Розглядається методика оцінки функціональної ефективності обміну даними в корпоративної науково-освітньої мережі, яка ґрунтується на простому багатофакторному аналізі, в якій враховуються як технічні показники мережі, показники безпеки технічних засобів захисту інформації, так і економічні параметри. Такий підхід дозволяє інтегровано оцінити як технічну, так і інформаційну ефективність якості обслуговування користувачів корпоративної науково-освітньої мережі, отримати кількісні показники для оцінки відповідності послуг, що надаються висунутим вимогам

Ключові слова: синергетичний підхід оцінки загроз, інтегрований показник якості обслуговування, корпоративна науково-освітня мережа

Рассматривается методика оценки функциональной эффективности обмена данными в корпоративной научно-образовательной сети, основывающаяся на простом многофакторном анализе, в которой учитываются как технические показатели сети, показатели безопасности технических средств защиты информации, так и экономические параметры. Такой подход позволяет интегрировано оценить как техническую, так и информационную эффективность качества обслуживания пользователей корпоративной научно-образовательной сети, получить количественные показатели для оценки соответствия предоставляемых услуг выдвигаемым требованиям

Ключевые слова: синергетический подход оценки угроз, интегрированный показатель качества обслуживания, корпоративная научно-образовательная сеть

UDC 621.391
DOI: 10.15587/1729-4061.2017.118329

ASSESSMENT OF FUNCTIONAL EFFICIENCY OF A CORPORATE SCIENTIFIC-EDUCATIONAL NETWORK BASED ON THE COMPREHENSIVE INDICATORS OF QUALITY OF SERVICE

S. Yevseiev
PhD, Associate Professor
Department of Information Systems*
E-mail: serhii.yevseiev@m.hneu.edu.ua
V. Ponomarenko
Doctor of Economic Sciences, Professor, Rector*
O. Rayevnyeva
Doctor of Economic Sciences,
Professor, Head of Department
Department of statistics and economic forecasting*
E-mail: olena.raev@m.hneu.edu.ua
*Simon Kuznets Kharkiv National
University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

1. Introduction

The advent of high technologies enables mankind to further develop capacities of computational systems. The rapid growth and expansion of the functionality of enterprise systems and social networks make it possible to construct integrated social-informational networks to address a diverse range of tasks. Further development of the data transmission technology *Ethernet* creates a global ideology for the deployment of telecommunication networks [1–4].

The development of e-learning systems and corporate educational systems (CES) is closely linked to the expansion of possibilities for remote access to the informational assets of state information educational systems (IES) based on *Ethernet* technologies [5]. Further integration of CES leads to the formation of corporate scientific-educational systems (CSES) – networking cooperation of associations of organizations aimed at producing particular intelligent products of the networking interaction [6]. Thus, revolutionary changes in the field of electronic education led to the establishment of CSES, to the integration of informational and computer networks of universities into a unified information and cybernetic space, which significantly extended the range of educational services and functions of CSES at educational establishments, to the integration of services into social networks, and further use of remote access in various forms of education. However, such an integration creates educational system with a mission-critical cybernetic infrastructure (SCCI), thereby increasing the risk of its hacking/destruction of its components and unauthorized access to confidential information of CSES.

The analysis of threats, performed in [7–12], indicates their substantial transformation and hybridity. Starting from threats to informational, cybernetic security and information safety of the infrastructure of CSES, the attributes of hybridity of threats now manifest themselves in the simultaneous activity on the object of protection – confidential, scientific/intellectual information at CSES due to the

emergence of phenomenon of synergy [7]. Based on a general concept of quality in line with the ISO 8402 standard, basic terms were defined in the field of quality of communication services (*Quality of Service, QoS*), first published in the ITU-T Recommendations E.800 [13]. Papers [14, 15] considered the requirements of standards to the main technical indicators of service quality – reliability and security. The ISO 9000:2015 standard [16] defines basic concepts and principles of quality control, the standard [17] outlines typical requirements to automated systems. In general, the quality of a service is characterized by a combination of the following basic consumer properties [15]: availability, ease of use, efficiency, safety, and other properties specific to each service.

Thus, it is an important task to estimate not only technical components of the operational efficiency of CSES but rather the effect of economic aspects on investment policy at universities to ensure safety of confidential information.

2. Literature review and problem statement

Remote access technologies and open resources of the Internet used by IES make it possible to substantially extend the range of scientific and educational services provided by a university. Therefore, there is a possibility to scale up and expand components of CSES, its software applications and tools, e-courses and educational modules, which enables better access to its scientific, informational-educational resources for its geographically scattered users. This creates considerable benefits and advantages in using CSES for extending the range of educational services, but, at the same time, the application of standard protocols for open systems increases the risks of hybrid attacks on the infrastructure of CSES [7, 18–21]. In order to ensure such components of security as informational safety (IS), cybersecurity (CBS), safety of information (SI), cryptographic mechanisms are typically employed based on symmetric and asymmetric cryptographic procedures, however, choosing from many software and hardware/software tools is a complex task. The analysis of standards, performed in paper [22], revealed that the key principle of control over IS is the assessment of risks. Experience shows that at present one can clearly distinguish two main groups of methods for assessing the risks for safety [22]. The first group of methods makes it possible to establish the level of risk by estimating the degree of correspondence to a specific set of requirements on ensuring information security. The second group of methods for IS risk estimation is based on determining the probability of attacks, as well as their level of damage. In this case, the value of risk is calculated separately for each threat, and, in a general case, is represented as the product of the probability of threat implementation by the magnitude of the potential harm from a given threat. The value of damage is determined by the owner of the information while the probability of a threat is estimated by a panel of experts who conduct the audit procedure. A signature of the first and the second groups of methods is the application of different scales for determining the magnitude of risk. In the first case, risk and all related parameters are expressed in numerical, that is, quantitative values. In the second case, qualitative scales are employed. In order to run a comparative analysis, different protocols are typically applied, such as *Vaughn-Hennig-Siraj*, *NIST STS*822, *OCIPEP*, *OCTAVE*, *CISWG*, *Erkan Kahraman*; using them, however, involves both time and economic costs [22].

In order to ensure safety of CES, papers [18, 21, 22] address the policies, standards, technologies and procedures for providing information security to corporate educational networks; a technique is proposed for protecting local servers of CSES based on the construction of virtual private networks. An integral part of CSES (IES) at educational institutions are social networks whose portals host personal data on millions of users, thereby representing huge online directories that, if desired, are accessible for everyone [19]. A modern University stores and processes a huge volume of various data related not only to ensuring the educational process. The servers of CSES contain information about scientific research and engineering developments, personal data on students and university staff, service and other confidential information [20]. However, conceptual strategy, as well as policies and procedures for ensuring the security of information assets of CSES, are virtually non-existent at legislative level. In paper [23], authors proposed a synergistic approach to the model of IES safety assessment, a procedure for constructing a modified system of electronic document circulation at a University based on electronic digital signature in line with the standard X.509. In paper [24], authors proposed a comprehensive technique for selecting protective tools based on the methods of game theory and analysis of hierarchies.

Increasing structural complexity and dimensionality of modern CSES significantly affects scalability and scaling up of its structure due to multiple information links, need to increase the level of information security, increasing number of consumers and volumes of information resources. Decrease in the performance operation of networks is connected with insufficient protection due to the widespread use of such vulnerable protocols as *HTTP, SNMP, FTP, TCP/IP*; participation of various categories of users in information processing, immediate and simultaneous access to systems resources and processes [25, 26]. In order to provide flexibility of the services provided by networks, papers [27, 28] propose the use of virtualization technologies and a protocol of multiple access with temporal division (TDMA) to a channel at the network level. In articles [29, 30], authors tackled issues on the evaluation and improvement of reliability in converged corporate networks based on technologies for ensuring a reserve of network infrastructure elements and scalability.

Paper [31] proposed a technique for the evaluation of data exchange in global computational networks (GCN) based on the comprehensive indicator of service quality that makes it possible to assess the quality of network service based on technical criteria for reliability and safety and economic cost related to a "loss" of confidential information on the basis of (FAIR) technique. In article [32], authors conducted a comparative analysis of the quality of service in IP networks based on the procedure proposed in [31].

Paper [33] addresses issues of modeling the effectiveness of control and service provision in mission-critical information and communication infrastructures, a methodology is proposed for performing a quantitative analysis of underlying dependences based on the violations of normal operation of SCCI. In [34], authors examined the relationship between investment in new technology and indicators of quality of service (*QoS*) – reliability and performance efficiency.

Thus, in order to satisfy the increasing need in qualitative service by the users of informational resources of a

University under conditions of growth of the hybrid threats to the informational resources of CSES, work of various applications and services of the elements of CSES, there is a necessity to estimate effectiveness of its functioning based on the criteria of service quality – reliability and safety [31, 32].

The proposed approach, however, does not take into consideration the impact of synergy in the manifestations of threats, manifestation of their hybridization and their aggregation on different directions of safety at corporate scientific-educational systems – IS, CBS, SI, it does not make it possible to select cryptographic mechanisms to ensure basic safety services: confidentiality, integrity and availability, does not allow analysis of the effectiveness of investment into information protection system (IPS). We denote by a *cybernetic impact* those actions that are directed against objects or subjects of cyberspace (social, technical and sociotechnical systems), in the form of various destructive impacts whose implementation leads to control over objects and/or subjects exposed to the impact. [7]. Main cyber threats (DOS attacks, R2L-attacks, U2R-attacks, Probe-attacks) affect basic indicators of quality of service (*QoS*) – reliability and safety and their components: throughput, overall coefficient of readiness of CSES to provide access to information resources of the network, information resources deliverability and fault tolerance of the system. *Informational impact* refers to activities aimed at changing the mass and/or individual consciousness of the subject exposed to the impact in order to stimulate a given type of conduct [7]. Informational impact is typically created through social networks [19] and it is based on social engineering methods: isolation, discrediting, warning, persuasion, disinformation, intimidation, etc. [7].

Social engineering techniques can influence the informational component of functional efficiency of CSES, thereby lowering safety indicators and particular reliability indices: throughput, network performance efficiency.

Thus, there is a need to take into consideration a synergistic approach to the assessment of possible impact from intruders on the elements of CSES (IES) infrastructure as a system with a mission-critical cybernetic infrastructure.

3. The aim and objectives of the study

The aim of present work is to devise a procedure for assessing functional efficiency of data exchange within a corporate scientific-educational network, based on a basic multivariate analysis with a synergistic approach to the estimation of hybrid threats to CSES. Such an approach takes into consideration both the technical parameters (data transmission rate, probability and time of delivery of a packet, etc. in IP-networks), safety indicators (resistance, efficiency of software implementation) and economic parameters (the cost of scaling and network servicing, etc.).

To accomplish the aim, the following tasks have been set:

– to devise a comprehensive indicator of the functional efficiency of data exchange within a corporate scientific-educational network;

– to conduct a study into efficiency of data transfer within CSES for different techniques of control over data exchange.

4. Development of a procedure for estimating functional efficiency of data exchange within a corporate scientific-educational network

Quality of a service is characterized by a combination of the following basic consumer properties [31, 34–36]: availability, ease of use, efficiency, safety and other properties specific to each service. In addition to such technical characteristics of networks as performance efficiency, latency, scalability, degree of transparency for end users, very important characteristics are comprehensive indicators of reliability: readiness factor and the mean downtime per year. Reliability indicators directly affect the availability of informational services for users. In addition, reliability of the network also indirectly influences productivity and network latency, because the cause of fire and faults in the network lead to the need to retransmit data blocks, and this eventually leads to an increase in delays in transmission and a reduction in the volume of data transferred per time unit [35]. In order to estimate technical component of the functional efficiency [6], we shall apply a general indicator of data exchange effectiveness that includes speed of reliable and confidential transmission of data over a computer network and makes it possible to compare effectiveness of the existing protocols during data exchange between two nodes, described in article [31]. This indicator allows choosing an optimal strategy for the functioning of computer network u^* out of the set of permissible strategies U, a selection from which is carried out based on a criterion of the maximum average result [36].

Such an approach is certainly effective, but it has some drawbacks. There is no substantiation of cryptographic resistance of the mechanisms for ensuring information safety, no accounting for the synergy of possible impacts on CSES infrastructure elements, no economic indicators for performance of a computer network and estimation of investment into IS of CSES informational resources.

Application of cryptographic means for information protection entails serious changes in the time of delivery of information, since this indicator includes the time spent on encryption/decryption of a packet. An analysis of encryption/decryption time by the winners of crypto-algorithms contests AES and NESSIE reveals that for asymmetric algorithms the complexity of implementation of cryptographic transformations is 3–5 orders of magnitude larger than that of similar systems of time stability (block symmetric ciphers).

Thus, in the IP-networks with a critical feedback, packet delivery time is equal to [36]:

$$t_{delivery} = t'_{delivery} + \Delta t_{delivery} + t_{encr} + t_{dencr}$$

for symmetric crypto-algorithms,

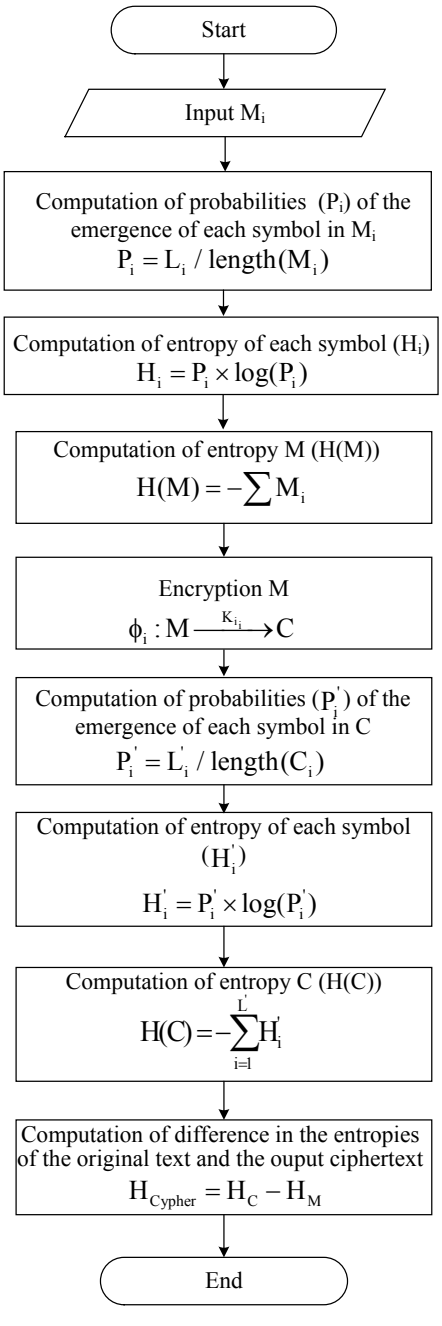
$$t_{delivery} = t'_{delivery} + \Delta t_{delivery} + (t_{encr} + t_{dencr})^s$$

for asymmetric (hybrid) crypto-algorithms, where t'_d is the time of delivery of packet with the first parcel, $\Delta t_{delivery}$ is the time of multiple repetition of information transmission at channel quality deterioration; t_{encr} is the time of data packet encryption by a crypto-algorithm; t_{dencr} is the time of data packet decryption by the recipient; s is the multiplicity of time for encryption/decryption.

A comparative estimation of the effectiveness (crypto-resistance) of symmetric crypto-algorithms typically

employs methods of linear and differential cryptanalysis whose main stages and effectiveness are addressed in paper [37]. A comparison of safety mechanisms for the algorithms of traditional cryptography, cryptography with a public-key, hybrid cryptosystems, is possible based on the comprehensive indicator that takes into consideration the criteria for crypto-resistance, performance speed, crypto-transformation rate, transparency of encryption procedures for the user, key sequences allocation, investments into IS, which does not make it possible to determine their effectiveness without significant temporal and economic expenditures. In order to assess stability of crypto-algorithms from various models of cryptosystems, authors suggest performing an express analysis based on the entropy method, applied in the package for statistical study of the random variable NIST STS 822 [39]. The proposed express analysis makes it possible, without significant computational and energy costs, at the intuitive level, to compare not only the resistance of various crypto-algorithms (cryptosystems), but their software implementation. The algorithm of the entropy method for assessing crypto-resistance is shown in Fig. 1.

Table 1 gives results of study into stability and software effectiveness of implementation of block and stream ciphers of varying complexity. We applied DES, 3DES, GOST 28147, Kalina, AES-256 as block ciphers. To implement a stream cipher, we used pseudo-random sequence generators of two different types: based on the rule "60" of cellular automata in its classical form, without modifications, and the cryptographically resistant generator SecureRandom from Java crypto-libraries, which is marketed as suitable for cryptographic applications.



Computation of entropy of the original message with a specified length

M_i – original message,
P_i – probability of the emergence of the *i*-th symbol in M_i,
L_i – number of the *i*-th symbols in M_i,
H_i – entropy of the *i*-th symbol,
H(M) – entropy M

Computation of entropy of the encrypted message with a specified length

C – encrypted message,
P_i' – probability of the emergence of the *i*-th symbol in C,

L_i' – number of the *i*-th symbols in C,

H_i' – entropy of the *i*-th symbol in a ciphertext,

H(C) – entropy C

Fig. 1. Algorithm for testing the cryptosystem for resistance based on the method for the estimation of randomness

Table 1

Results of testing the resistance of crypto-algorithms using an express-method

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Difference	% of entropy, added by the cipher
1	Cellular automata, the rule "60"	0.5023775 (5.023775)	0.6820179 (6.820179)	0.1796404 (1.796404)	35.7580505
2	Crypto-resistant generator Secure-Random from Java crypto-libraries	0.5023767 (5.023767)	0.7999982 (7.999982)	0.2976215 (2.976215)	59.2426958
3	DES	0.469276	0.812043	0.342767	73.0416642
4	3DES	0.469276	0.812043	0.342767	73.0416642
5	GOST 28147-89	0.469276	0.811348	0.342072	72.8935637
6	Kalina	0.469276	0.954519	0.485243	103.4024753
7	AES-256	0.469276	0.95454	0.485264	103.4069503

In Table 1, we calculated entropy of the input and the encrypted text, difference, as well as the percentage of entropy added to the entropy of plaintext by the cipher itself. An analysis of Table 1 allows us to assess the contribution of the cipher in the total entropy of the encrypted message. As they all were tested under identical conditions, it is possible to judge their relative performance.

The AES-like ciphers (SPN-system, substitution-permutation schemes) are worth mentioning. Both such ciphers, Kalina and AES, made the greatest contribution, larger than 103 %, to the entropy of the plaintext. According to the given results, both ciphers have the best diffusing effect. Approximately the same results were demonstrated by the symmetric block cipher (SBC) GOST 28147-89: 72.89 % against 73.04 % for DES/3DES. This probably confirms conclusions about the maximally possible degree of dispersion as a characteristic of the architecture.

To compare the results, we conducted experiments using stream ciphers based on two different generators with a pseudorandom key sequence. Encryption was performed by the rule of addition for modulo two. In the first case, this is a generator based on cellular automata (the rule "60"). This is not a crypto-resistant generator whose sequence does not passes testing for NIST STS 822, while the second one is positioned as the crypto-resistant generator SecureRandom in the Java crypto-library. In both cases, the obtained values for entropy are much smaller than those for classic SBC, which does not allow us to argue about quality encryption with their help.

Thus, the results presented suggest that a simple entropy method allows rapid assessment of the quality of ciphers used without referring to expert estimations. Such an express technique is available to anyone with a minimal knowledge of the information theory. Moreover, in this way one can evaluate different implementations of ciphers that will make it possible to select the best (optimal) software implementation that matches terms and requirements of the user. For example, in our computer experiments, we used two implementations of the DES algorithm. One of them, given in Table 1 at number 3, demonstrated a 73.04 % increase in entropy after encrypting compared to the original text, another one – 64.4 %. It is obvious that for practical purposes it makes sense to choose the first implementation, since it appears that its scattering characteristics are better. Thus, the express-analysis allows assessment of the quality of implementation of classic (and other) crypto-algorithms in order to select optimal crypto library out of many commercially available libraries.

We shall consider the results obtained in terms of maximum cryptographic information protection. An indicator of such protection is the entropy of the encrypted binary file, given in Table 2.

Table 2

Estimation of maximal cryptographic protection of information

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Probability of cryptographic protection, P_c
1	Cellular automata, the rule "60"	0.469276	0.637079949	0.637079949
2	Crypto-resistant generator Secure-Random from Java crypto-libraries	0.469276	0.747287753	0.747287753
3	DES	0.469276	0.812043	0.812043
4	3DES	0.469276	0.812043	0.812043
5	GOST 28147-89	0.469276	0.811348	0.811348
6	Kalina	0.469276	0.954519	0.954519
7	AES-256	0.469276	0.95454	0.95454
8	Perfect cipher		1.000	1.000

It is known that the maximum possible cryptographic protection is provided by the so-called "perfect cipher" by Shannon, which as a result of encryption produces a random number [38]. Such a file will have maximum entropy, which in the binary case is equal to unity. We assume that encryption using a given cipher will ensure maximal cryptographic protection; we assume that it equals unity. One can say that the probability of protection using such a cipher is equal to unity. It is natural that imperfect ciphers do not produce such a probability of cryptographic protection. By using such an approach, one can rank all the examined ciphers for the probability of cryptographic protection. This indicator can be employed for various procedures for the assessment of protection of integrated protection systems of different corporate networks, which testifies to its universality.

In order to assess the impacts (informational and/or cybernetic) on the infrastructure elements, we shall refer to a threat classifier, proposed in paper [40] (online access: http://skl.hneu.edu.ua/). The main difference between a given classifier and the known ones is a synergistic approach to assessing threats to main components of safety provision:

IS, CBS, SI. Many threats to IS, CBS, SI can be found at resource [22].

A description of the modified threat classifier consists of four numerical magnitudes:

– a component of safety provision: information security (IS) (01), safety of information (SI) (02), cybersecurity (CBS) (03);

– a character of directions: legal (01), organizational (02), engineering-technical (03);

– main features of information: confidentiality (01), integrity (02), accessibility (03), authenticity (04);

– hierarchy levels of CSES infrastructure: FL – physical layer (01), NL – network layer (02), OSL – operating systems level (OS) (03), DBL – database management systems level (04), BL – level of technological applications and services (05).

To determine an indicator of threat assessment based on synergistic approach $W_{synerg}^{IS,CBS,SI}$ (indicator of hybridity of threats $W_{synerg}^{hybrid\ C,I,A,Au}$), we shall introduce (Table 3) frequencies of threat occurrence, which allows translation of verbal categories into digital.

Table 3

Frequency of threats

Points	Frequency of threat occurrence
0	No threat
1	Threat occurs not oftener than once per 5 years
2	Approximately, once per year
3	Approximately, once per month
4	Approximately, once per week
5	On a daily basis

We denote the frequency of threat occurrence via P_i; metric coefficients for each threat that show expert estimates of the impact of a particular threat on confidentiality, integrity, accessibility and authenticity will be denoted w_i^C, w_i^I, w_i^A, w_i^{Au}.

The possibility of implementation of each i-th threat considering the frequency of its occurrence is assigned by expression:

$$w_i = w_i^C P_i \cup w_i^I P_i \cup w_i^A P_i \cup w_i^{Au} P_i = 1,$$

where $w_i^C P_i$ is the implementation of the i-th threat to the service of confidentiality; $w_i^I P_i$ is the implementation of the i-th threat to the service of integrity; $w_i^A P_i$ is the implementation of the i-th threat to the service of accessibility; $w_i^{Au} P_i$ is the implementation of the i-th threat to the service of authenticity.

Assessment of a few threats to a particular safety service is assigned by respective expression:

$$W_{synerg}^C = \sum_{i=1}^{N} w_i^C P_i \ - \text{service of confidentiality;}$$

$$W_{synerg}^I = \sum_{i=1}^{N} w_i^I P_i \ - \text{service of integrity;}$$

$$W_{synerg}^A = \sum_{i=1}^{N} w_i^A P_i \ - \text{service of accessibility;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{N} w_i^{Au} P_i \ - \text{service of authenticity,}$$

where N is the total number of threats in the classifier.

When forming metric coefficients, it is considered that the results obtained are related to independent threats; in the case of their dependence (a threat classifier match) it is necessary to apply the expression for determining a complete probability of dependent events.

Statistical processing of the results of estimating a probability of impact of the i-th threat to the service of safety of CSES is conducted by experts in line with the procedure described in paper [41].

The final estimate of the i-th threat is averaged by the number of experts according to expression:

$$\widetilde{x_i} = \frac{\sum_{n=1}^{N_{\exp}} x_n \times k_n}{N_{\exp}},$$

where x_n is the estimate of the n-th expert of the impact of the i-th threat; k_n is the level of competence of the expert; N_{exp} is the number of experts.

In order to determine a synergistic indicator of threats to IS W_{synerg}^{IS}, we shall apply expression:

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i.$$

In order to determine a synergistic indicator of threats to CBS W_{synerg}^{CBS}, we shall apply expression:

$$W_{synerg}^{CBS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i.$$

In order to determine a synergistic indicator of threat hybridity to SI W_{synerg}^{SI}, we shall apply expression:

$$W_{synerg}^{SI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i.$$

In order to determine an integrated synergistic indicator of threats $W_{synerg}^{IB,KBrB,BI}$, we shall apply expression:

$$W_{synerg}^{IS,CBS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CBS} \cup W_{synerg}^{SI}. \quad (1)$$

In order to determine an integrated synergistic indicator of threats based on their hybridity $W_{synerg}^{hybrid\ C,I,A,Au}$, we shall apply expression:

$$W_{synerg}^{hybrid\ C,I,A,Au} = \\ = W_{synerg}^C \cap W_{synerg}^I \cap W_{synerg}^A \cap W_{synerg}^{Au}. \quad (2)$$

The results of study of threats with a max frequency of their manifestations to CSES are given in Table 4.

An analysis of Table 4 reveals that the probability of implementation of threats to CBS is an order of magnitude higher than that to IS, SI. Synergy of threats for the components of safety: IS, CBS, SI, leads to an increase in the probability of implementation of threat to the service of safety by 2 times, and their hybridization leads to a further increase in the probability of threat implementation. The obtained results allow us to refine the indicator of safety in the proposed procedure for the evaluation of functional efficiency of CSES.

Based on the proposed express analysis for the evaluation of crypto resistance of procedures of crypto-transformations

and the integrated indicator of threats, we shall obtain the resistance of CSES safety system against possible activities of an intruder:

$$B = H_{Cypher} \times W_{synerg}^{IS,CBS,SI} = \\ = \left(H_C - \log_2 n\right) \times \left(W_{synerg}^{IS} \cup W_{synerg}^{CBS} \cup W_{synerg}^{SI}\right). \quad (3)$$

Table 4

Results of the assessment of threats based on a synergistic approach

Components of safety	Safety services				
	C, W_{synerg}^{C}	I, W_{synerg}^{I}	A, W_{synerg}^{I}	Au, W_{synerg}^{Au}	Total
IS W_{synerg}^{IS}	0.023	0.223	0.193	0.207	0.0002
CBS W_{synerg}^{CBS}	0.222	0.234	0.197	0.134	0.0014
SI W_{synerg}^{SI}	0.226	0.109	0.152	0.189	0.0007
Total	0.471	0.566	0.542	0.53	
$W_{synerg}^{IS,CBS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CBS} \cup W_{synerg}^{SI} =$ $= 0,0002 + 0,0014 + 0,0007 = \mathbf{0,0223}$		$W_{synerg}^{\text{hybrid}\,C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{1} \cap W_{synerg}^{A} \cap W_{synerg}^{Au} =$ $= 0,471 \times 0,566 \times 0,542 \times 0,53 = \mathbf{0,0766}$			

In order to estimate the informational component of functional efficiency [6], we shall apply a *modified procedure for assessing investment into SI*, proposed in paper [42].

To assess the economic component of the effectiveness of IT projects, basic indicators of financial status are most often used: return on investment (*ROI*), net present value (*NPV*), internal rate of return (*IRR*), payback period (*Payback Period*), economic attractiveness (*EVA*), balanced scorecard (*BSC*), total cost of ownership (*TCO*), etc. [43]. The analysis of methods for estimating the effectiveness of IT investments that we conducted revealed that the formation of an objective assessment of the effectiveness of investments is an extremely time-consuming process and, typically, estimation of the activities related to information security comes down to finding such categories as *ROI*, return on investment, the rate of return on investment, *TCO*, *Total Cost of Ownership*, *PB*, *Payback Period*.

A procedure for evaluating effectiveness of investments, proposed in paper [42], comes down to estimating the risks of safety violation at CSES, which makes it possible to assess the continuity of business processes functioning, a coefficient of internal rate of return on investments in CSES security.

Representing information security as an information process, rather than a product, allows us to interpret safety of informational assets as a multi-purpose process of managing risks in the violations of CSES safety regime. As a result of risk management, it is possible to balance informational risks for CSES activities, reducing potential threats to computing tools that process information resources. The results of the balance of risks to information assets is the selection of effective management method, which makes it possible to define with maximum accuracy parameters of information security, and to receive maximum profit from the funds invested into building IPS at CSES [42].

A formal description of the model for estimating investment in IS of CSES can be represented as:

$$W_{effinv} = \begin{Bmatrix} I_O, \Delta, \{DF\}, rang, \{SZ\}, d, D \\ ROI, NPV, ROSI, r, CV, OU \end{Bmatrix},$$

where I_O is the significance of an informational asset; Δ is an indicator of cost effectiveness; $\{DF\}$ is the set of sources of threats to information safety of CSES; *rang* is the cost of IPS development; $\{SZ\}$ is the set of a IPS; d is the resulting value of cash flow; *ROI* is the return on investment ratio; *NRV* is the net present value; *ROSI* is the ROI in IPS; r is the factor of profitability of information security; *CV* is the risk per unit of average income; D is the income from the use of IPS; *OU* is the assessment of income from the use of IPS.

Assessment procedure consists of the following steps [42]:

Step 1. Determining the significance of an informational asset;

Step 2. Determining an indicator of cost-effectiveness Δ;

Step 3. Determining net present value *NPV*;

Step 4. Estimation of cost for the development of IPS at CSES;

Step 5. Determining the resulting value of cash flow d;

Step 7. Assessment of risk per unit of average income *CV*;

Step 8. Determining income D from the use of IPS.

The proposed methodology is based on the assessment of investments into SI of CSES (IES) and the discounting of future cash inflows and expenses.

Thus, it takes into consideration a change in investments into SI of CSES over time. It is proposed to use, as optimization measures, the assessment of overall cost of expenses for the elimination of consequences of threats and other reasons for IPS failure, and total payments to funding sources.

Estimation of overall cost of expenses M_{costs} for eliminating consequences of threat implementation and other reasons for IPS failure is conducted according to formula:

$$M_{\text{costs}} = \sum_{i=1}^{m} C_i,$$

where C_i is the cost of the i-th measure; m is the total number of steps taken.

The proposed model of the efficiency of investment into SI of CSES solves the task on improving investment efficiency by minimizing the cost of SI at CES.

Minimization of cost for SI of CSES is carried out by the optimization process, reflected by the following formula:

$$\min\left(E_1 b_1 + E_2 b_2 + ... + E_j b_n\right),$$

where E_j is the j-th optimization criterion, j=1,..., n_{opt}, n_{opt} is the number of criteria; $b_{n_{opt}}$ is the attribute of using the j-th funding source

$$b_{n_{opt}} = \begin{cases} 1, \text{ if the source of funding is used,} \\ 0, \text{ if the funding source is not used.} \end{cases}$$

Within the framework of the proposed model for assessing the efficiency of investment into SI of CSES, we estimate the following parameters – overall cost of eliminating consequences of threat implementation, total payments of funding sources. In this case, the minimization of damage is ensured and the cost of safety of SI of CSES is effective because profits earned from the implementation of IPS exceed the invested capital [24, 25].

By generalizing parameters used within the framework of the proposed model, we shall determine an integral criterion for the efficiency of investment into SI of CSES using formula:

$$W_{effinv} = \sum_{i=1}^{N_{criterion}} w_i M_{costs}. \quad (4)$$

This approach will allow us to determine permissible levels of risks in violating CSES IS, to assess the required preventive measures to eliminate potential information leakage channels, investment policy of educational institutions into IPS for a dynamically scalable CSES in order to provide a comprehensive approach to security and reliability.

Development of a comprehensive performance indicator of corporate scientific-educational network. In order to assess the integrated indicator of operational efficiency, authors of paper [31] compiled supporting tables that make it possible to select the ranges of change in the required parameters of the analyzed systems and to express them in conditional points. Such a simple method allows obtaining adequate enough results of the estimation, and, in addition, combining them with the results of precise calculations for specific parameters.

Thus, it is possible to describe completely different parameters that cannot be analytically combined in any other way. To compare existing data transmission technologies, the following were selected: packet switching by standard *X.25*; *Frame Relay; Ethernet, Fast Ethernet; Gigabit, 10 Gb, 40 Gb/100 Ethernet* [31, 36]. Results of the generalized effectiveness of computer networks (CN) for data transmission are given in conditional points in Table 5 and shown in Fig. 2.

Table 5

Generalized effectiveness of networks for data transmission

Technology	Cost	*V*	$P_{delivery}$ of packet	$T_{delivery}$	Packet delay	Performance	Indicator of multifactorial efficiency, W_{eff}	Normalized indicator of efficiency, W_{norm}	Relative efficiency, %
X.25	3	1	3	1	1	1	9	0.0078	0.25
Frame Relay	3	2	1	5	3	3	270	0.2344	7.37
Ethernet	3	1	2	4	3	3	216	0.1875	5.89
Fast Ethernet	3	2	2	4	3	3	432	0.3750	11.79
Gigabit Ethernet	2	3	4	4	3	3	864	0.7500	23.59
10 Gb Ethernet	2	4	4	4	3	3	1152	1	31.45
40/100 Gb Ethernet	1	5	4	4	3	3	720	0.6250	19.66
TOTAL:							3,663	–	100

Table 5 and Fig. 3 demonstrate that the proposed simple approach makes it possible to obtain a rather adequate result. One can see that today the most effective, given the values presented, is 10 Gb *Ethernet*. *Fast Ethernet,* popular for commercial communications, does not fully "cope" with increasing traffic, and 40 Gb *Ethernet* remains fairly expensive for the end user, which does not allow us to categorize it as an optimal network infrastructure.

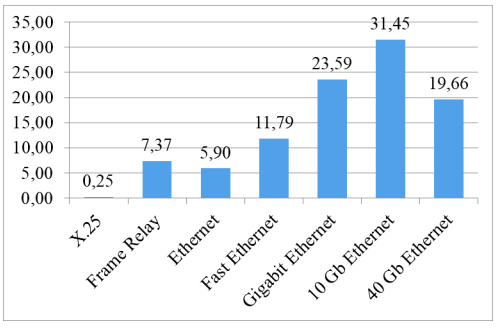


Fig. 2. Normalized indicator of efficiency of different technologies of CN, W_{norm}

At the same time, 10MB *Ethernet, Frame Relay*, not to mention the packet switching *X.25*, are considered, by even such a simple analysis, to be obsolete technologies that do not meet current realities.

Based on the study conducted, we propose a comprehensive indicator of CSES functional efficiency. The structure of building the indicator is such that it combined two basic characteristics of the system:

– the required probability of achieving the objective with the required indicator for ensuring confidentiality under certain conditions of external environment and at a certain level of influence from internal random factors;

– the cost of reaching the goal with the required probability and economic cost on the implementation of construction of corporate networks, taking into consideration the required quality of service.

Given all the above, we propose to complement the indicator of functional efficiency of a computer network with the normalized multifactor performance indicator W_{norm} in the following way:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times \times P_{cor\_rec}^{(u_i)} \times W_{effinv} \times W_{norm}, \quad (5)$$

where $W(u_i)$ is the indicator of efficiency of a computer network for selected strategy (reliability improvement method) u_i; $n^{(ui)}$ is the number of informational bits of a packet for selected strategy u_i; $t^{(ui)}$ is the delivery time of packet t for selected strategy u_i; $B^{(ui)}$ is the security system resistance for selected strategy u_i; $P_{cor\_rec}^{(u_i)}$ is the probability of correct delivery of a packet for selected strategy; U is the set of permissible strategies (methods of reliability improvement that are used in a computer network); $W_{eff}^{(ui)}$ is the indicator of multi-factor efficiency, calculated by the proposed method; W_{norm} is the normalized multifactor indicator of efficiency.

Such an approach would allow taking into consideration not only technical, but also economic parameters of the examined CSES, which would make it possible to better evaluate its functional efficiency, to account for research results when scaling a network, selecting IPS for CSES.

5. Discussion of results of the study into effectiveness of data transmission over computer systems and networks at different techniques for managing data exchange

Authors of paper [36], in order to increase the value of indicator of functional efficiency of a computer network, considered different techniques for managing data exchange: without a feedback with the detection of *r*-multiples errors; without a feedback with the correction of *t*-multiple errors. The most commonly used control protocols are: with a critical feedback and continuous transmission of frames (CFctr) "Return-to-*N*"; with a critical feedback and a positive receipt (CFpr). Studies reported in papers [31, 32, 36] showed that in order to ensure the maximum level of functional efficiency of IP-networks, it is required to employ protocols with a critical feedback based on the continuous transmission of frames (CFctr) "Return-to-*N*"; with a critical feedback and a positive receipt (CFpr). In addition, a detailed study into statistical properties of error sequences in actual communication channels [44–46] found that errors are dependent and tend to be grouped (combined in a packet), that is, there is a certain dependence among them, which is correlation. Most of the time, information travels along communication channels without distortion, but at certain points there occur the condensation of errors, the so-called packets (bundles, groups) of errors. Inside the packets of errors, an error probability turns out to be considerably larger than the average probability of error calculated for a significant time of transmission. Under such conditions, protection that is optimal for a hypothesis on independent mistakes proves ineffective when used in real-world communication channels. To account for the statistical properties of sequences of errors in actual communication channels, we shall consider a model of channel with memory.

In a given model, we should assign to the original data, instead of the probability of error in bit P_0, the following four channel parameters:

– probability of the occurrence of error packet P_n;

– the probability of an error inside a packet equals P_ε;

– mathematical expectation m_{ln} of the error packet length;

– root-mean-square deviation σ_{ln} of the error packet length.

We accepted in calculation:

$P_n=10^{-5}\div 10^{-2}$; $P_\varepsilon=0{,}8$; $m_{ln}=10$; $\sigma_{ln}=2$.

For CSES with a critical feedback and continuous transmission of frames "Return-to-N", the value for an indicator of efficiency is determined from:

$$W(u_3)=\frac{n^{(u_3)}-t^{(u_3)}}{n^{(u_3)}}\times B^{(u_3)}\times \times P_{cor\_rec}^{(u_3)}\times W_{effinv}\times W_{norm}, \quad (6)$$

where $W(u_i)$ is the indicator of efficiency of a computer network for selected strategy (reliability improvement method) u_i; $n^{(ui)}$ is the number of informational bits of a packet for selected strategy u_i; $t^{(ui)}$ is the delivery time of packet t for selected strategy u_i; $B^{(ui)}$ is the security system resistance for selected strategy u_i; $P_{cor\_rec}^{(u_i)}$ is the probability of correct delivery of a packet for selected strategy; U is the set of permissible strategies (methods of reliability improvement that are used in a computer network); $W_{eff}^{(ui)}$ is the indicator of multi-factor efficiency, calculated by the proposed method; W_{norm} is the normalized multifactor indicator of efficiency;

$$\mathrm{m}_t^{(u_3)}=\frac{n}{C}+\frac{L}{V_p}+t_{encr}+t_{dencr}+ +\frac{\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}\times \times\left(\frac{n+s}{C}+2\frac{L}{V_p}\right),$$

$$P_{cor\_rec}^{(u_3)}=\frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}.$$

For CSES with a critical feedback and a positive frame receipt, the value for an indicator of efficiency is determined from

$$W(u_4)=\frac{n^{(u_4)}-t^{(u_4)}}{n^{(u_4)}}\times B^{(u_4)}\times \times P_{cor\_rec}^{(u_4)}\times W_{effinv}\times W_{norm}, \quad (7)$$

where

$$t^{(u_4)}=\frac{n+s}{C}+2\frac{L}{V_p}+t_{encr}+t_{dencr}+\frac{n}{C}\times \times\frac{\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right)-\Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}},$$

$$P_{nor\_rec}^{(u_4)} = 1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P)^{n+i} \right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}} \right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}} \right) \right] \right\} \times$$

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

Fig. 3, 4 show estimates of functional efficiency of a computer network by the normalized multifactor indicator of effectiveness based on the use of SBC.

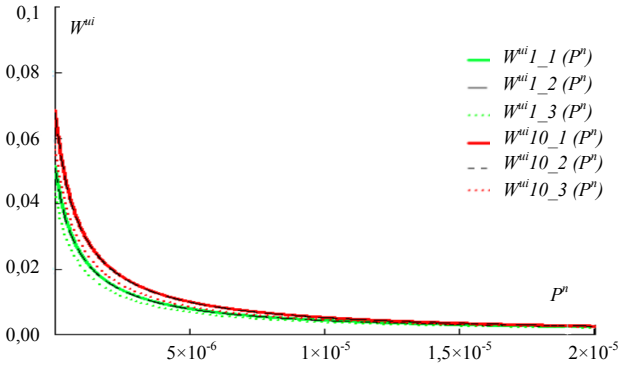


Fig. 3. Results of research into functional efficiency of CSES with a critical feedback and a continuous transmission of frames "Return-to-N" using a FAIR procedure

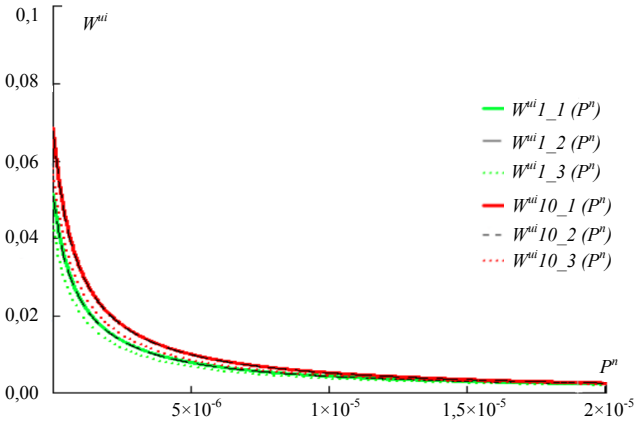


Fig. 4. Results of research into functional efficiency of CSES with a critical feedback and continuous transmission of frames "Return-to-N" using a procedure for assessing investment

When conducting a study into crypto-resistance, we applied an express-method for estimation based on an entropy method, as well as different procedures for evaluating economic cost based on a FAIR procedure; research results are reported in paper [32] (Fig. 4); and based on the proposed methodology for estimating the effectiveness of investment into information safety at CSES. Original data for the research are: technologies 1 Gbit Ethernet, 10 Gbit Ethernet, with a critical feedback and continuous transmission of frames "Return-to-N",

$W_{synerg}^{IS,CBS,SI} = 0.0022839$,

$t_{encr} = t_{dencr} = 0.01$ s,

$P_C^{AES} = 0.95454$,

$P_C^{Kalyna256} = 0.9454519$,

$P_C^{3DES} = 0.812043$,

$n = 1518$,

$C = 36{,}000$,

$P_{cor\_rec} = 0.99$.

An analysis of results in Fig. 3, 4 showed that the proposed procedure for estimating functional efficiency of CSES makes it possible, without significant time and expert costs, to evaluate the status of quality customer service at CSES, to apply evaluation results of CSES functional efficiency for scaling it up, to improve technical indicators of a computer network.

6. Conclusions

1. We performed an analysis of the development of services and functionality of IES (CSES) that showed that such systems should be considered as SCCI. With the growth of information technologies and further development of remote access for social systems and CSES, the growth and hybridization of threats to elements of SCCI, an important issue is to ensure safety and reliability of the functional efficiency of CSES. In order to assess it, it is proposed to use the integrated indicator of the quality of service for users of a network that takes into consideration the synergistic assessment of the possible impacts (informational and/or cybernetic) on the elements of CSES structure, indicators of technical and informational components of functional efficiency.

2. The developed technique makes it possible to standardize the assessment of efficiency of data exchange in global protocols of IP networks, taking into consideration economic cost of hardware and software and technologies, which provide the required indicators of safety and reliability of CSES functional efficiency, as well as the required value for the indicator of IP-network service quality. Practical application of the introduced indicator will make it possible to better assess effectiveness of protocols for data exchange used in global protocols of IP-networks. In addition, such an approach would solve the tasks on scaling and extension of CSES, since it includes not only technical, but also economic indicators of functional efficiency, which is very important to ensure the required quality of service for users of CSES. The obtained expressions for the efficiency of data transfer in CSES with different techniques to manage data exchange allow us to obtain comparative quantitative estimates of the resistance of software (hardware-software) implementation of technical means for information protection (TMIP), possible implementation of hybrid threats to CSES, the efficiency of investment into TMIP, integrated performance indicator when using various protocols for managing data exchange in networks based on Ethernet technologies.

References

1. Goloshchapov, S. 100GB Ethernet: osnovnye printsipy [Text] / S. Goloshchapov, I. Shahnovich // Pervaya milya. – 2011. – Issue 3. – Available at: http://www.lastmile.su/files/article_pdf/2/article_2820_580.pdf
2. Godovoy analiz rynka promyshlennyh setey 2016 v sootvetstvii s HMS [Electronic resource]. – Available at: http://www.industrialnets.ru/news/2016/godovoj-analiz-rynka-promyshlennykh-setej-2016-v-sootvetstvii-s-hms/
3. Ethernet i promyshlennye seti [Electronic resource]. – Available at: https://www.osp.ru/lan/2013/09/13037411/
4. Raspredelenie rynka promyshlennyh setey v 2016 g. po dannym HMS Industrial Networks [Electronic resource]. – Available at: http://ua.automation.com/content/raspredelenie-rynka-promyshlennyh-setej-v-2016-g-po-dannym-hms-industrial-networks
5. Kucheryaviy, A. E. Internet veshchey i setevye protokoly. Internet veshchey i setevye protokoly [Text] / A. E. Kucheryaviy, E. A. Kucheryaviy, A. V. Prokop'ev // Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovani. II-ya Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya. – Sankt-Peterburg: Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. prof. M. A. Bonch-Bruevicha, 2013. – P. 23–29.
6. Funktsional'naya effektivnost' [Electronic resource]. – Available at: https://www.ngpedia.ru/id625108p1.html
7. Hryshchuk, R. V. Osnovy kibernetychnoi bezpeky [Text]: monohrafiya / R. V. Hryshchuk, Yu. H. Danyk; Yu. H. Danyk (Ed.). – Zhytomyr: ZhNAEU, 2016. – 636 p.
8. Kiberbezopasnost' 2016–2017: Ot itogov k prognozam [Electronic resource]. – Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf
9. Rise of IoT Botnets Showcases Cybercriminals' Ability to Find New Avenues of Attack [Electronic resource]. – Available at: http://storage.pardot.com/44731/127332/Cybercrime_Trends_Report___2016_Year_in_Review__1_.pdf
10. Issledovanie HP: Srednіy godovoy ushcherb ot kiberatak vyros do 15 mln doll. na organizatsiyu [Electronic resource]. – Available at: http://www.connect-wit.ru/issledovanie-hp-crednij-godovoj-ushherb-ot-kiberatak-vyros-do-15-mln-doll-na-organizatsiyu.html
11. CISCO: Kiberataki na industrial'nye sistemy usilivayutsya, a doverie k imeyushchimsya sistemam zashchity padaet [Electronic resource]. – Available at: https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/01-21a.html
12. Bank dannyh ugroz bezopasnosti informatsii [Electronic resource]. – Available at: http://bdu.fstec.ru/vul
13. MSE-T E.800. Opredelenie terminov, otnosyashchihsya k kachestvu obsluzhivaniya [Electronic resource]. – Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-R&type=items
14. Yanovskiy, G. G. Kachestvo obsluzhivaniya v setyah IP [Text] / G. G. Yanovskiy // Vestnik svyazi. – 2008. – Issue 1. – Available at: http://niits.ru/public/2008/2008-006.pdf
15. Vegeshny, Sh. Kachestvo obsluzhivaniya v setyah IP [Text] / Sh. Vegeshny. – Moscow, 2003. – Available at: http://it-ebooks.ru/publ/cisco/cisco_ip_quality_of_service/11-1-0-293
16. ISO 9000:2015(en). Quality management systems – Fundamentals and vocabulary [Text]. – International Organization for Standardization. – Available at: https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en
17. GOST RV 51987. Informatsionnaya tekhnologiya, kompleks standartov na AS [Text]. – Gosstandart Rossii. – Moscow, 2002.
18. Uskov, A. V. Tekhnologii obespecheniya informatsionnoy bezopasnosti korporativnyh obrazovatel'nyh setey [Text] / A. V. Uskov, A. D. Ivannikov, V. L. Uskov // Educational Technology & Society. – 2008. – Vol. 11, Issue 1. – P. 472–479.
19. Kondratova, E. G. Sotsial'nye seti kak kanal utechki korporativnoy informatsii [Text] / E. G. Kondratova // Bezopasnost' informatsionnyh tekhnologiy. – 2013. – Vol. 20, Issue 1. – Available at: https://elibrary.ru/item.asp?id=21003147&
20. Litvinov, V. A. Informatsionnaya bezopasnost' vysshego uchebnogo zavedeniya v ramkah sovremennoy globalizatsii [Electronic resource] / V. A. Litvinov, E. V. Lypko, A. A. Yakovleva // Available at: http://conference.osu.ru/assets/files/conf_reports/conf13/132.doc
21. Sohrabi Safa, N. Information security policy compliance model in organizations [Text] / N. Sohrabi Safa, R.Von Solms, S. Furnell // Computers & Security. – 2016. – Vol. 56. – P. 70–82. doi: 10.1016/j.cose.2015.10.006
22. Yevseiev, S. P. For information technologies security evaluation for automated banking systems of Ukraine [Text] / S. P. Yevseiev // Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, Issue 3. – P. 297–309. doi: 10.18372/2225-5036.22.11103
23. Evseev, S. P. Modelirovanie protsessov upravleniya v informatsionnoy ekonomike. Metodologiya postroeniya modifitsirovannoy sistemy elektronnogo dokumentooborota v universitete na osnove elektronnoy tsifrovoy podpisi standarta H.509 [Text] / S. P. Evseev. – Berdyansk: Izdatel' Tkachuk A.V., 2017. – 420 p.
24. Petrichenko, G. S. The technique of a security tools choice for a corporate network [Text] / G. S. Petrichenko, N. Y. Naryzhnaya, L. M. Kritskaya // Polythematic Online Scientific Journal of Kuban State Agrarian University. – 2016. – Issue 121 (07). – P. 1–10. doi: 10.21515/1990-4665-121-130
25. Karakus, M. Quality of Service (QoS) in Software Defined Networking (SDN): A survey [Text] / M. Karakus, A. Durresi // Journal of Network and Computer Applications. – 2017. – Vol. 80. – P. 200–218. doi: 10.1016/j.jnca.2016.12.019
26. Hailu, D. H. Unified study of Quality of Service (QoS) in OPS/OBS networks [Text] / D. H. Hailu, G. G. Lema, E. A. Yekun, S. H. Kebede // Optical Fiber Technology. – 2017. – Vol. 36. – P. 394–402. doi: 10.1016/j.yofte.2017.05.016
27. Han, B. Network function virtualization: Challenges and opportunities for innovations [Text] / B. Han, V. Gopalakrishnan, L. Ji, S. Lee // IEEE Communications Magazine. – 2015. – Vol. 53, Issue 2. – P. 90–97. doi: 10.1109/mcom.2015.7045396
28. Emfinger, W. Modeling Network Medium Access Protocols for Network Quality of Service Analysis [Text] / W. Emfinger, G. Karsai // 2015 IEEE 18th International Symposium on Real-Time Distributed Computing. – 2015. doi: 10.1109/isorc.2015.47

29. Stepanova, I. V. Ispol'zovanie perspektivnyh tekhnologiy dlya razvitiya raspredelennyh korporativnyh setey svyazi [Text] / I. V. Stepanova, A. A. Mohammed Omar // T-Comm: Telekommunikatsii i transport. – 2017. – Vol. 11, Issue 6. – P. 10–15.
30. Borodin, V. V. Some aspects of reliability assessment of the corporative data network with consideration of redundancy management [Text] / V. V. Borodin, E. A. Rastrelin // Systems and Means of Informatics. – 2015. – Vol. 25, Issue 4. – P. 150–157. doi: 10.14357/08696527150411
31. Yevseiev, S. P. Data exchange evaluation in global networks based on integrated quality indicator of service network [Text] / S. P. Yevseiev, H. N. Rzayev, S. E. Ostapov, V. I. Nikolaenko // Radio Electronics, Computer Science, Control. – 2017. – Issue 1. – P. 115–128. doi: 10.15588/1607-3274-2017-1-14
32. Korol, O. H. Otsinka yakosti obsluhovuvannia hlobalnoi merezhi na osnovi tekhnolohiy Ethernet za dopomohoiu kompleksnoho pokaznyka [Text] / O. H. Korol // Systemy obrobky informatsiy. – 2017. – Issue 2. – P. 100–110.
33. De Nicola, A. A methodology for modeling and measuring interdependencies of information and communications systems used for public administration and eGovernment services [Text] / A. De Nicola, M. L. Villani, M. C. Brugnoli, G. D'Agostino // International Journal of Critical Infrastructure Protection. – 2016. – Vol. 14. – P. 18–27. doi: 10.1016/j.ijcip.2016.06.001
34. Ali, H. Quality of service: Introduction of a new framework and a novel measurement technique [Text] / H. Ali // 2017 3rd International Conference on Information Management (ICIM). – 2017. doi: 10.1109/infoman.2017.7950439
35. Kayashev, A. I. Analiz pokazateley nadezhnosti lokal'nyh komp'yuternyh setey [Text] / A. I. Kayashev, P. A. Rahman, M. I. Sharipov // Vestnik UGATU. – 2013. – Vol. 17, Issue 5 (58). – P. 140–149.
36. Yevseiev, S. P. The analysis of data transfer efficiency in computer systems with usage of the integrated mechanisms of reliability and safety support [Text] / S. P. Yevseiev, D. V. Sumtsov, O. G. Korol', B. P. Tomashevskiy // Eastern-European Journal of Enterprise Technologies. – 2010. – Vol. 2, Issue 2 (44). – P. 45–49. – Available at: http://journals.uran.ua/eejet/article/view/2622/2428
37. Yevseiev, S. P. Use of mini-versions to evaluate the security of block-symmetric ciphers [Text] / S. P. Yevseiev, S. E. Ostapov, R. V. Korolov // Ukrainian Scientific Journal of Information Security. – 2017. – Vol. 23, Issue 2. – P. 100–108. doi: 10.18372/2225-5036.23.11796
38. Shennon, K. Raboty po teorii informatsii i kibernetike [Text] / K. Shennon. – Moscow: IL, 1963. – P. 333–369.
39. Rukhin, A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Text] / A. Rukhin, J. Sota, J. Nechvatal, M. Smid, E. Barker, S. Leigh et. al. – NIST Special Publication 800-22, 2000. – 169 p. doi: 10.6028/nist.sp.800-22
40. Yevseiev, S. P. Model' narushitelya prav dostupa v avtomatizirovannoy bankovskoy sisteme na osnove sinergeticheskogo podhoda [Text] / S. P. Yevseiev // Informatsiyna bezpeka. – 2017. – Issue 2 (26). – P. 110–120.
41. Buchyk, S. S. Metodyka ekspertnoho otsiniuvannia funktsionalnykh profiliv zahroz derzhavnykh informatsiynykh resursiv [Text] / S. S. Buchyk // Otkrytye informatsionnye i komp'yuternye integrirovannye tekhnologii. – 2015. – Issue 70. – P. 271–280.
42. Yevseiev, S. P. Otsenka effektivnosti investitsiy v bezopasnost' organizatsiy bankovskogo sektora na osnove sinergeticheskoy modeli ugroz [Text] / S. P. Yevseiev // Systemy obrobky informatsiy. – 2017. – Issue 2. – P. 88–94.
43. Homyakov, K. G. Otsenka effektivnosti investitsiy v kompleksnye sistemy zashchity informatsii kompaniy neftegazovogo kompleksa dlya prinyatiya vzveshennogo investitsionnogo resheniya [Text] / K. G. Homyakov, L. V. Kanitskaya // Ekonomika. Fundamental'nye issledovaniya. – 2015. – Issue 2. – P. 5173–5177.
44. Bleyhut, R. Teoriya i praktika kodov, kontroliruyushchih oshibki [Text] / R. Bleyhut. – Moscow: Mir, 1986. – 576 p.
45. Klark, Dzh.-ml. Kodirovanie s ispravleniem oshibok v sistemah tsifrovoy svyazi [Text] / Dzh.-ml. Klark; B. S. Tsybakov (Ed.). – Moscow: Radio i svyaz', 1987. – 392 p.
46. Mak-Vil'yams, F. Dzh. Teoriya kodov, ispravlyayushchih oshibki [Text] / F. Dzh. Mak-Vil'yams, N. Dzh. A. Sloen. – Moscow: Svyaz', 1979. – 744 p.