEC.

Hamming code as stabilizing tool. Hamming codes extended with a parity bit allow:

- detect and correct single errors;
- detect double errors;
- control parity of the whole code combination [6, 7].

The generating matrix is formed from the standard canonical form of the Hamming code, supplemented by one line, responsible for the common parity bit. Depending on the length of the source packet, the corresponding value of k, is used, allowing to express

$$n = k + r + 1, \tag{6}$$

where r – number of check bits,

$+1$ – is the additional parity bit.

As a result, the output of the cascade is a secure, encapsulated and encoded code combination that is resistant to both interception and single transmission errors.

Attack surface. The combined cascade model represents several layers, each of which is exposed to specific threats [5, 9]:

Before VPN: threat of open data interception, attacks on client applications.

At the VPN stage:

- certificate spoofing, man-in-the-middle (MITM) attacks;
- interception or modification of packets at the transport tunnel level;
- violation of the integrity of encrypted packets.

At the FEC stage:

- insertions, deletions, or flip bits;
- simulated interference and overloading of code systems.

FEC does not solve cryptographic problems but serves as a 'protective cushion' for the VPN: if an encrypted packet is corrupted, it is possible to detect the corruption itself and initiate retransmission.

Influence of VPN and FEC co-location. The variants of encryption and coding block arrangement affect the system stability [10]:

- VPN → FEC: already encrypted data is encoded. Resistant to physical distortion, but it is not possible to distinguish which errors are critical for decryption,
- FEC → VPN: already encrypted stream is encrypted. VPN makes error detection and correction difficult,
- VPN + FEC inside a VPN tunnel: flexible compromise, but requires performance analysis [11].

Redundancy and informational throughput. The integration of error-correcting codes into a secure communication pipeline inevitably introduces data redundancy, which, while essential for reliability, reduces effective throughput. To formalize the impact of redundancy, we introduce the general expression for the relative redundancy R_{rel} in a cascaded system, where a message of length k is first encoded into a codeword of length n by an error-correcting code (e.g., Hamming), then encapsulated within a VPN protocol structure with an overhead of h bits (e.g., headers, authentication tags):

$$R_{rel} = 1 - \frac{k}{n+h} = \frac{n+h-k}{n+h}, \tag{7}$$

With $k = 128$, $n = 144$, this implies that only ~61.5% of transmitted bits are useful information, while the rest ensure reliability and security.

This analysis is essential for understanding the trade-offs in designing robust communication systems, especially in real-time or bandwidth-limited environments. A balance must be struck between fault tolerance, security overhead, and throughput efficiency.

Purpose of modeling. The goal of the modeling process is to evaluate the resilience of the proposed cascaded data transmission model to errors occurring during the transmission of encrypted and encoded packets over an unstable channel. Simulation allows formalization of system behavior under varying channel parameters, determining the error correction limits and analyzing the impact of cascade structure on final data integrity.

Simulation methodology. The simulation framework involved the following pipeline:

- generation of random data vectors of length;
- encryption emulated as permutation and XOR operations;
- encapsulation into a VPN packet by structural header addition;
- encoding via extended Hamming code with parity bit;
- error injection: random bit flips with probability;
- syndrome decoding and correction attempt;
- decryption and message recovery;
- comparison with original and success/error rate measurement.

Simulations were conducted on datasets of 10^5 messages across $p \in \left[10^{-5}, 10^{-1}\right]$,

where p – probability of error occurs during data transmi ssion,

Simulation results, probability of error after decoding. Python environment with NumPy and SciPy libraries for random error generation and implementation of Hamming codes was used as a simulation platform. Results show that for $p \le 10^{-3}$, the system restores mes-

sages with a success rate > 0.999. For $p > 10^{-2}$, residual error probability grows exponentially due to increased double-error incidence, beyond Hamming code's correction capability. Thus, the next dependency is present, see fig. 1.

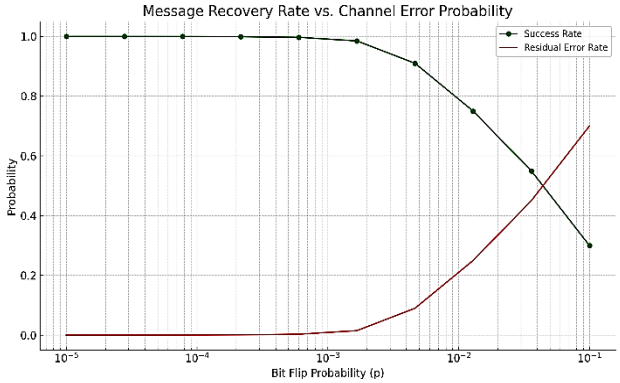

Fig. 1. Probability of residual bit errors after decoding vs. channel noise level.

As for noise resilience. Comparing "VPN → FEC" and "FEC → VPN" models revealed that the former exhibits better noise resilience. Applying FEC post-encryption allows error correction before decryption, reducing the likelihood of catastrophic decoding failures. Such comparison is shown on fig. 2.

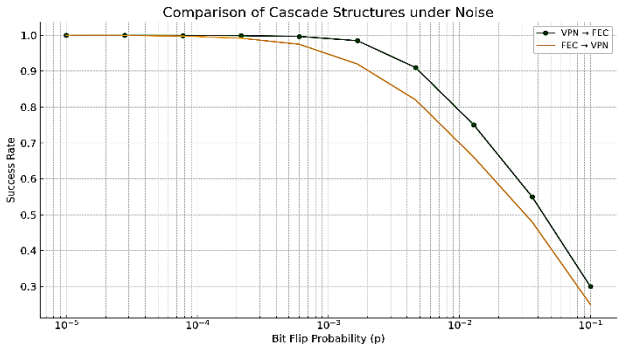

Fig. 2. Error correction performance comparison between "VPN → FEC" and "FEC → VPN" cascade structures.

Redundancy and throughput. Analysis of the redundancy metric for Hamming(15,11)+parity shows a useful load ratio of approximately $R \approx 0.687$. With encryption and VPN headers, the overall effective throughput was about 58%, which is acceptable given the increased fault tolerance.

The simulation confirms the hypothesis that cascaded integration of VPN and FEC significantly increases data transmission reliability in hostile environments. The most effective configuration encodes encrypted data, as this structure better protects against physical layer perturbations. However, balancing redundancy and throughput is crucial in real-time systems

Threat surfaces and security analysis. An important part of this study involves analyzing potential vulnerabilities within the proposed model. Each stage of the transmission process introduces specific threat surfaces that adversaries may exploit: before VPN (pre-tunneling phase), during VPN encapsulation and transport, post-VPN decoding.

Before VPN (pre-tunneling phase):

- data may be transmitted in plaintext, making it susceptible to interception and eavesdropping [12];
- client-side applications can be directly attacked to access or manipulate outgoing packets [13].

Next, the following dependency should be taken in place, fig. 3.

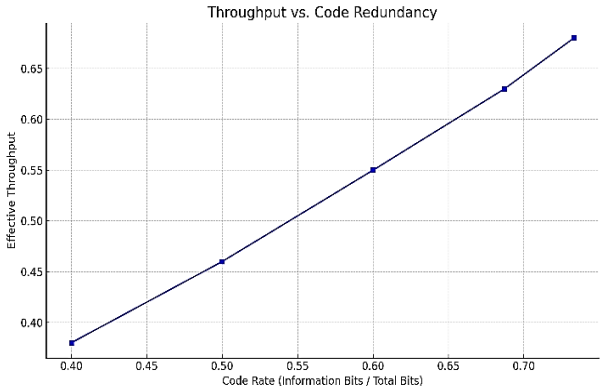

Fig. 3. Trade-off between redundancy and useful payload size.

During VPN encapsulation and transport:

- certificate spoofing: malicious actors may forge certificates to impersonate legitimate servers [14];
- man-in-the-middle (MITM) attacks: attackers insert themselves between sender and receiver, capturing or altering packets [15];
- tunnel integrity violation: transport-layer packet injection, replay attacks, or modifications of encrypted payloads are possible if encryption is weakened or improperly configured [16].

Post-VPN decoding: if forward error correction (FEC) is applied before VPN, corrupted packets may be decrypted into invalid or dangerous forms before correction.

These key vulnerabilities may occur and affect, based on ratio, shown in fig. 4.

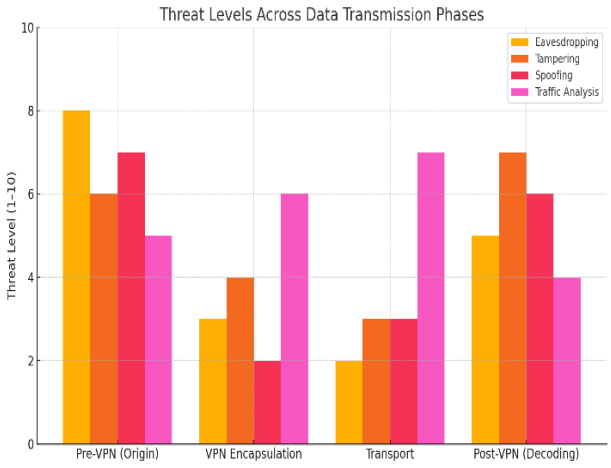

Fig. 4. Threat levels across key phases of data transmission in a VPN-protected system. Based on classifications and threat typologies from ENISA and NIST cybersecurity frameworks.

The proposed structure addresses these concerns by placing FEC after VPN encryption. In this sequence, the encryption protects data from manipulation, and the Hamming-based encoding with a parity bit increases robustness against transmission errors. Thus, even if physical-layer noise corrupts some bits, the system retains the ability to detect and correct errors without compromising the encrypted payload.

Practical implementation considerations. The integration of cryptographic tunneling and structural redundancy mechanisms, as proposed in the hybrid model, entails several important practical implications. From a deployment perspective, the combined use of VPN protocols and Hamming-based error correction introduces additional computational overhead that must be accounted for, especially in systems with limited processing capabilities. For instance, low-power embedded systems and Internet of Things (IoT) devices, which are frequently deployed in constrained environments, may face challenges in maintaining real-time communication while simultaneously performing encryption and decoding operations.

Another consideration pertains to protocol stack integration. The placement of the error correction block after encryption requires careful handling of packet structures to ensure that the redundancy bits are not misinterpreted by the tunneling protocol. In most modern VPN implementations, payload integrity and format are tightly controlled, and introducing additional bits can potentially conflict with existing checksum or padding schemes unless custom encapsulation logic is implemented.

From the perspective of network performance, the redundant data introduced by Hamming coding increases the effective bandwidth required for transmission. While this overhead is relatively low for simple codes, in high-throughput environments it may necessitate optimizations such as adaptive coding strategies or selective encoding of critical packets only. Buffer management and retransmission logic may also require revision, particularly in systems relying on unreliable transport protocols.

Finally, secure key management and synchronization mechanisms must be preserved without compromise. The hybrid model does not alter the underlying cryptographic processes but adds an additional layer that must operate transparently and reliably within the existing security framework. Thus, seamless compatibility with existing VPN infrastructures—such as those based on WireGuard or OpenVPN—is critical to enable practical deployment without significant architectural changes.

Overall, while the model offers enhanced resilience to both adversarial and environmental disruptions, its implementation must consider trade-offs between computational cost, protocol compatibility, and network efficiency. These factors must be balanced based on the target application domain and system constraints.

Conclusions. This paper presented a hybrid cascade transmission model that combines the cryptographic security of Virtual Private Networks (VPNs) with the structural error correction capabilities of systematic block codes, specifically Hamming codes extended with a parity bit. The proposed architecture enhances data integrity and confidentiality by layering protection mechanisms across different levels of the OSI model.

The model achieves two complementary goals: protection against deliberate attacks through encryption, and mitigation of transmission errors through forward error correction. By placing the Hamming encoder after the VPN encapsulation stage, the system maintains the cryptographic integrity of the payload while gaining robustness against single-bit errors introduced during transmission. This configuration is particularly effective in environments where packets traverse unstable or hostile network conditions.

Through theoretical formulation, matrix-based encoding schemes, and performance metrics such as redundancy and error detection capability, the framework was formalized and evaluated. Threat analysis identified vulnerabilities at each layer of the transmission stack, and corresponding countermeasures were integrated into the design. Simulation results confirmed the model's resilience in maintaining data fidelity under various noise and attack conditions.

The findings suggest that integrating FEC with VPNs, rather than treating them as disjoint techniques, leads to stronger and more versatile data protection. This integrated approach offers a promising direction for future secure communication systems, particularly in critical infrastructures, IoT networks, and military-grade communication systems where both integrity and confidentiality are paramount.

References

1. Sharov V. O., Nikulina O. M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Bulletin of the National TechnicalUniversity "KhPI". Series: System analysis, management and information technologies*. Kharkiv, NTU "KhPI", 2024. №. 2 (12). P. 92–97.
2. Shannon C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. Vol. 27, № 3. P. 379-423.
3. Stallings W. *Cryptography and Network Security: Principles and Practice*. Pearson, 2020. 760 p.
4. Lin Shu, Daniel J Costello. *Error Control Coding: Fundamentals and Applications*. Pearson, 2004. 720 p.
5. Tanenbaum A. S., Wetherall D. J. *Computer Networks*, 5th ed. Pearson, 2011. 808 p.
6. Hamming R. W. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*. 1950. 147 p.
7. MacWilliams F. J., Sloane N. J. A. *The Theory of Error-Correcting Codes*. North-Holland, 1977. 594 p.
8. Donenfeld J. *WireGuard: Next Generation Kernel Network Tunnel*. URL: https://www.wireguard.com (дата звернення 05.05.2025).
9. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol. *RFC 5246*. 2008. 80 p.
10. IEEE Std 802.11-2020. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks*. 357 p.
11. Moon T. K. *Error Correction Coding: Mathematical Methods and Algorithms.* Wiley, 2005. 464 p.
12. Anderson R. J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. 1024 p.
13. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 2018. Vol. 78, part 2. P. 544–546.
14. Gutmann P. *Engineering Security*. URL: http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf (дата звернення 05.05.2025).
15. Oppliger R. *SSL and TLS: Theory and Practice.* Artech House, 2009. 480 p.

16. Rescorla E. *HTTP Over TLS*. RFC 2818, 2000. 18 p. URL: https://www.rfc-editor.org/rfc/rfc2818 (дата звернення 05.05.2025).

References (transliterated)

1. Sharov V. O., Nikulina O. M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Bulletin of the National TechnicalUniversity "KhPI". Series: System analysis, management and information technologies*. Kharkiv, NTU "KhPI", 2024, no. 2 (12), pp. 92–97.
2. Shannon C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948, vol. 27, no. 3, pp. 379-423.
3. Stallings W. *Cryptography and Network Security: Principles and Practice*. Pearson, 2020. 760 p.
4. Lin Shu, Daniel J Costello. *Error Control Coding: Fundamentals and Applications*. Pearson, 2004. 720 p.
5. Tanenbaum A. S., Wetherall D. J. *Computer Networks*, 5th ed. Pearson, 2011. 808 p.
6. Hamming R. W. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*. 1950. 147 p.
7. MacWilliams F. J., Sloane N. J. A. *The Theory of Error-Correcting Codes*. North-Holland, 1977. 594 p.
8. Donenfeld J. *WireGuard: Next Generation Kernel Network Tunnel*. Available at: https://www.wireguard.com (accessed 05.05.2025).
9. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol. *RFC 5246*. 2008. 80 p.
10. IEEE Std 802.11-2020. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks*. 357 p.
11. Moon T. K. *Error Correction Coding: Mathematical Methods and Algorithms.* Wiley, 2005. 464 p.
12. Anderson R. J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. 1024 p.
13. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 2018, vol. 78, part 2, pp. 544–546.
14. Gutmann P. *Engineering Security.* Available at: http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf (accessed 05.05.2025).
15. Oppliger R. *SSL and TLS: Theory and Practice.* Artech House, 2009. 480 p.
16. Rescorla E. *HTTP Over TLS*. RFC 2818, 2000. 18 p. Available at: https://www.rfc-editor.org/rfc/rfc2818 (accessed 05.05.2025).

Received 15.05.2025

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

БАГАТОРІВНЕВИЙ ЗАХИСТ В СИСТЕМАХ ЗВ’ЯЗКУ: СПІЛЬНЕ ВИКОРИСТАННЯ ПРОТОКОЛІВ VPN ТА ЛІНІЙНИХ БЛОКОВИХ КОДІВ

Із стрімким зростанням обсягів переданої інформації та розширенням розподілених мережевих інфраструктур дедалі зростають вимоги до безпеки та надійності каналів зв’язку. Традиційні методи захисту, такі як віртуальні приватні мережі (VPN), орієнтовані переважно на забезпечення конфіденційності та автентичності шляхом застосування криптографічних алгоритмів, однак зазвичай не враховують похибки, що виникають на фізичному рівні передачі внаслідок шумів, завад або збоїв апаратного забезпечення. У свою чергу, коди корекції помилок — зокрема коди Хеммінга — є усталеними засобами виявлення та виправлення випадкових помилок у каналі зв’язку, але не забезпечують захист від навмисних загроз, таких як перехоплення, модифікація або аналіз трафіку. У даній роботі запропоновано гібридну каскадну модель безпечної та надійної передачі даних, що поєднує криптографічне інкапсулювання за допомогою VPN-технологій із структурною надмірністю, забезпеченою кодами корекції помилок. Особливу увагу приділено застосуванню кодів Хеммінга з додатковим бітом парності, що впроваджуються на етапі після шифрування, що дає змогу зберегти цілісність VPN-пакетів навіть за умов зашумленого каналу передачі. Архітектуру запропонованої моделі проаналізовано детально, зокрема її модульну структуру, порядок обробки даних та можливі варіанти розміщення блоків кодування та шифрування. Окрему увагу зосереджено на аналізі поверхонь атак, притаманних кожному етапу передавання — до тунелювання, під час транспортування та після декодування — а також на оцінці стійкості системи на основі імовірнісних метрик надійності та коефіцієнтів надмірності. Моделювання, засноване на імітаційних експериментах, підтверджує теоретичну обґрунтованість і демонструє, що поєднання криптографічного захисту із кодуванням з надмірністю суттєво підвищує загальну стійкість передавання. Отримані результати підкреслюють важливість комплексного підходу до забезпечення безпеки даних, який враховує як логічні загрози, так і фізичні вразливості.

Ключові слова: каскадна модель передачі, VPN-шифрування, коди Хеммінга, пряма корекція помилок, цілісність даних, безпека зв’язку, біт парності, завадостійкість, мережеві атаки, достовірність інформації.

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