Model of the System for Special Purpose of Critical Infrastructure Objects

Mikolaj Karpinski [1], Bogdan Tomashevsky[2], Natalia Zahorodna[3], Serhii Yevseiev[4], Stanislaw Rajba [5], Oleksandr Milov[6]

[1,3,5] *University of Bielsko-Biala, Department of Computer Science and Automatics, Willowa Str. 2, Bielsko-Biala, 43-309, Poland*
[2] *Ternopil Ivan Puluj National Technical University, Department of Cyber Security, Ruska str., 56, Ternopil, 46001, Ukraine*
[4,6] *Simon Kuznets Kharkiv National University of Economics, Cybersecurity and Information Systems Department, ave. Science, 9-A, Kharkiv, 61166, Ukraine*

Abstract

The rapid development of computing, mobile and Internet technologies, the digital economy, on the one hand, hybridity and synergy, the development of post-quantum cryptography (the emergence of a full-scale quantum computer), on the other, put forward more stringent requirements for the principles of building special security mechanisms in modern special-purpose systems. Targeted attacks in cyberspace also require a change not only in the principles of building a special communication system for critical infrastructure objects (SCS CIO), the system for communicating commands / control signals to the CIO elements, as well as the creation of fundamentally new approaches to the formation and transmission of commands for their use not only of the SCS equipment, as well as open modern commercial systems based on Internet technologies. This approach allows, in the context of the economic crisis, to ensure the delivery of the signal within a certain time frame in the conditions of modern hybrid cyber threats to the control system through the use of cyberspace infrastructure (synthesis of modern technologies of computer systems and networks, Internet technologies and technologies of mobile communication). The proposed mathematical component of the assessment of the reliability and probability of delivering the corresponding commands / signals allows the proposed model to be used to simulate various interventions into a special-purpose system, both external and internal.

Keywords

modified special purpose system, critical infrastructure, cyberspace, quantum period.

1. Introduction

The modern development of computer technology, the rapid development of cyberspace technologies, the emergence of new hybrid threats and their modification put forward more stringent requirements for special-purpose systems. This is due to the need to bring commands / control signals with a high degree of reliability, safety and efficiency to the elements of the CIO infrastructure in the post-quantum period (the emergence of a full-scale quantum computer). This approach requires not only the formation of

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: mkarpinski@ath.bielsko.pl (A. 1); bogdan_tomashevsky@tntu.edu.ua (A. 2); zagorodna.n@gmail.com (A. 3); Serhii.Yevseiev@hneu.net (A. 4); srajba@ath.bielsko.pl (A. 5); Oleksandr.Milov@hneu.net (A. 6)
ORCID: 0000-0002-8846-332X (A. 1); 0000-0002-1934-4773 (A. 2); 0000-0003-1647-6444 (A. 4); 0000-0001-9291-8879 (A. 5); 0000-0001-6135-2120 (A. 6);

programs for the standardization of the information infrastructure of the CIO elements based on international standards and Green Paper approaches, but also the ability to counter modern threats with signs of hybridity and synergy.

1.1. Analysis of recent research and publications

[1-8] determines the need to create a special-purpose system for critical infrastructure facilities, which makes it possible to form a control system in the conditions of post-quantum cryptography, the growing demands of cyber terrorists, targeted cyberattacks on communication channels and elements of the CIO. In [7], it is predicted that by 2025, 2.8 billion subscribers will use the 5G network. By the same year, the share of fixed wireless access networks in global traffic will increase to 25%, reaching 160,000,000 connections. According to research [9,12], today more than 5,000,000,000 consumers interact with data every day − by 2025 this number will be 6,000,000,000, or 75% of the world's population. In 2025, every connected person will have at least one data access every 18 seconds. Many of these interactions are driven by the billions of IoT devices connected around the world, which are expected to generate over 90 ZB (10^{21} bytes) of data in 2025. This indicates the possibility of considering the use of these systems as possible channels of a modified special-purpose system, subject to additional information transformation. However, in [2-5,14], US experts note the possibility of breaking symmetric and asymmetric cryptosystems that provide security in cyberspace as a combination of Internet technologies, computer systems and networks, as well as LTE (Long-Term Evolution − long-term development) technologies in the context of the emergence full-scale quantum computer (post-quantum period).

1.2. The purpose and objectives of the study

The aim of the research is to develop a model of a promising special-purpose system for critical infrastructure facilities.

To achieve the goal of the reserch, it is necessary to solve the following tasks:

− development of a mathematical model of a promising special-purpose system CIO;

− mathematical assessment of the probability of delivering a message using a special-purpose system CIO;

− mathematical assessment of the reliability of the proof of the message using the special-purpose system CIO.

2. Development of a mathematical model of a promising special-purpose system.

To ensure the safety, reliability and efficiency of the transmission of commands and / or control signals, a national system of confidential communication is used.

The national confidential communication system is a set of special dual-use communication systems (networks) that, using cryptographic and / or technical means, ensure the exchange of confidential information in the interests of state authorities and local governments, create appropriate conditions for their interaction in peacetime and in in the case of the introduction of a special and martial law [1, 6,13].

A special communication system (network) is a communication system (network) intended for the exchange of information under limited access. A special dual-purpose communication system (network) is a special communication system (network) designed to provide communication in the interests of state authorities and local authorities, using part of its resource to provide services to other consumers. The subjects of the National System of Confidential Communication are state authorities and local self-government bodies, legal entities and individuals who take part in the creation, functioning, development and use of this system. Management of the National System of Confidential Communications, its functioning, development, use and protection of information are provided by a specially authorized central executive body in the field of confidential communications in accordance with the legislation. Centralized systems of information protection and operational and technical management are state-owned and are not subject to privatization. The owners of other components of the National System of Confidential Communications may be subjects of economic activity, regardless of the form of ownership. The main feature of such systems is its hierarchical structure and transmission method based on forward error correction. This approach

requires the transmission of additional ("unnecessary" − checking) characters, greatly simplifies the detection-suppression and / or complete blocking of these communication channels for the adversary[15,16].

However, the rapid development of computing resources for both Internet and mobile technologies LTE (Long-Term Evolution) allows the use, given the "steganographic" properties of these communication channels. The "steganographic" property is understood as the possibility of hiding from the attacker the fact, place, time and content of information transmitted by breaking the commands and / or control signals of the OCI into separate blocks (packets). This approach allows the use of open communication channels with a commercial method of delivering information to the recipient − the decisive feedback. In addition, the use of this approach does not require significant economic and human resources. Consider the model of a modified CIO control system on the example of the Armed Forces of Ukraine. In the system that is proposed to be used as a projects of the National Confidential Communication System: special communication systems (networks) as well as systems of open public Internet systems and mobile communication systems based on “G” technologies. In this system, the switching nodes are denoted by: 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), $l \in \overline{1,\dots L}$, special dual-purpose system ch_k^{sdpsD} (special dual-use system), $k \in \overline{1,\dots K}$, open Internet system ch_m^{oIS} $m \in \overline{1,\dots M}$, open mobile communication system ch_q^{omcs} (open mobile communication system) $q \in \overline{1,\dots Q}$. Communication channels are 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 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} ,, $n \in \overline{1,\dots N}$.

Thus, the overall system of the proposed special purpose control system CIO will be a set of individual components of the intermediate switching nodes and channels, and the total probability of receiving a command and / or signal is determined by the formula:

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

where:

p_i^{scsGF} − the probability of correct reception / transmission of the i-th switching node ch_i^{scsGF} ;

p_{ix}^{scsGF} − 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} − the probability of correct reception / transmission of the j-th switching node ch_j^{scsAF} ;

p_{jy}^{scsAF} − 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} - the probability of correct reception / transmission of the l-th switching node ch_l^{scsNF} ;

p_{lz}^{scsNF} - 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} − the probability of correct reception / transmission of the k-th switching node ch_k^{sdpsD} ;

p_{kf}^{sdpsD} − 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} - the probability of correct reception / transmission of the m-th switching node ch_m^{oIS} ;

p_{mv}^{oIS} - 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} - the probability of correct reception / transmission of the q-th switching node ch_q^{omcs};

p_{qn}^{omcs} - the probability of correct transmission from the q-th switching node ch_q^{omcs} through the n-th channel l_{qn}^{omcs}.

3. Mathematical assessment of the probability of delivering a message using a special-purpose control system for the OQI

Taking into account the possibility of modern cyber threats, the computing capabilities of cyber terrorists in the special-purpose control system of the CIO, it is proposed to transmit commands and / or control signals by separate independent units through all channels, both a special confidential communication system and over open networks. Commands are transmitted in parallel. Each of the networks can be subject to attacks of a different nature, which lead to the failure of the corresponding network. We calculate the probability of delivery of a message that is transmitted (hereinafter, a packet), with the parallel operation of three networks (a special communication system (network) of the aircraft, an open Internet network, an open mobile network), provided that there is a majority body on the receiving side that makes decisions and the correctness of information transmission in the case of identity of at least two packets.

Let the probability of command transmission without distortion and failure for a special system (network) of communication – $P_{cr}^{Q^{SCS}}$, second network – $P_{cr}^{Q^{oIS}}$, third network – $P_{cr}^{Q^{omcs}}$, ie packet transmission without failures and losses, which can be caused by attacks of different classes. If there was no majority body on the host side, the probability of receiving a package on at least one of the networks could be calculated as follows:

$$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{oIS}} + P_{cr}^{Q^{oIS}} + P_{cr}^{Q^{omcs}} = \\ = \left(1 - P_{err}^{Q^{SCS}}\right) \times \left(1 - P_{err}^{Q^{oIS}}\right) \times \left(1 - P_{err}^{Q^{omcs}}\right),$$

where

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

This expression can be interpreted as the value of the probability that all three networks will not fail simultaneously.

If there is a majority body on the receiving party to the calculation of the probability of receipt and confirmation of the correctness of the received package must be approached in a slightly different way.

Consider all possible states of the three listed networks. All sets of states are summarized in table. 1.

Table 1

Possible states of the three command transmission networks

№ situations	Network status			Probability of implementation
	$P_{err}^{Q^{SCS}}$	$P_{err}^{Q^{oIS}}$	$P_{err}^{Q^{omcs}}$	
1	+	+	+	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{oIS}} \times P_{cr}^{Q^{omcs}}$
2	+	+	-	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{oIS}} \times \left(1 - P_{cr}^{Q^{SCS}}\right)$
3	+	-	+	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times P_{cr}^{Q^{omcs}}$
4	-	+	+	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times P_{cr}^{Q^{oIS}} \times P_{cr}^{Q^{omcs}}$
5	+	-	-	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times \left(1 - P_{cr}^{Q^{omcs}}\right)$
6	-	+	-	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times P_{cr}^{Q^{oIS}} \times \left(1 - P_{cr}^{Q^{omcs}}\right)$
7	-	-	+	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times P_{cr}^{Q^{omcs}}$

The "+" sign indicates that the packet was transmitted successfully, and the "-" sign indicates that due to various reasons (attacks, physical damage, technical failures, etc.), the packets were not delivered, or the packet came with distortions. The first four situations correspond to cases where the majority body can confirm that 2 of the 3 packets are identical, and can be interpreted as a correctly transmitted command. In other cases, the majority body cannot confirm the identity of the received packets on at least 2 networks. The probabilities of realization of the corresponding situations are given in the last column of table. 1.

Then the probability of receiving identical packages on at least 2 networks, which allows the majority body to work, will be equal to the sum of the probabilities of the first four situations:

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

However, when using a special network, it is possible to detect and correct any number of errors based on decoding algorithms. The payment for reliability and efficiency is the additional transmission of redundant (check) characters, which greatly simplifies the execution of a DOS0 attack by a cyber attacker.

4. Mathematical assessment of the control signal reliability using a special-purpose system.

A detailed study of the statistical properties of error sequences in real communication channels [10, 11] showed that errors are dependent and tend to group (package), ie there is a certain relationship between them − correlation. Most of the time the information passes through communication channels without distortion, and at certain points in time there are condensations of errors, so-called packets (packs, groups) of errors, within which the error probability is much higher than the average error probability calculated for a significant transmission time. In such conditions, the protection methods that are optimal for the hypothesis of independent errors are ineffective when used in real communication channels. HF radio channels and wired data transmission channels used for the organization of control and communication in a special system (network) of communication of the Armed Forces, prone to a significant grouping of errors with a slight mean asymmetry. Then, with the group nature of the error distribution, one parameter (error probability) does not fully characterize the channel, additional parameters are needed that reflect the degree of error grouping in different data transmission channels.

To calculate the reliability of command transmission in a special system (network) of communication of the Armed Forces, we use a simplified mathematical model of Bennett-Freulich, which does not impose restrictions on the type of law of distribution of error packet lengths [10, 11]. The advantages of the simplified Bennett – Freulich model include relatively low computational complexity, a small number of parameters, high accuracy compared to the Gilbert model, and the possibility of arbitrary choice of the nature of the distribution of error packet lengths. To set a simplified Bennett – Freulich model, it suffices to set the probability P_n – the probability that from this position will begin a continuous package of errors of any length and distribution, $P(l)$ − the probability of a continuous package of length l. Then $P_n(l)$ − the probability that from this position will start a continuous packet of errors of length l is equal to:

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

Consider a simplified Bennet-Freulich model with disparate bundles of errors and their possible adjacency. In this case, no more than n characters can occur on a block length

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

blocks of length errors l.

Then the probability of correct receiving of commands and / or signals in a special communication system (network) of the Armed Forces is determined by the formula:

$$P_{cr}^{Q^{SCS}} = 1-(1-P_{err}^{Q^{SCS}})^n - \sum_{\xi=1}^{\lambda'} C_n^{\xi} \cdot P_{err}^{\xi} \cdot \left(1-P_{err}^{Q^{SCS}}\right)^{n-\xi} =$$

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

where ξ − number of packet combinations, n − packet length.

To calculate the probability of correct reception of commands on the Internet, we also use a simplified Bennet-Freulich model. One of the modifications of the Bennett-Freulich model, which provides a polygeometric distribution of the lengths of error packets considered in[10, 11].

In [11] it was shown that the lengths of error packets in most real channels are distributed according to the normal law. Thus, instead of the packet length distribution function F (ln), it is sufficient to specify the mathematical expectation mln and the standard deviation σln. The length of the interval between the beginnings of neighboring error packets Λ is a discrete random variable (DRV). We construct a series of DRV distributions and find the DVV distribution function Λ. The range of distribution of DRV Λ is shown in table. 2.

Table 2

A series of distributions of a discrete random length of the interval between the start of error bursts Λ

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

where P_b is the probability of an error packet.

DRV distribution function Λ

$$F_{\Lambda}(\lambda) = P\{\Lambda < \lambda\} = \sum_{i=0}^{\lambda\text{-}1} P(\lambda) =$$

$$= P_b\left(1+(1-P_b)+(1-P_b)^2+...(1-P_b)^{\lambda\text{-}1}\right) =$$

$$= P_b \times \frac{1-(1-P_b)^{\lambda}}{1-(1-P_b)} = P_n \times \frac{1-(1-P_b)^{\lambda}}{P_b} = 1-(1-P_b)^{\lambda}.$$

The error burst length L_n is also a random variable. It is distributed according to the normal distribution law with the parameters m_{ln} and σ_{ln}, and in the general case can take values from 0 to ∞.

Let's introduce into consideration a random variable A equal to the difference between Λ and L_n

$$A = \Lambda - L_n.$$

Random variable A can take values from 0 to ∞. A is the length of the i-th error-free interval (Fig. 1).

The probability of correct transmission of an n-bit data block can be defined as the probability of a random event, random variable A takes on a value greater than or equal to n, that is

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

where $F_A(n)$ is the distribution function of the random variable A from the argument n.

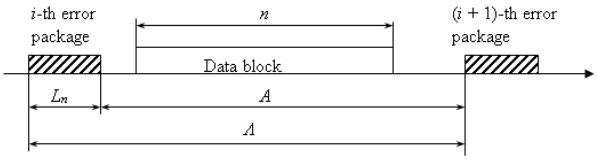

Figure 1: Explanation of the meaning of the random variable A

A random event B, which is that random value A will take a value less than n, can be represented as the sum of incompatible events:

B_0 − a random event, which is that Λ <n and 0≤L_n <1;

B_1 − a random event, which is that Λ <n + 1 and 1≤ L_n <2;

B_2 − a random event, which is that Λ <n + 2 and 2≤ L_n <3;

…

V_i − a random event, which is that Λ <n + i and i≤L_n <i + 1.

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

$$P(B_0) = P\{(\Lambda < n) \bigcap (0 \leq L_{\mathrm{n}} < 1)\} =$$
$$= P\{\Lambda < n\} \times P\{0 \leq L_{\mathrm{n}} < 1\};$$
$$P(B_1) = P\{(\Lambda < n+1) \bigcap (1 \leq L_{\mathrm{n}} < 2)\} =$$
$$= P\{\Lambda < n+1\} \times P\{1 \leq L_{\mathrm{n}} < 2\};$$
$$P(B_2) = P\{(\Lambda < n+2) \bigcap (2 \leq L_{\mathrm{n}} < 3)\} =$$
$$= P\{\Lambda < n+2\} \times P\{2 \leq L_{\mathrm{n}} < 3\};$$

…

$$P(B_i) = P\{(\Lambda < n+i) \bigcap (i \leq L_{\mathrm{n}} < i+1)\} =$$
$$= P\{\Lambda < n+i\} \times P\{i \leq L_{\mathrm{n}} < i+1\};$$

…

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

$$\mathrm{P}\{\mathrm{A} < \mathrm{n}\} = P(B) = \sum_{i=0}^{\infty} P(B_i) =$$

$$= \sum_{i=0}^{\infty} \left[P\{\Lambda < n+i\} \cdot P\{i \leq L_{\mathrm{n}} < i+1\}\right].$$

The probability P{Λ <n + i} is nothing but the distribution function random variables Λ from the argument n + i

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

In order to find the probability that the value of random variables L_n, distributed by the normal law with the parameters m_{Ln} and σ_{Ln}, falls in the interval $[i, i + 1)$, we use the known formula

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

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

Substituting (2), (3) into (1), we obtain the distribution function BB BB

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

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

where n – length of i-th frame, P_n − probability of burst errors; m_{Ln} − mathematical expectation of packet length in errors; σ_{Ln} -standard deviation of length packet of errors, N is the maximum number of repetitions determined by the formula, which is determined by by the formula:

$$N \ge \left\lceil \frac{\ln\left(1-\frac{P_{nec}\cdot(1-P_{I\,ae})}{P_{I\,ct}}\right)}{\ln P_{I\,ae}} \right\rceil,$$

where

P_{nec} − necessary probability delivery packagein;

P_{Iae} − the probability of an error in the package;

P_{Ict} − probability right packet transmission with one attempts;

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

In cellular networks for determination of signal strength and interference at the input of the receiver of the subscriber terminal for prediction of losses when signal propagation is used model Okamura-Cottage. In accordance with this model, the signal power at the input of the receiver P_{ave} subscriber station, which is at a distance R from the transmitter,is equal to

$$P_{cr}^{Q^{omcs}}(R) = P_{rad}(\Theta)\times L(R),$$

where $P_{rad}(\Theta)$ − which emits the power of the transmitter depending on the direction to the subscriber station; at this is expectedthat the antenna of the subscriber station has a pie chart; $L(R)$ − losses (size, reverse attenuation) signal at distribution in urban areas,, depends from altitude, antennas which transmit and accept, distance between them,, carrier frequencies, empirical coefficient.

Power signal on during receiver back proportional distance to transmitter:

$$P_{cr}^{Q^{omcs}}(R) = \frac{P_{rad}(\Theta)}{B\times R^x},$$

where B − coefficient, calculated empirically and depends from altitude, transmitting and reception antennas -h_{BS}, carrier frequencies; x -indicator degree at R:

$$x = 4.49\text{-}0.655\lg(h_{BS}).$$

Power interference obstacles,, created six interfering transmitters the first hexagon,, is equal to

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

$$\mathrm{F_A(n)} = \mathrm{P}\{\mathrm{A} < n\} =$$

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

Then the formula for calculating the probability of correct transmission of a data block of length n bits takes the form

$$P_{cor} = 1-F_A(n) = 1-$$

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

Thus, for an open Internet with crucial feedback and a positive receipt, the probability of receiving the correct commands is determined by the formula:

Formula power interference obstacles,, created six interfering transmitters another hexagon:

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

the third hexagon:

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

At work in cellular network appear interference from transmitters base stationsthat work on matching frequencies (in adjacent channels), and in results on during receiver necessary consider relation signal/ (noise + interference obstacle):

$$h_{\sum} = \frac{P_s}{P_{noise} + P_{obs\sum}}$$

The probability of non-compliance with the requirements for permissible relation signal/obstacle (S/OBS) in point reception P(C) depends from dimensionality cluster. Probability *P(C)* decreases with growth dimensionality cluster. At this simultaneously falls frequency efficiency network. Evaluated different options clusters and absorbs optimal. Results evaluation different options clusters for standard GSM-900 bent in table. 2.

Table 3

Evaluation of clusters for the GSM-900 network

Dimensionality cluster 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

Thus, for a mobile network based on LTE technologies, the probability of correct command reception is determined by the formula:

$$P_{cr.}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} + P_{cr}^{Q^{omcs}} + P_{cr}^{Q^{oIS}} = \left(1-\sum_{\xi=0}^{\lambda'} C_n^{\xi}\cdot P_{no.M}^{\xi}\cdot\left(1-P_{obs}^{Q^{SCS}}\right)^{n-\xi}\right)\times\left(1-h_{\sum} = \frac{P_s}{P_{noise}+P_{obs\sum}}\right)\times$$

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

$$P_{cr}^{Q^{omcs}} = 1-h_{\sum} = \frac{P_s}{P_{noise}+P_{obs\sum}}.$$

Then the probability of correct reception in the proposed modified special-purpose system is equal to:

5. Conclusions

1. The analysis of the existing special-purpose model in the control systems of critical infrastructure facilities does not allow the transmission of control signals / commands to the elements of the AQI infrastructure with the required level of reliability in the context of modern targeted cyber threats requires new approaches and the use of all possible channels for communicating combat orders.

2. The proposed model of a promising special-purpose system for managing objects of OKI uses both a system of special communication equipment and open commercial systems of cyberspace. When transmitting, it is proposed that each message is split into separate components,

which are transmitted over all channels. In open channels, it is proposed to use digital steganography and / or unprofitable cryptography methods. Interception in each channel of individual components will not allow the enemy to get the original text. The final recipient (an element of the OCI infrastructure), on the basis of majority choice from all channels in all parts of the message, receives a command / control signal. This approach allows, in the context of the economic crisis, to ensure the fulfillment of the assigned tasks on time,

3. The mathematical component of assessing the reliability and probability of delivering the corresponding commands / signals allows modeling the proposed model taking into account various interventions into the special-purpose system of critical infrastructure objects, both external and internal. A promising area of further research is the formation of mechanisms for breaking into parts and concealment during transmission over open channels.

6. References

[1] Hrishchuk R. V., and Danyk Yu. G. Fundamentals of cyber security: Monograph (ed. Dannik Yu. G.). Zhytomyr: ZhNAEU, 2016.

[2] Lily Chen et. al. Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal Report 8105. National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 15pp. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[3] Ankur Lohachab, Anu Lohachab, Ajay Jangra. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, Vol. 9, March 2020, 100174. https://doi.org/10.1016/j.iot.2020.100174.

[4] Kyrylo Petrenko, Atefeh Mashatan, Farid Shirazi. Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications, Volume 46, 2019, Pages 151-163. https://doi.org/10.1016/j.jisa.2019.03.007.

[5] Jeffrey Cichonski, Joshua M. Franklin, Michael Bartock. Guide to LTE Security. NIST Special Publication 800-187. National Institute of Standards and Technology, December 2017. 49pp. https://doi.org/10.6028/NIST.SP.800-187.

[6] G. P. Leonenko, and A. Yu. Yudin, “Problems of ensuring information security of systems of critical information infrastructure of Ukraine”, Information Technology and Security, № 1 (3), s. 44 − 48. 2013.

[7] Ericsson Mobility Report: 5G is growing faster than forecasted. https://softline.ua/ua/news/ericsson-mobility-report-5g-zrostaie-shvydshe-za-prohnozy.html

[8] Experts predict "the onset of smart attachments". https://www.ukrinform.ua/rubric-technology/2444363-eksperti-prognozuut-nastup-smartpristroiv.html

[9] IDC "The Digitization of the World − From Edge to Core". https://www.seagate.com/gb/en/our-story/data-age-2025/

[10] Sklar Bernard. Digital communication. Fundamentals and Applications. Prentice Hall, 2012. 954pp.

[11] Korchenko, A., Breslavskyi, V., Yevseiev, S., Sievierinov, O., Tkachuk, S.

[12] Development of a Method for Constructing Linguistic Standards for Multi-Criteria Assessment of Honeypot Efficiency.Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2021, 1(2(109)), pp. 14–23

[13] Androshchuk, A., Yevseiev, S., Melenchuk, V., Lemeshko, O., Lemeshko, V. Improvement of project risk assessment methods of implementation of automated information components of non-commercial organizational and technical systems. EUREKA, Physics and Engineeringthis link is disabled, 2020, 2020(1), pp. 48–55

[14] Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.

[15] Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method

dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020.pp 5713-5718. OI:10.30534/ijeter/2020/130892020.
[16] Fink L.M. The theory of transmission of discrete messages. Moscow, Publishing house "Soviet Radio", 1970. 728pp.