UDC 004.75 **doi:** https://doi.org/10.20998/3083-6298.2025.01.07

Bogdan Tomashevsky[1], Serhii Yevseiev[2], Oleksandr Sitchenko[2], Roman Korolov[2]

[1] Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
[2] National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine

MODEL OF A COMBINED SPECIAL PURPOSE COMBAT CONTROL SYSTEM

Abstract. Topicality. The rapid advancement of computing technology, mobile and Internet technologies, and the digital economy, hybridity and synergy, as well as the development of post-quantum cryptography (particularly the advent of full-scale quantum computers), impose increasingly stringent requirements on the design principles of specialized security mechanisms in contemporary special purpose systems. The conduct of hybrid warfare necessitates modifications not only to the architectural principles of special communication systems (SCS) and systems for delivering combat commands and signals to operational units, but also requires the development of fundamentally novel approaches for command formation and transmission utilizing both dedicated SCS equipment and open commercial systems based on Internet technologies and modern wireless data transmission protocols. **Objective.** In this article, the authors propose a structural scheme of the advanced combat command and control system of the Armed Forces of Ukraine, which uses both the special communication system in service and open commercial cyberspace systems, with each message being divided into separate components transmitted through all channels, with open channels using digital steganography and/or lossy cryptography methods. **Results.** At the same time, the interception of individual components in each channel will not allow the adversary to obtain the source text. The final recipient receives a combat command/signal on the basis of a majority selection from all channels, for all parts of the message. This approach makes it possible, in the context of the economic crisis, to ensure the fulfilment of tasks in a timely manner in the face of modern countermeasures (suppression, partial or complete destruction) to the combat control system through the use of cyberspace infrastructure (synthesis of modern technologies of computer systems and networks, Internet technologies, and mobile communication technologies). **Conclusions.** The presented mathematical component of the assessment of the reliability and probability of delivery of relevant commands/signals allows the proposed model to be modelled with due regard for various interventions in the special-purpose system, both external and internal.

Keywords: modified special purpose system, cyberspace, quantum period, steganography

Introduction

Contemporary developments in computing technology, the rapid evolution of cyberspace technologies, and the emergence of novel hybrid threats impose increasingly rigorous requirements on special purpose systems. These requirements stem from the necessity to deliver combat commands and signals with high levels of reliability, security, and operational efficiency under hybrid warfare conditions, while considering the adversary's capability to suppress and/or destroy military combat control systems.

The developmental trajectory of modern Armed Forces of Ukraine encompasses the integration of cutting-edge information technologies. Given the imperative to preserve the achievements of the Unified Control System Project of the Armed Forces of Ukraine [1-7] while incorporating NATO standards, this approach necessitates not only the development of standardization programs for the Ministry of Defense of Ukraine's information infrastructure based on international standards and NATO methodologies, but also the capability to counter contemporary threats characterized by hybridity and synergism.

Analysis of recent research and publications [1-11] establishes the requirement for an automated C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) system for defense force components that must comply with NATO standards, doctrines, and recommendations across all command levels (tactical, operational, and strategic) with clearly defined baseline capabilities. However, under conditions of national economic decline, pandemic-related constraints, reduced modernization rates, delayed implementation of advanced information technologies within Armed Forces of Ukraine units, and the potential emergence of full-scale quantum computers, the critical issue becomes the creation or modification of existing combat control systems in the context of rapidly advancing Internet technologies and mobile communications [12-14].

Furthermore, specialists at NIST USA [15-18] have identified the vulnerability of symmetric and asymmetric cryptographic systems that ensure cyberspace security (encompassing Internet technologies, computer systems and networks, and LTE technologies) under conditions of full-scale quantum computer deployment (post-quantum period).

Concurrently, the Internet of Things (IoT) ecosystem is experiencing rapid expansion. By 2030, IoT device populations may reach hundreds of billions; Cisco projects approximately 500 billion devices [20]. Data transmission rates continue to escalate: 5G networks achieve approximately 10 Gbps, while prospective 6G and 7G networks are projected to attain peak velocities of 1 Tbps and 1 Pbps respectively [13]. These specifications enable the implementation of fundamentally novel communication systems, including military and specialized channels requiring ultra-high bandwidth and transmission reliability. By 2025, each connected individual interacts with digital data approximately every 18 seconds [20]; consequently, the exponential growth in IoT-generated data volumes underscores the critical role of advanced 5G/6G/7G networks in supporting and utilizing this information flow.

Research objectives. The primary objective of this research is to develop a structural model for a prospective special purpose system.

To achieve this objective, the following tasks must be accomplished:

- development of a structural framework and mathematical model for a prospective special purpose system;
- mathematical evaluation of message delivery probability using a special purpose system;
- mathematical assessment of message delivery reliability using a special purpose system;
- development of reliability assessment methodologies for message delivery via special purpose systems;
- development of a prospective data transmission model utilizing steganographic techniques.

1. Mathematical model and structural framework of the prospective special purpose combat control system

To ensure security, reliability, and operational efficiency in transmitting combat commands and / or signals, the national confidential information system is employed.

The National Confidential Communication System represents an integrated collection of special dual-purpose communication systems and networks that, through cryptographic and technical means, facilitate the exchange of confidential information in support of state government agencies and local self-government bodies, creating appropriate conditions for their interaction during peacetime and under conditions of special or martial law [1-4]. The National Confidential Communication System constitutes a component of Ukraine's Unified National Communication System.

Components of the National Confidential Communication System include:

- special communication systems and networks;
- stationary and mobile components of special communication systems and networks;
- centralized information protection systems and operational-technical management systems.

A Special Communication System (Network) is defined as a communication system or network designed for exchanging information with restricted access. A Special Dual-Purpose Communication System (Network) is a special communication system or network designed to provide communications for state government agencies and local self-government bodies, utilizing a portion of its resources to provide services to other consumers. Subjects of the National Confidential Communication System include state government agencies and local self-government bodies, legal entities and individuals participating in the creation, operation, development, and utilization of this system. Management of the National Confidential Communication System, including its operation, development, utilization, and information protection, is ensured by a specially authorized central executive body in the field of confidential communications in accordance with legislation. Centralized information protection systems and operational-technical management systems remain under state ownership and are not subject to privatization. Other components of the National Confidential Communication System may be owned by business entities regardless of ownership form. The primary characteristic of such systems is their hierarchical structure and transmission methodology based on forward error correction. This approach requires the transmission of additional (redundant or verification) symbols, which significantly facilitates enemy detection, suppression, and/or complete blocking of these communication channels.

However, the rapid development of computational resources, network, and mobile technologies enables the utilization of these communication channels, considering their "steganographic" properties. This approach has been implemented in defense and combat management systems DRMIS (Defense Resource Management Information System) and C4ISR (Automated Operational Combat Control System of the Armed Forces of Ukraine). However, these systems were not developed in Ukraine and require significant economic and human resources for deployment, training, and maintenance. Furthermore, their utilization does not ensure the possibility of forming a unified automated combat control system for the Armed Forces of Ukraine and necessitates transition to new communication complexes. "Steganographic" properties refer to the capability of concealing from adversaries or malicious actors the fact, location, timing, and content of transmitted information by decomposing combat commands and signals into discrete blocks or packets. This approach enables the utilization of open communication channels with commercial information delivery methods to recipients through decisive feedback mechanisms. Additionally, implementing this approach does not require significant economic and human resources.

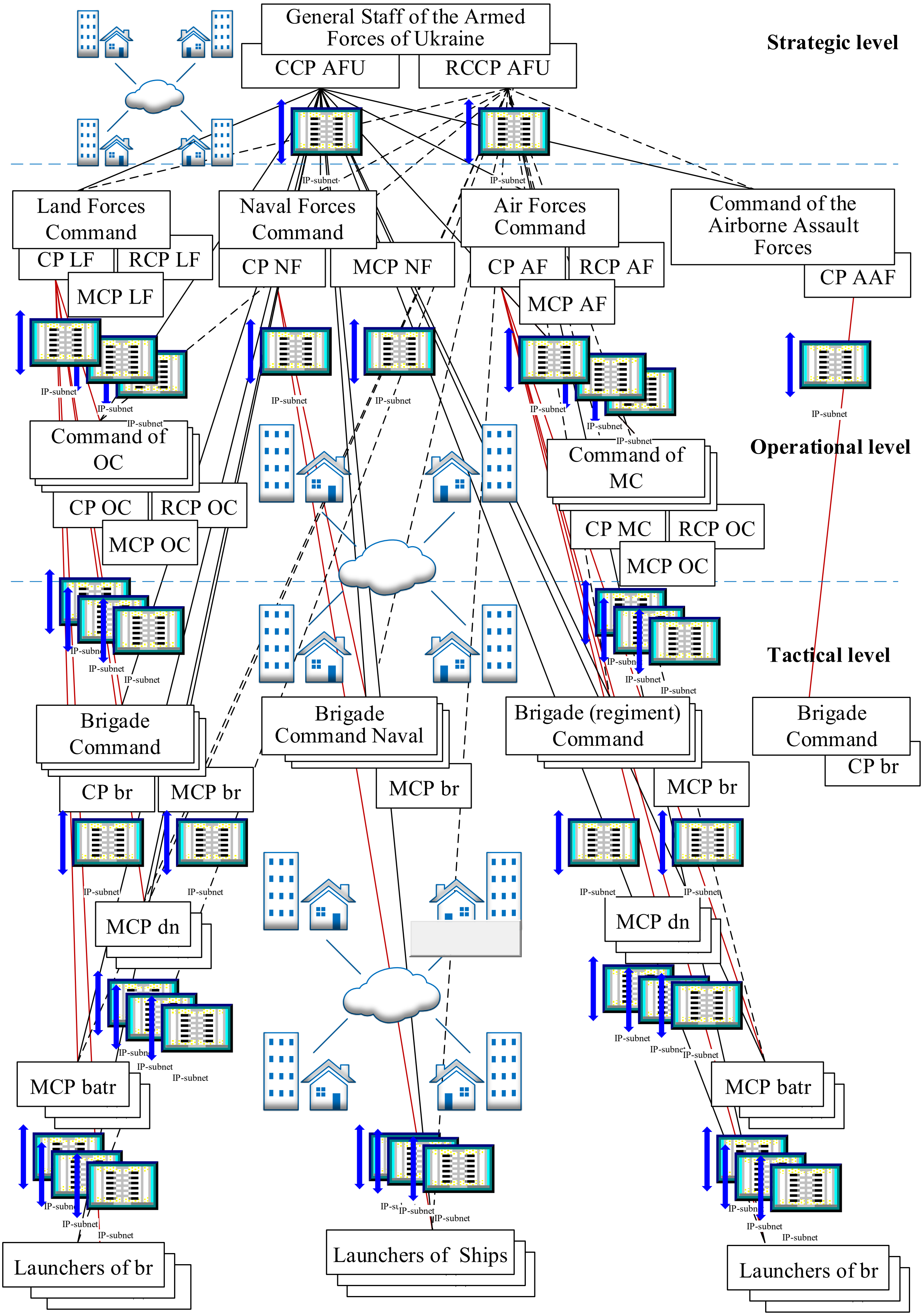


Fig. 1. Structural diagram of the modified combat control system model of the Armed Forces of Ukraine

Consider the model of the modified combat control system using the Armed Forces of Ukraine as an example, illustrated in Figure 1. The modified system proposes utilizing both National Confidential Communication System objects: special communication systems and networks (automated combat control systems for Armed Forces branches, military communication systems), special dual-purpose systems (the "Dnipro" system), as well as open public Internet systems and mobile communication systems based on "G" technologies.

In this system, switching nodes are designated as: ch_i^{scsGF} *special communication systems of the Ground Forces*, $i \in \overline{1,\dots I}$, ch_j^{scsAF} *special communication systems of the Air Force*, $j \in \overline{1,\dots J}$, ch_l^{scsNF} *special communication systems of the Naval Forces*, $l \in \overline{1,\dots L}$, ch_k^{sdpsD} *special dual-use system Dnipro*, $k \in \overline{1,\dots K}$, ch_m^{oIS} *open Internet system* $m \in \overline{1,\dots M}$, ch_q^{omcs} *open mobile communication system* $q \in \overline{1,\dots Q}$. Communication channels are designated accordingly: l_{ix}^{scsGF}, $x \in \overline{1,\dots X}$, l_{jy}^{scsAF}, $y \in \overline{1,\dots Y}$, l_{lz}^{scsNF}, $z \in \overline{1,\dots Z}$, special dual-purpose system l_{kf}^{sdpsD}, $f \in \overline{1,\dots F}$, open Internet system l_{mv}^{oIS}, $v \in \overline{1,\dots V}$, open mobile communication system l_{qn}^{omcs}, $n \in \overline{1,\dots N}$.

In this system, switching nodes will be denoted as: special communication systems of the Ground Forces ch_i^{scsGF}, $i \in \overline{1,\dots I}$, special communication systems of the Air Force ch_j^{scsAF}, $j \in \overline{1,\dots J}$, special communication systems of the Naval Forces ch_l^{scsNF}, $l \in \overline{1,\dots L}$, special dual-use system Dnipro ch_k^{sdpsD} , $k \in \overline{1,\dots K}$, open Internet system ch_m^{oIS} $m \in \overline{1,\dots M}$, open mobile communication system ch_q^{omcs}, $q \in \overline{1,\dots Q}$. The communication channels will be denoted accordingly: l_{ix}^{scsGF}, $x \in \overline{1,\dots X}$, l_{jy}^{scsAF}, $y \in \overline{1,\dots Y}$, l_{lz}^{scsNF}, $z \in \overline{1,\dots Z}$, special-purpose dual-use system l_{kf}^{sdpsD}, $f \in \overline{1,\dots F}$, open Internet system l_{mv}^{oIS}, $v \in \overline{1,\dots V}$, open mobile communication system l_{qn}^{omcs}, $n \in \overline{1,\dots N}$.

Thus, the overall system of the proposed combat control system will comprise a set of individual components of intermediate switching nodes and channels, and the overall probability of receiving a command and/or signal is determined by the following formula:

$$
\begin{aligned}
P_{\text{пр.п.}}^{Q^{ACCS}} = {} & \left(\sum_{i=1}^{I} p_i^{scsGF} ch_i^{scsGF} \times \sum_{ix=1}^{X} p_{ix}^{scsGF} l_{ix}^{scsGF} \right) \bigcup \left(\sum_{j=1}^{J} p_j^{scsAF} ch_j^{scsAF} \times \sum_{jy=1}^{Y} p_{jy}^{scsAF} l_{jy}^{scsAF} \right) \bigcup \\
& \bigcup \left(\sum_{l=1}^{L} p_l^{scsNF} ch_l^{scsNF} \times \sum_{lz=1}^{L} p_{lz}^{scsNF} l_{lz}^{scsNF} \right) \bigcup \left(\sum_{k=1}^{K} p_k^{sdpsD} ch_k^{sdpsD} \times \sum_{kf=1}^{F} p_{kf}^{sdpsD} l_{kf}^{sdpsD} \right) \bigcup \\
& \bigcup \left(\sum_{m=1}^{M} p_m^{oIS} ch_m^{oIS} \times \sum_{mv=1}^{V} p_{mv}^{oIS} l_{mv}^{oIS} \right) \bigcup \sum_{q=1}^{Q} p_q^{omcs} ch_q^{omcs} \times \sum_{qn=1}^{N} p_{qn}^{omcs} l_{qn}^{omcs} .
\end{aligned}
$$

where p_i^{scsGF} – is the probability of correct reception/transmission by the *i*-th switching node ch_i^{scsGF} ; p_{ix}^{scsGF} – is the probability of correct transmission from the *i*-th switching node ch_i^{scsGF} through the *x*-th channel l_{ix}^{scsGF}; p_j^{scsAF} – is the probability of correct reception/transmission by the j-th switching node ch_j^{scsAF}; p_{jy}^{scsAF} – is the probability of correct transmission from the j-th switching node ch_j^{scsAF} through the y-th channel l_{jy}^{scsAF} ; p_l^{scsNF} – is the probability of correct reception/transmission by the l-th switching node ch_l^{scsNF} ; p_{lz}^{scsNF} – is the probability of correct transmission from the l-th switching node ch_l^{scsNF} through the z-th channel l_{lz}^{scsNF} ; p_k^{sdpsD} – is the probability of correct reception/transmission by the k-th switching node ch_k^{sdpsD}; p_{kf}^{sdpsD} – is the probability of correct transmission from the k-th switching node ch_k^{sdpsD} through the f-th channel l_{kf}^{sdpsD}; p_m^{oIS} – is the probability of correct reception/transmission by the m-th switching node ch_m^{oIS}; p_{mv}^{oIS} – is the probability of correct transmission from the m-th switching node ch_m^{oIS} through the v-th channel l_{mv}^{oIS}; p_q^{omcs} – is the probability of correct reception/transmission by the q-th switching node ch_q^{omcs}; p_{qn}^{omcs} – is the probability of correct transmission from the q-th switching node ch_q^{omcs} through the n-th channel l_{qn}^{omcs} .

2. Mathematical evaluation of message delivery probability using the special purpose system

Considering the possibility of "suppression" (both partial and complete) of confidential communication system channels of the Armed Forces of Ukraine, the modified special purpose system proposes transmitting commands and signals as separate independent components across all channels, including both special confidential communication systems and open networks. Commands are transmitted in parallel. Each network may be subject to attacks of various natures that result in network failure. We calculate the message delivery probability for packets transmitted during parallel operation of three networks (special communication system of the Armed Forces of Ukraine, open Internet network, open mobile communication network), assuming a majority decision-making mechanism at the receiving end that determines transmission correctness when at least two packets transmitted across different networks are identical.

Let the probability of command transmission without distortion and failures for the special communication system be $P_{\text{пр.п.}}^{Q^{SCS}}$, for the second network $P_{\text{пр.п.}}^{Q^{oIS}}$, and for the third network $P_{\text{пр.п.}}^{Q^{omcs}}$, representing packet transmission without failures and losses caused by various classes of attacks.

Without a majority decision-making mechanism at the receiving end, the probability of receiving a packet through at least one network could be calculated as:

$$P_{\text{пр.п.}}^{Q^{ACCS}} = P_{\text{пр.п.}}^{Q^{oIS}} + P_{\text{пр.п.}}^{Q^{oIS}} + P_{\text{пр.п.}}^{Q^{omcs}} = \left(1 - P_{\text{пом}}^{Q^{SCS}}\right) \times \left(1 - P_{\text{пом}}^{Q^{oIS}}\right) \times \left(1 - P_{\text{пом}}^{Q^{omcs}}\right),$$

where $P_{\text{пом}}^{Q^{SCS}}$ – the probability of erroneous command reception in a special communication system (network); $P_{\text{пом}}^{Q^{oIS}}$ – the probability of erroneous reception of the command on the Internet; $P_{\text{пом}}^{Q^{omcs}}$ – probability of erroneous command reception in the mobile network.

This expression represents the probability that not all three networks fail simultaneously.

With a majority decision-making mechanism at the receiving end, calculating the probability of packet reception and correctness confirmation requires a different approach.

Let's consider all possible states of the three networks listed above. All state sets are summarized in Table 1.

The "+" symbol indicates successful packet transmission, while "-" indicates that packets were not delivered or arrived with distortions due to various factors (attacks, physical damage, technical failures, etc.). The first four situations correspond to cases where the majority decision-making mechanism can confirm that 2 out of 3 packets are identical and can be interpreted as correctly transmitted commands.

In other cases, the majority body cannot confirm the identity of the received packets on at least 2 networks. The probabilities of the respective situations are given in the last column of Table 1.

In this case, the probability of receiving identical packets on at least 2 networks, which allows the majority body to operate, will be equal to the sum of the probabilities of the first four situations:

$$P_{\text{пр.п.}}^{Q^{ACCS}} = P_{\text{пр.п.}}^{Q^{SCS}} \times P_{\text{пр.п.}}^{Q^{oIS}} \times P_{\text{пр.п.}}^{Q^{omcs}} + P_{\text{пр.п.}}^{Q^{SCS}} \times P_{\text{пр.п.}}^{Q^{oIS}} \times \left(1 - P_{\text{пр.п.}}^{Q^{omcs}}\right) + P_{\text{пр.п.}}^{Q^{SCS}} \times P_{\text{пр.п.}}^{Q^{omcs}} \times \left(1 - P_{\text{пр.п.}}^{Q^{oIS}}\right) + P_{\text{пр.п.}}^{Q^{oIS}} \times P_{\text{пр.п.}}^{Q^{omcs}} \times \left(1 - P_{\text{пр.п.}}^{Q^{SCS}}\right)$$

However, using a specialized network ensures the detection and correction of any number of errors through decoding algorithms. The trade-off for increased reliability and responsiveness is the additional transmission of redundant (check) symbols, significantly simplifying the execution of electronic countermeasure (ECM) activities by an adversary.

3. Mathematical assessment of message delivery reliability using the special purpose system

Detailed investigation of statistical properties of error sequences in real communication channels [10-12] demonstrates that errors are dependent and exhibit clustering tendencies, indicating correlation between errors. Information passes through communication channels without distortion most of the time, while at specific moments, error concentrations occur in so-called error packets (bursts or groups), where error probability significantly exceeds the average error probability calculated over extended transmission periods. Under such conditions, protection methods optimized for independent error hypotheses prove ineffective when applied to real communication channels. HF radio channels and wired data transmission channels used for control and communication organization in special Armed Forces communication systems are susceptible to significant error clustering with minimal average asymmetry.

Table 1 - **Possible states of the three command transmission networks**

Situation no.	Network status			Probability of implementation
	$P^{Q^{SCS}}_{пом}$	$P^{Q^{oIS}}_{пр.п.}$	$P^{Q^{omcs}}_{пр.п.}$	
1	+	+	+	$P^{Q^{ACCS}}_{пр.п.} = P^{Q^{SCS}}_{пр.п.} \times P^{Q^{oIS}}_{пр.п.} \times P^{Q^{omcs}}_{пр.п.}$
2	+	+	–	$P^{Q^{ACCS}}_{пр.п.} = P^{Q^{SCS}}_{пр.п.} \times P^{Q^{oIS}}_{пр.п.} \times \left(1 - P^{Q^{SCS}}_{пр.п.}\right)$
3	+	–	+	$P^{Q^{ACCS}}_{пр.п.} = P^{Q^{SCS}}_{пр.п.} \times \left(1 - P^{Q^{oIS}}_{пр.п.}\right) \times P^{Q^{omcs}}_{пр.п.}$
4	–	+	+	$P^{Q^{ACCS}}_{пр.п.} = \left(1 - P^{Q^{SCS}}_{пр.п.}\right) \times P^{Q^{oIS}}_{пр.п.} \times P^{Q^{omcs}}_{пр.п.}$
5	+	–	–	$P^{Q^{ACCS}}_{пр.п.} = P^{Q^{SCS}}_{пр.п.} \times \left(1 - P^{Q^{oIS}}_{пр.п.}\right) \times \left(1 - P^{Q^{omcs}}_{пр.п.}\right)$
6	–	+	–	$P^{Q^{ACCS}}_{пр.п.} = \left(1 - P^{Q^{SCS}}_{пр.п.}\right) \times {}^{Q^{oIS}}_{пр.п.} \times \left(1 - P^{Q^{omcs}}_{пр.п.}\right)$
7	–	–	+	$P^{Q^{ACCS}}_{пр.п.} = \left(1 - P^{Q^{SCS}}_{пр.п.}\right) \times \left(1 - P^{Q^{oIS}}_{пр.п.}\right) \times P^{Q^{omcs}}_{пр.п.}$
8	–	–	–	$P^{Q^{ACCS}}_{пр.п.} = \left(1 - P^{Q^{SCS}}_{пр.п.}\right) \times \left(1 - P^{Q^{oIS}}_{пр.п.}\right) \times \left(1 - P^{Q^{omcs}}_{пр.п.}\right)$

Table 2 - **Distribution series of the discrete random length of the interval between the beginnings of error packets** ***Λ***

Λ	0	1	2	…	i	…
$P\{\Lambda = \lambda\}$	P_n	$P_n(1 - P_n)$	$P_n(1 - P_n)^2$	…	$P_n(1 - P_n)^i$	…

Table 3 - **Evaluation of clusters for the GSM-900 network**

Cluster dimension C	Parameters	Sectorality M								
		1			3			6		
3	$P(C)$, %	–	–	–	6,2	21,8	29,5	0,4	6,6	14,5
4	$P(C)$, %	39	49,6	–	2,3	14,7	23,6	0,3	4,3	11,5
7	$P(C)$, %	6,4	25,8	35	0,2	6,4	15,2	0,01	1,7	6,8

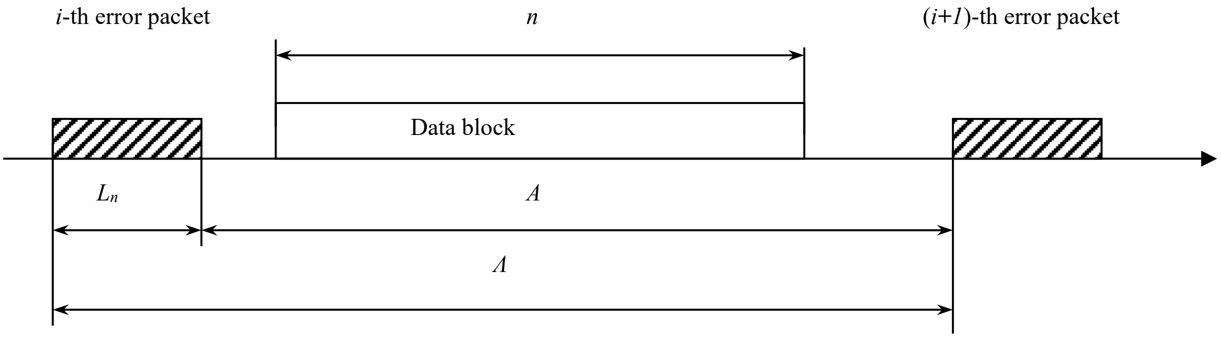


Fig.2. Explanation of the meaning of the random variable *A*

For grouped error distribution, a single parameter (error probability) does not fully characterize the channel; additional parameters reflecting the degree of error clustering in various data transmission channels are necessary.

For calculating reliability indicators of command transmission in special Armed Forces communication systems, we employ the simplified Bennett-Frolich mathematical model, which imposes no restrictions on the distribution law of error packet lengths [10-12]. The simplified Bennett-Frolich model advantages include relatively low computational complexity, few parameters, high accuracy compared to the Gilbert model, and arbitrary selection of error packet length distribution characteristics. The simplified Bennett-Frolich model requires specifying: P_n – probability that a continuous error packet of any length begins at a given position, $P(l)$ – probability of continuous error packet length l occurrence. Then $P_n(l)$ – the probability that a continuous error packet of length l will start from this position is equal to:

$$P_n(l) = P_n \times P(l).$$

Consider the simplified Bennett-Frolich model with non-overlapping error packets and possible adjacency. In this case, within a block length of nn symbols, no more than

$$\lambda' = \left\lfloor \frac{n}{l} \right\rfloor$$

error blocks of length ll can occur.

Then the probability of correct command and signal reception in the special Armed Forces communication system is determined by:

$$P_{np.n.}^{Q^{SCS}} = 1-(1-P_{пом}^{Q^{SCS}})^n - \sum_{\xi=1}^{\lambda'} C_n^{\xi} \cdot P_{пом}^{\xi} \cdot \left(1-P_{пом}^{Q^{SCS}}\right)^{n-\xi} = 1-\sum_{\xi=0}^{\lambda'} C_n^{\xi} \cdot P_{пом}^{\xi} \cdot \left(1-P_{пом}^{Q^{SCS}}\right)^{n-\xi}$$

where x represents the number of error packet combinations and n represents packet length.

For calculating correct command reception probability in Internet networks, we also employ the simplified Bennett-Frolich model. One modification of the Bennett-Frolich model assumes polygeometric distribution of error packet lengths, as examined in works [19].

In studies [19], it has been demonstrated that the lengths of error bursts in most practical channels follow a normal distribution. Consequently, instead of specifying the distribution function of burst lengths $F(l_n)$, it suffices to define the mathematical expectation m_{ln} and standard deviation σ_{ln}. The interval length between the beginnings of consecutive error bursts, denoted by Λ is a discrete random variable (DRV). Let us construct the probability distribution series for the DRV Λ\Lambda and determine its distribution function. The distribution series of DRV Λ is presented in Table 2, where P_n is represents error packet occurrence probability.

The DRV Λ distribution function:

$$F_{\Lambda}(\lambda) = P\{\Lambda < \lambda\} = \sum_{i=0}^{\lambda\text{-}1} P(\lambda) = P_n\left(1+(1-P_n)+(1-P_n)^2+...(1-P_n)^{\lambda\text{-}1}\right) =$$
$$= P_n \times \frac{1-(1-P_n)^{\lambda}}{1-(1-P_n)} = P_n \times \frac{1-(1-P_n)^{\lambda}}{P_n} = 1-(1-P_n)^{\lambda}.$$

Error packet length L_n is also a random variable following normal distribution with parameters m_{ln} and σ_{ln}, potentially ranging from 0 to ∞.

Introducing random variable A, equal to the difference between Λ i Ln. The random variable A is the length of the i-th error-free interval and can take values from 0 to ∞ (Fig. 2).

$$A = \Lambda - L_n.$$

The probability of correct data block transmission of length n bits can be defined as the probability that random variable A takes values greater than or equal to n:

$$P_{np} = \mathrm{P}\{\mathrm{A} \geq \mathrm{n}\} = 1 - \mathrm{P}\{\mathrm{A} < \mathrm{n}\} = 1 - F_A(n),$$

where $F_A(n)$ represents the distribution function of random variable A on the variable n.

The random event B, which consists in the fact that random variable A takes a value less than n, can be represented as a sum of incompatible events:

B_0 is a random event such that $\Lambda < n$ and $0 \leq L_n < 1$;

B_1 is a random event such that $\Lambda < n+1$ and $1 \leq L_n < 2$;

B_2 is a random event such that $\Lambda < n+2$ and $2 \leq L_n < 3$;

…

B_i is a random event such that $\Lambda < n+i$ and $i \leq L_n < i+1$.

The random variables Λ and Ln are independent. Then the probabilities of these events are equal to

$$P(B_0) = P\{(\Lambda < n) \cap (0 \leq L_п < 1)\} = P\{\Lambda < n\} \times P\{0 \leq L_п < 1\};$$
$$P(B_1) = P\{(\Lambda < n+1) \cap (1 \leq L_п < 2)\} = P\{\Lambda < n+1\} \times P\{1 \leq L_п < 2\};$$
$$P(B_2) = P\{(\Lambda < n+2) \cap (2 \leq L_п < 3)\} = P\{\Lambda < n+2\} \times P\{2 \leq L_п < 3\};$$
$$\dots$$
$$P(B_i) = P\{(\Lambda < n+i) \cap (i \leq L_п < i+1)\} = P\{\Lambda < n+i\} \times P\{i \leq L_п < i+1\};$$
$$\dots$$

Since the events B_0, B_1, B_2, …, B_i, … are incompatible, then

$$\mathrm{P}\{\mathrm{A} < \mathrm{n}\} = P(B) = \sum_{i=0}^{\infty} P(B_i) = \sum_{i=0}^{\infty}\left[P\{\Lambda < n+i\} \cdot P\{i \leq L_п < i+1\}\right].$$

The probability $P\{Л<n+i\}$ is a function of the distribution of the the random variables $Л$ on the argument $n+i$

$$P\{\Lambda < n+i\} = F_{\Lambda}(n+i) = 1-(1-P_n)^{n+i}.$$

In order to find the probability that the value of the random variable Ln, distributed according to the normal law with parameters m_{ln} and σ_{ln}, falls in the interval [i, i+1], we use the well-known formula

$$P\{i \le L_{\text{п}} < i+1\} = \Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right),$$

where $\Phi(x)$ is the Laplace function of the argument x.

Substituting (2), (3) into (1), we obtain the distribution function of the random variable A

$$F_A(n) = P\{A<n\} = \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}.$$

Then the formula for calculating the probability of correct transmission of a data block of n bits is

$$P_{пр} = 1-F_A(n) = 1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}.$$

Thus, for an open Internet network with decisive feedback and positive acknowledgement, the probability of correct command reception is determined by the formula:

$$P^{Q^{olS}}_{пр.п.} = 1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\times$$
$$\times\frac{1-\sum\limits_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}^N}{1-\sum\limits_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}},$$

where n represents I-frame length, P_n represents error packet occurrence probability; m_{ln} represents mathematical expectation of error packet length; σ_{ln} – represents standard deviation of error packet length, and N represents maximum number of repetitions determined by:

$$N \ge \left\lceil \frac{\ln\left(1-\frac{P_{необх}\cdot\left(1-P_{I\,вп}\right)}{P_{I\,пр}}\right)}{\ln P_{I\,вп}} \right\rceil,$$

where $P_{необх}$ – required represents required packet delivery probability,

$P_{I\,вп}$ – detect represents packet error detection probability,

$P_{I\,пр}$ – correct represents single-attempt correct packet transmission probability,

$\lceil x \rceil$ – represents the nearest integer greater than or equal to x.

For cellular communication networks, the Okumura-Hata model is used to determine signal and interference power at subscriber terminal receiver inputs for predicting propagation losses. According to this model, signal power at subscriber station $P_{\text{пр}}$ receiver input located at distance R from transmitter equals:

$$P^{Q^{отс}}_{пр.п}(R) = P_{випр}(\Theta)\times L(R),$$

where $P_{\text{випр}}(\Theta)$ represents transmitter radiated power depending on subscriber station direction, assuming subscriber station antenna has circular radiation pattern, and $L(R)$ represents signal propagation losses in urban areas, depending on transmitting and receiving antenna heights, distance between them, carrier frequency, and empirical coefficient.

Signal power at receiver input is inversely proportional to transmitter distance:

$$P^{Q^{отс}}_{пр.п}(R) = \frac{P_{випр}(\Theta)}{B\times R^x},$$

where B represents empirically calculated coefficient depending on transmitting and receiving antenna heights $h_{\text{БС}}$ and carrier frequency, and x represents exponent at R:

$$x = 4{,}49 - 0{,}655\lg(h_{\text{БС}}).$$

Interference power created by six interfering transmitters of the first hexagon equals:

$$P_{n1} = 6\frac{P_{випр}(\Theta)}{B\times(R_3)^x}\times\frac{1}{\left(\sqrt{27}\right)^x}$$

Interference power formula for six interfering transmitters of the second hexagon:

$$P_{n1} = 6\frac{P_{випр}(\Theta)}{B\times(R_3)^x}\times\frac{1}{9^x},$$

Third hexagon interference power:

$$P_{n1} = 6\frac{P_{випр}(\Theta)}{B\times(R_3)^x}\times\frac{1}{(108)^x}.$$

During cellular network operation, interference from base station transmitters operating on coinciding frequencies (adjacent channels) appears, requiring consideration of signal-to-(noise + interference) ratio at receiver input:

$$h_{\sum} = \frac{P_c}{P_ш + P_{npu\sum}}.$$

The probability of failing to meet acceptable signal-to-interference ratio (S/N_I) requirements at reception point $P(C)$ depends on cluster dimensionality. Probability $P(C)$ decreases with increasing cluster dimensionality while simultaneously reducing network frequency efficiency. Different cluster options are evaluated and the optimal one is selected. The results of evaluating different cluster options for the GSM-900 standard are shown in Table 3.

Therefore, for mobile networks, the probability of correct command reception is determined by:

$$P_{np.n}^{Q^{omcs}} = 1 - h_{\sum} = \frac{P_c}{P_ш + P_{npu\sum}}.$$

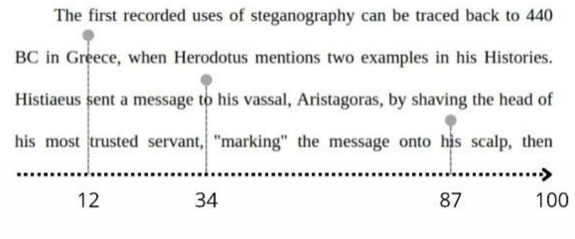
The probability of correct reception in the proposed modified special purpose system equals:

$$P_{np.n.}^{Q^{ACCS}} = P_{np.n.}^{Q^{SCS}} + P_{np.n.}^{Q^{omcs}} + P_{np.n.}^{Q^{oIS}} = \left(1 - \sum_{\xi=0}^{\lambda'} C_n^{\xi} \cdot P_{пом}^{\xi} \cdot \left(1 - P_{пом}^{Q^{SCS}}\right)^{n-\xi}\right) \times \left(1 - h_{\sum} = \frac{P_c}{P_ш + P_{npш\sum}}\right) \times$$

$$\left(\begin{array}{l} 1 - \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\} \times \\ \times \dfrac{1 - \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1 - \frac{1}{2^r}\cdot\left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}^N}{1 - \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1 - \frac{1}{2^r}\cdot\left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}} \end{array}\right).$$

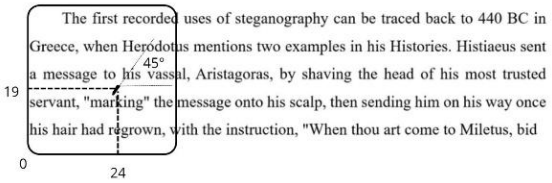
4. A model for ensuring authenticity using steganographic methods

To address authenticity concerns, this study proposes utilizing printed textual documents, both official and commercial, as containers by incorporating special characters disguised as residual printing artifacts. Information encoding employs the coordinate positioning of symbols (Fig. 2) and angular orientation for vector-directed elements (Fig. 3).



The first recorded uses of steganography can be traced back to 440
BC in Greece, when Herodotus mentions two examples in his Histories.
Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of
his most trusted servant, "marking" the message onto his scalp, then

Fig. 2. Positioning of symbols

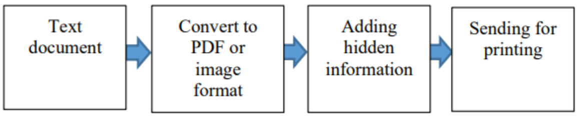


The first recorded uses of steganography can be traced back to 440 BC in
Greece, when Herodotus mentions two examples in his Histories. Histiaeus sent
a message to his vassal, Aristagoras, by shaving the head of his most trusted
servant, "marking" the message onto his scalp, then sending him on his way once
his hair had regrown, with the instruction, "When thou art come to Miletus, bid

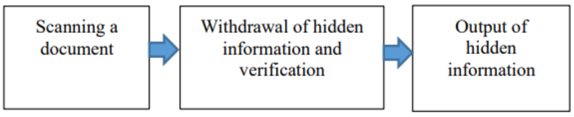
Fig. 3. Vector-Directed Artifact Sample

.

For embedding information into the container, two methods are employed: the first involves utilizing a defined algorithm or a combination of algorithms, while the second entails hashing textual information and storing the relationship between the hash values.

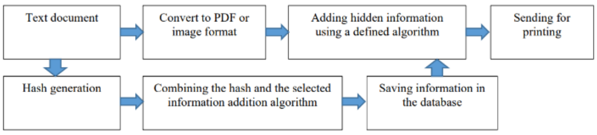


Schema 1. Information Embedding Using the First Method



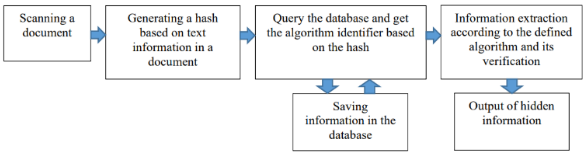
Scanning a document
Withdrawal of hidden information and verification
Output of hidden information

Schema 2. Information Extraction Using the First Method



Text document
Convert to PDF or image format
Adding hidden information using a defined algorithm
Sending for printing
Hash generation
Combining the hash and the selected information addition algorithm
Saving information in the database

Schema 3. Information Addition Using the Second Method



Scanning a document
Generating a hash based on text information in a document
Query the database and get the algorithm identifier based on the hash
Information extraction according to the defined algorithm and its verification
Saving information in the database
Output of hidden information

Schema 4. Information Extraction Using the Second Method

The first method offers advantages in terms of simplicity of implementation and standardization. The second method requires the utilization of a database for information storage and potentially additional security measures for its protection. However, if documents are already stored in such a manner, its implementation may be preferable to the first method, as it is theoretically more resistant to container-based attacks.

5. Conclusions

Analysis of existing special purpose system models in security structures does not enable signal/command transmission with required reliability levels under contemporary countermeasures (suppression, partial or complete destruction) against combat control systems. Hybrid warfare conduct requires new approaches and utilization of all possible channels for delivering combat orders.

The proposed structural framework for the prospective Armed Forces of Ukraine combat control system utilizes both special communication equipment currently in service and open commercial cyberspace systems. The transmission methodology proposes decomposing each message into separate components transmitted across all channels. Open channels employ digital steganography and/or lossy cryptography methods. Interception of individual components in each channel prevents adversaries from obtaining original text. The final recipient uses majority selection across all channels and message components to receive combat commands/signals. This approach enables task completion within prescribed timeframes under economic crisis conditions by utilizing cyberspace infrastructure (synthesis of modern computer systems and network technologies, Internet technologies, and mobile communication technologies).

The mathematical framework for assessing reliability and probability of corresponding command/signal delivery enables modeling the proposed system while accounting for various external and internal interferences in special purpose systems. Future research directions include developing mechanisms for component decomposition and concealment during open channel transmission.

The steganographic authentication model employing printed documents with embedded printing artifacts offers a practical solution for message verification in hybrid warfare. The dual-method approach provides operational flexibility through algorithmic simplicity or enhanced database-secured hash verification, enabling seamless integration into multi-channel communication systems while maintaining operational security in contested environments.

References

1. Pro rishennja Radi nacional'noї bezpeki i oboroni Ukraïni vid 20 travnja 2016 roku “Pro Strategichnij oboronnij bjuleten' Ukraïni” (2016), http://www.president.gov.ua/documents/2402016-20137.
2. Kirpichnikov J., Fedoriienko V., Golovchenko O., Androshhuk O. Analiz ramkovyh arhitektur pobudovy informa-cijnyh system NATO ta vyznachennja osoblyvostej arhitektury S4ISR, http://znp-cvsd.nuou.org.ua/article/view/125555.
3. Fedoriienko V. Analiz special'nogo programnogo zabezpechennja GIS informacijnoi' infrastruktury Ministerstva oboro-ny Ukrai'ny, http://znp-cvsd.nuou.org.ua/article/view/177986.
4. Bila kniga – 2018. Zbrojni Sili Ukraïni (2018), http://www.mil.gov.ua/content/files/whitebook/WB-2018.pdf.
5. Building C4ISR Capabilities in and for the Gulf, https://www.files.ethz.ch/isn/164095/227_Thiele.pdf.
6. C4ISR for Future Naval Strike Groups (2006), http://nap.edu/11605.
7. Doktryna informacijnoi' bezpeky Ukrai'ny, zatverdzheno Ukazom Prezydenta Ukrai'ny vid 25.02.2017 № 47/2017 (2017), http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.
8. Grishhuk R. V., Danik Ju. G. (2016), Osnovi kibernetichnoї bezpeki: Monografija, Zhitomir: ZhNAEU.
9. Leonenko G., Judin O. (2013), Problemy zabezpechennja informacijnoi' bezpeky system krytychno vazhlyvoi' infrastruktury Ukrai'ny, *Information Technology and Security*, № 1(3), p. 44 – 48.
10. Yevseiev S., Tomashevsky B., Korol O. (2012), Pryncypy pobudovy pidsysem kryptografichnogo zahystu informacii' v ASUV operatyvnogo grupuvannja ob’jednanyh Syl shvydkogo reaguvannja, *Zbirnyk naukovyh prac' akademii' vijs'kovo-mors'kyh syl im. P.S. Nahimova*, № 2 (10), p. 68 – 77.
11. Yevseiev S., Tomashevsky B., Korol O., Nosyk O. (2012), Doslidzhennja bojovyh mozhlyvostej zasobiv povitrjanogo napadu protyvnyka, *Vijs'kovo-tehnichnyj zbirnyk*, № 1 (6). p. 127 – 135.
12. Zontou E. Unveiling the Evolution of Mobile Networks: From 1G to 7G, https://www.researchgate.net/publication/390980121.
13. Kumar V., Kaur K., Mahajan J. How 6G and 7G Will Shape the Future of Wireless Connectivity, https://ijrpr.com/uploads/V6ISSUE4/IJRPR42302.pdf.
14. IDC “The Digitization of the World – From Edge to Core”, https://www.seagate.com/gb/en/our-story/data-age-2025/.
15. Report on Post-Quantum Cryptography, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
16. A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks, https://www.sciencedirect.com/science/article/pii/S2542660520300159.
17. Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization, https://www.sciencedirect.com/science/article/abs/pii/S2214212618301212.
18. Guide to LTE, https://Security,csrc.nist.gov/publications/drafts/80 187/sp800_187_draft.pdf.
19. Skljar B. (2003), Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie. Izd. 2-e, ispr. /Per. s angl. M.: Izdatel'skij dom “Vil'jams”.
20. Reinsel D., Gantz J., Rydning J. (2018), The Digitization of the World, from Edge to Core, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

Received (Надійшла) 24.04.2025
Accepted for publication (Прийнята до друку) 15.05.2025

Відомості про авторів/ About the Authors

Томашевський Богдан Паїсійович – кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки, Тернопільський національний технічний університет ім. І. Пулюя, Тернопіль, Україна;

Bogdan Tomashevsky – PhD, Associate Professor, Associate Professor Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine;

e-mail: bogdan_tomashevsky@tntu.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-1934-4773;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57208026171.

Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Professor, Head of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: Serhii.Yevseiev@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-1647-6444;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190440690.

Сітченко Олександр Анатолійович – аспірант кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Oleksandr Sitchenko – PhD student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: oleksandr.sitchenko@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0007-8756-398X;

Корольов Роман Володимирович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Roman Korolov – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: korolevrv01@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-7948-5914;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57204143490.

МОДЕЛЬ КОМБІНОВАНОЇ СИСТЕМИ БОЙОВОГО КЕРУВАННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Б. П. Томашевський, С. П. Євсеєв, О. А. Сітченко, Р. В. Корольов

Анотація. Актуальність. Стрімкий розвиток обчислювальних технологій, мобільних та інтернет-технологій, цифрової економіки, гібридності та синергії, а також розвиток постквантової криптографії (зокрема, поява повномасштабних квантових комп'ютерів) висувають дедалі жорсткіші вимоги до принципів проектування спеціалізованих механізмів безпеки в сучасних системах спеціального призначення. Ведення гібридної війни вимагає модифікації не лише архітектурних принципів систем спеціального зв'язку (СКЗ) та систем передачі бойових команд і сигналів оперативним підрозділам, але й вимагає розробки принципово нових підходів до формування та передачі команд з використанням як спеціалізованого обладнання СКЗ, так і відкритих комерційних систем на основі інтернет-технологій та сучасних протоколів бездротової передачі даних. **Мета статті**. В статті автори пропонують структурну схему перспективної системи бойового управління Збройними Силами України, яка використовує як систему спеціального зв'язку, що перебуває на озброєнні, так і відкриті комерційні системи кіберпростору, при цьому кожне повідомлення розділяється на окремі компоненти, що передаються по всіх каналах, з використанням відкритих каналів методів цифрової стеганографії та/або криптографії з втратами. **Отримані результати.** Водночас перехоплення окремих компонентів у кожному каналі не дозволить противнику отримати вихідний текст. Кінцевий одержувач отримує бойову команду/сигнал на основі мажоритарного відбору з усіх каналів, для всіх частин повідомлення. Такий підхід дозволяє в умовах економічної кризи забезпечити своєчасне виконання завдань в умовах сучасних контрзаходів (придушення, часткове або повне знищення) системи бойового управління шляхом використання інфраструктури кіберпростору (синтез сучасних технологій комп'ютерних систем та мереж, інтернет-технологій та технологій мобільного зв'язку). **Висновки.** Представлена математична складова оцінки надійності та ймовірності доставки відповідних команд/сигналів дозволяє моделювати запропоновану модель з урахуванням різних втручань у систему спеціального призначення, як зовнішніх, так і внутрішніх.

Ключові слова: модифікована система спеціального призначення, кіберпростір, квантовий період, стеганографія.