http://doi.org/10.35784/iapgos.3317 *received: 22.11.2022 | revised: 7.12.2022 | accepted: 15.12.2022 | available online: 30.12.2022*

GENERALIZED MODEL OF INFORMATION PROTECTION PROCESS IN AUDIOVISUAL CONTENT DISTRIBUTION NETWORKS

Heorhii Rozorinov[1], Oleksandr Hres[2], Volodymyr Rusyn[2]
[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Department of Acoustic Multimedia Electronic Systems, Kyiv, Ukraine, [2]Yuriy Fedkovych Chernivtsi National University, Department of Radio Engineering and Information Security, Chernivtsi, Ukraine

Abstract. *The most important indicators of the effectiveness of content protection systems are indicators of the achieved security level, i.e. functional properties of security. These indicators are: confidentiality, integrity, availability. Each of the indicators of the functional properties of content security is distributed according to the methods of ensuring and the degree of its achievement. A significant drawback of such indicators is that they are qualitative. This significantly narrows the scope of their use and makes it impossible to use them in mathematical expressions for optimizing the parameters of protection means, obtaining quantitative estimates of the performance quality of the protection system or its components, etc. The work offers a number of quantitative indicators, which, depending on the purpose, can be probabilistic and temporal. Calculation of such indicators makes it possible to assess the degree of ensuring the functional properties of information security or the possible degree of ensuring the functional properties of protected information.*

Keywords: security, content, communication network, model, indicator

UOGÓLNIONY MODEL PROCESU OCHRONY INFORMACJI W SIECIACH DYSTRYBUCJI TREŚCI AUDIOWIZUALNYCH

Streszczenie*. Najważniejszymi wskaźnikami skuteczności systemów ochrony treści są wskaźniki osiągniętego poziomu bezpieczeństwa – właściwości funkcjonalne zabezpieczeń. Takimi wskaźnikami są: poufność, integralność, dostępność. Każdy ze wskaźników właściwości funkcjonalnych bezpieczeństwa treści jest podzielony ze względu na metody zapewnienia i stopień ich osiągnięcia. Istotną wadą takich wskaźników jest to, że są one jakościowe. Zawęża to znacznie zakres ich stosowania i uniemożliwia wykorzystanie ich w wyrażeniach matematycznych do optymalizacji parametrów środków ochrony, uzyskania ilościowych ocen jakości działania systemu ochrony lub jego elementów itp. W pracy zaproponowano szereg wskaźników ilościowych, które w zależności od celu mogą mieć charakter probabilistyczny i czasowy. Obliczenie takich wskaźników pozwala ocenić stopień zapewnienia właściwości funkcjonalnych bezpieczeństwa informacji lub możliwy stopień zapewnienia właściwości użytkowych chronionych informacji.*

Słowa kluczowe: bezpieczeństwo, treść, sieć komunikacyjna, model, wskaźnik

Introduction

Computer facilities and infocommunication technologies are intensively implemented in all areas of human activity, the protection of information in audiovisual content distribution networks being of particular importance [4].

At the same time, significant contradictions arise: on the one hand, process automation significantly increases the capabilities of controls, and on the other hand, it leads to an increase in the dependence of control stability on the reliability of the operation of automation equipment and information protection from unauthorized access and interference [20].

Therefore, along with the requirements for efficiency, stability, continuity of operation, audiovisual content distribution networks are also subject to the requirements of such basic system security indicators as confidentiality, integrity, availability, and observability of processes related to the use of content.

This raises the classical problem of ensuring the maximum (or maximum possible) level of efficiency of the protection system by optimizing the parameters of its elements [17].

One of the main vectors of cyber threats to multimedia audiovisual content distributed in networks are cyber attacks. Today, these attacks can be seen simply as secondary threats creating "noise" in the network.

IoT are very common for protection of information in modern telecommunication networks [10, 22]. One of the most important functions of effective protection of the organization's information system is threat tracking and analysis and calculation of quantitative indicators of the functional properties of the security of content distributed in networks [1, 3, 5, 8, 9, 12, 19]. In [11] methods for ensuring data security in mobile standards are presented. Some methods can be used in programming level with biometric technical realization [16].

Today, the number of multimedia devices that use audiovisual content in networks continues to grow rapidly, therefore the issue of ensuring confidentiality and data security in networks is urgent, in particular, the development and improvement of information protection methods and data transmission methods (for example, based on pseudo-random sequences, chaos, etc.) [13, 14, 15].

The purpose of the work is to develop an effective system for the protection of audiovisual content with the formalization of the protection process in general, by developing its model.

1. Indicators of protection efficiency

Developing an effective content protection system is impossible without knowing what this efficiency is and how it is evaluated. The efficiency of the system means the degree of achievement of the goal set before it, and its assessment requires quantitative or qualitative characteristics, or a combination of them – the so-called performance indicators [2]. In so doing, the degree of achievement of the goal is determined by comparing the value of the achieved performance indicator with the desired or optimal value.

Quite often, it is difficult or even impossible to evaluate a complex system with a single efficiency indicator. In such cases, a system of indicators is introduced, and these indicators can be contradictory, that is, the improvement of the system according to some indicators leads to its deterioration according to others. In such cases, it is necessary to somehow combine these indicators into one, generalized, or define one of them as the main one, dominant, and the rest should be considered as certain peculiar restrictions. It is clear that such a problem is more or less well solved if these performance indicators have a numerical value and there are mathematical expressions for their calculation.

To build an effective audiovisual content protection system, it is necessary to:

1. formulate the purpose of the system functioning,
2. develop an objective function – an expression (expressions) for calculating an indicator or a set of system indicators,
3. find the optimal or acceptable value of the efficiency indicator and determine the conditions (values of the system parameters) under which this value is achieved,
4. determine the components of the system (subsystems or elements) that provide the necessary parameters.

There are system-wide and partial performance indicators, which can be qualitative or quantitative. Quantitative performance indicators are preferable, as they allow easier obtaining numerical values of the objective function and finding their optimal values.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Utwór dostępny jest na licencji Creative Commons Uznanie autorstwa – Na tych samych warunkach 4.0 Miedzynarodowe.

The task of content protection can be formulated as:

1. achieving the necessary level of protection at the minimum cost of the permissible level of restrictions on types of information activities;
2. achieving the highest possible level of protection at acceptable costs and a given level of restrictions on types of information activities;
3. achieving the maximum level of protection at the necessary costs and the minimum level of restrictions on types of information activities.

Any of these options requires the presence of indicators that would allow evaluating the effectiveness of solving the problem of content protection.

The most important indicators of the effectiveness of content protection systems are indicators of the achieved level of security, which are called functional properties of security. These indicators of functional properties of content security are:

1. confidentiality (a feature of information that information cannot be obtained by an unauthorized user or process),
2. integrity (a feature of information that information cannot be modified by an unauthorized user or process),
3. availability (a property of information that a user (or process) with the appropriate authority can use the content in accordance with the rules established by the security policy without waiting longer than a specified (small) period of time).

Each of these indicators of the functional properties of content security is distributed according to the methods (mechanisms) of ensuring and the degree of its achievement and has certain levels [18].

A significant drawback of such indicators is that they are qualitative. This significantly narrows the scope of their use and makes it impossible to use them in mathematical expressions for optimizing the parameters of protective equipment, obtaining quantitative estimates of the quality of the functioning of the protection system or its components, etc.

Therefore, this work offers a number of quantitative indicators, which, depending on the goal, can be probabilistic and temporal, namely:

1. Quantitative characteristic of violation of the confidentiality of the content – the probability of meaningful (that is, with an understanding of the content) reading of the information, which, depending on the features of the construction of the protection system, is determined by:
   - the probability of unauthorized access when confidentiality is ensured only by means of access restriction, as well as in the absence or when the violator overcomes the means of cryptographic transformation of information,
   - cryptographic stability of the encrypted content (when confidentiality is ensured only by means of cryptographic transformation of information, as well as when the violator overcomes the means of restricting access to information).
2. Quantitative characteristics of violation of the integrity of the content, which, depending on the features of the construction of the protection system is determined by:
   - the probability of unauthorized access (when integrity is ensured only by means of access restriction, deliberate influence of authorized users, and also if the violator does not have or overcome the means of integrity control),
   - the probability of information distortion (during random user impacts, as well as direct impacts of natural factors on information resources).
3. Quantitative characteristics of violation of content availability, which, depending on the features of the construction of the protection system is determined by:
   - the probability of unauthorized access (when integrity is ensured only by means of restricting access and intentional user influences),
   - delay time in content access (or content delivery).

Calculation of the indicated quantitative characteristics of content security by means of technical protection makes it possible to assess the degree of ensuring the functional properties of information security or the possible degree of ensuring the functional properties of protected information with the aid of tools designed for implementation. In both cases, for such a definition, it is necessary to have either the actual structural diagrams of the tools used, or models of the tools being developed for implementation.

An extremely important type of indicators is the economic (cost) indicators of the effectiveness of the content protection system. This follows from the fact that cost indicators, regardless of their origin, can always be reduced to economic costs. In addition, if the task of protection is not fulfilled or appropriate tools of protecting the content are not applied, its owner suffers some damage, which is also often easily reduced to additional costs and, thus, to economic indicators. And, on the contrary, the fulfillment of the protection task with the use of appropriate tools reduces such possible costs and damage, that is, it allows preventing possible costs.

The amount of damage, including the amount of harm that can be prevented or the cost of spending a particular content, can be estimated using:

1. quantitative indicators of security,
2. time indicators of processes related to the organization and implementation of control,
3. the specific cost per time unit of the delay in the provision of relevant services for the use of content and the duration of such a delay,
4. the cost of spending this or that content – also due to the cost of the time unit of its use and the duration of its use,
5. the intensity of content security threat flows.
6. At the same time, the dependence of cost indicators of security on the listed variables can be considered as an objective function, and time and other characteristics can be used as parameters (in some cases, as restrictions) for optimizing economic (cost) performance indicators.

For the technical protection of content, which effectively provides the required level of functional services or functional security properties in the conditions of the influence of threats to these functional security properties, it is advisable to:

1. Formalize the process of technical protection of content in general, by developing its adequate model.
2. Formalize the processes of ensuring the functional properties of content security by developing models of such processes and introduce their quantitative characteristics.
3. Determine the composition and sufficiency (functional completeness) of the tools that should be used for the technical protection of content.

2. Generalized model of technical content protection

The general formulation of the task of formalizing the content protection process is as follows [6].

Let there be a protected audiovisual content distribution network, the information resources of which are the objects of influence of unauthorized users-infringers, who, by their unauthorized actions on the resources of this network, create i (i = 1, 2, 3) types of threats to these resources, namely: threats to privacy, threats to integrity and availability threats (Fig. 1). Let a successful attempt to implement each of these threats cause damage to the system (or its owner) (for example, in the form of monetary damage), the amount of which depends on the type of threat, the duration of its action and is equal to conventional units per unit of time on average. Let also this damage be of an additive nature, that is, it can accumulate depending on the number and duration of threats that have not been countered.

Obviously, the amount, nature and even the time of manifestation of damage depends on the type of the corresponding threat. For example, the implementation

of an availability threat leads to the blocking of the network and the termination of the service provision process. Realized threats to the integrity of part of the basic and application software are equivalent to threats to availability, and as threats to some information resources.

Realized privacy threats most likely will not affect the network performance in any way, but may manifest themselves in the area of damage due to loss of image, trust in the owner of the content (or relevant information), failure of contracts, loss of positions in the service market, etc. Therefore, the mechanisms of calculating or recalculating the possible damage into conventional units F_i per unit of time have different complexity, but these mechanisms are either known or can be developed quite simply.

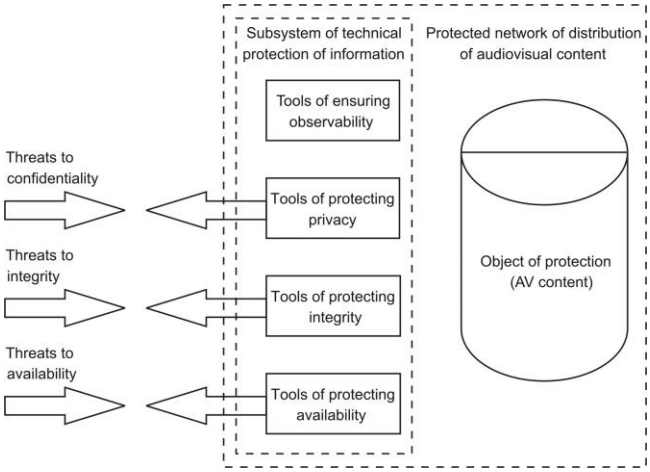

Fig. 1. Abstract model of technical content protection

Thus, there is a subsystem of technical protection of information, which provides protection against each of the types of specified threats with probability p_i, and includes tools of protecting confidentiality, tools of protecting integrity, and tools of protecting availability (Fig. 1) [6]. The subsystem performs its functions by periodically (with a period T_{ki}) monitoring the network's performance, which is formulated as its ability to provide its own functional service – observation, through the use of appropriate monitoring tools. We will assume that such control requires ΔT_{ki} time units. The frequency of control is determined by the owners of the protected resources, by any regulatory documents, or by the security administrator, and this control can be carried out at the start of the protection procedure. During the control, there is a check for violations of the network performance, its update, an audit of events related to information security, necessary reconfiguration of the parameters of the tools of ensuring the corresponding functional properties (for example, changing identifiers, passwords, key sets, with the help of which access control is ensured, necessary crypto- and impersonation resistance, etc.). The duration of control depends on the control methods implemented in the protection subsystem and the methods of their implementation [7, 20, 21]. Violations detected during control are eliminated. For this, it is possible to use various tools – the same backup copies, special fast-acting procedures (algorithms) for restoring integrity, etc. It is clear that the duration of the relevant procedures and the probability of correctly solving these problems depend on the quality of the applied methods and means of control and elimination of violations (resumption of working capacity).

In so doing, the overall goal of the functioning of the protection system is to minimize possible harm to the system or its owner by counteracting a variety of possible threats to the integrity, confidentiality and availability of network information resources.

In the mathematical formulation, this problem is reduced to the definition and optimization of the objective function, which describes the dependence of certain harm on the parameters of the protection system, the conditions for its application, and the characteristics of threats.

When determining the objective function, it should be assumed that the effects of these threats have certain frequency-time characteristics (for example, in the form of the probability of the occurrence of a threat during some average time interval). But for protection with information resources that are tempting for violators, it is appropriate to assume that such a probability is close to unity throughout the entire time of protection.

Each of the mentioned threats has as a consequence some damage to the content owner, if the corresponding protection system did not detect and counteract this damage. Let the probability of such an event be equal to $q_i = 1 - p_{di}$, where p_{di} is the probability of detection and subsequent countermeasures against the *i*-th type threat. It is clear that $p_{di} = p_{i1} p_{i2}$ is the probability for a threat of the *i*-th type, where p_{i2} is the probability of countering the same threat.

In this case, an undetected threat causes damage to the content $Q_i = F_i(1 - p_{di})$ owner per unit of time.

If we assume that the duration of the impact of the *i*-th threat is equal to T_{Di}, then the amount of damage can be determined as

$$Q_i = T_{Di} F_i (1 - p_{di}). \tag{1}$$

The duration of the impact of the threat T_{Di}, hence the duration of damage accumulation, is a random value in the time interval (0, $T_{ki} - \Delta T_{ki}$), where T_{ki} is the duration of time between two adjacent checks of the performance of the protection system against threats of the *i*-th type, and ΔT_{ki} is the duration of the *i*-th type of control and update of the functional properties of information security, for example, integrity (we believe that during control the system is inoperable and it is impossible to harm it by implementing any threats). It can be assumed that $T_{Di} = T_{ki} - \Delta T_{ki}$, if the violator managed to implement the threat immediately after the end of the corresponding control procedure, and $T_{Di} = 0$ in the case of an attempt to implement the threat immediately before its start. The worst conditions, in terms of the amount of possible damage, are created at $T_{Di} = T_{ki} - \Delta T_{ki}$, therefore, when developing a protection system, it is advisable to focus on this duration of the threat. At the same time, the maximum possible value of damage of the *i*-th type

$$Q_{i\max} = T_{Di}(T_{ki} - \Delta T_{ki}) F_i (1 - p_{di}) \tag{2}$$

Since the damage is additive in nature, the maximum amount of possible total damage (PTD) can be defined as

$$Q_{PTD1} = \sum_{i=1}^{i=n} Q_{i\max} = \sum_{i=1}^{i=n} (T_{ki} - \Delta T_{ki}) F_i (1 - p_{di}) \tag{3}$$

But (3) does not take into account the fact that during the performance control of the protection system for the duration ΔT_{ki} of time units, it is unable (especially in the case of detection of an attempt to influence with the probability of this event p_i) to perform its functions (at least in full), which is equivalent to damage, which occurs when the system is idle, since the implementation of the functional service "observability" and "maintenance" of attempts at such influence also requires spending a protection resource.

The amount of this damage can be defined as

$$Q_{PTD2} = \sum_{i=1}^{i=n} p_{di} \Delta T_{ki} C_i \tag{4}$$

where C_i is the damage due to downtime of the corresponding network resources during control, in conventional units per unit of time. Then

$$Q_{PTD} = Q_{PTD1} + Q_{PTD2} = \sum_{i=1}^{i=n} F_i (T_{ki} - \Delta T_{ki})(1 - p_{di}) + p_{di} C_i \Delta T_{ki} \tag{5}$$

It can be seen from expression (5) that it can be accepted as the target function of the protection system, since it reflects the dependence on the process and conditions of system operation. Indeed, the value of possible total damage (PTD) is the smaller, the smaller the number of threats *n*; the amount of damage C_i that can be caused by the successful implementation of each type of threat; control period T_{ki}; duration of the *i*-th type of control ΔT_{ki}; and the more is the probability of detecting and counteracting the threat of the *i*-th type p_{di}; size difference $T_{ki} - \Delta T_{ki}$.

Expression (5) is easily reduced to the form

$$Q_{PTD} = \sum_{i=1}^{i=n} F_i T_{ki} - \left\{ \sum_{i=1}^{i=n} F_i T_{ki} p_{di} - \sum_{i=1}^{i=n} \left[p_{di} C_i - F_i (1 - p_{di}) \right] \Delta T_{ki} \right\} \quad (6)$$

It is easy to make sure that the minuend, provided that the value of the frequency of control T_{ki} is not a control parameter, is equal to the maximum possible damage that can be caused to the network in the absence of counteraction to the impact of threats from the information security system.

Then it is clear that the value

$$Q_{PTDP} = \sum_{i=1}^{i=n} F_i T_{ki} p_{di} - \sum_{i=1}^{i=n} \left[p_{di} C_i - F_i (1 - p_{di}) \right] \Delta T_{ki} \quad (7)$$

is equal to the amount of damage that is eliminated (prevented) due to the protection of resources by the system. Therefore, this value can be applied as a separate objective function.

In expression (7), the value ΔT_{ki} consists of the duration of the control process (search for the fact of violation or non-violation of the corresponding functional property of information security) Δt_{ki} and the duration of the process of resuming the possibility of its provision.

For the sake of certainty, we will assume that now we are talking about ensuring the integrity of information. As already mentioned, control of the network's ability to provide the appropriate functional service, in this case – the integrity of information, can be carried out by applying some standard procedures (checking by tests, etc.). Let the characteristic of the control process be its duration Δt_{ki}. If a violation of integrity is detected during the control process, it is updated using, for example, backup copies of the relevant information. That is, the duration of the update is equal to zero, if a violation of the network's ability to provide one or the other of its functional properties, for example, integrity, is not detected during monitoring, or, if such a violation is detected, it is equal to the duration of the update process of the same functional property – Δt_{ni}. Characteristics of the update process – the duration of the update itself Δt_{ni} and the likelihood of its need p_{di} – the probability of detecting integrity violations. Then the expectation of the update duration is

$$\Delta t_{ni} p_{di} + 0 \cdot (1 - p_{di}) = \Delta t_{ni} p_{di} \quad (8)$$

That is, the duration of the entire control and update process is a random variable and is determined by the duration of the control process itself Δt_{ki} and the duration of the update Δt_{ni} with probability p_{di}. The average value of a quantity ΔT_{ki}, its mathematical expectation can be defined as

$$\Delta T_{ki} = \Delta t_{ki} + \Delta t_{ni} p_{di}. \quad (9)$$

Extending this to processes associated with threats of any type, the expression for calculating the value of harm to be prevented can be written as:

$$Q_{PTDPi} = F_i T_{ki} p_i - \left[p_i C_i - F_i (1 - p_i) \right] \left[\Delta t_{ki} + \Delta t_{ni} p_{ni} \right] \quad (10)$$

It is clear that the protection system is more effective the smaller the amount of damage (5) and the larger the amount of damage prevented (10). To do this, you should increase the value of the probability p_i and reduce the duration of the control procedure ΔT_{ki}. By the way, at $p_i = 1$ i.e. with a protection system that is absolutely reliable in terms of detecting and eliminating threats, the amount of damage that is prevented acquires a maximum value, which is equal to:

$$\max Q_{PTDP} = \sum_{i=1}^{i=n} F_i T_{ki} - \sum_{i=1}^{i=n} C_i \Delta T_{ki} \quad (11)$$

or

$$\max Q_{PTDP} = \sum_{i=1}^{i=n} F_i T_{ki} - \sum_{i=1}^{i=n} C_i \left[\Delta t_{ki} + \Delta t_{ni} p_{di} \right] \quad (12)$$

that is, it is equal to the maximum possible damage due to the successful implementation of threats, which is reduced by the amount of the maximum possible damage due to an idle network during control. It also follows from expressions (7), (10) that it is advisable to apply network protection against threats of any type only when the value of the damage to be prevented is not negative (is greater than zero). For threats of the *i*-th type, this means that

$$F_i T_{ki} p_i - \left[p_i C_i - F_i (1 - p_i) \right] \Delta T_{ki} > 0. \quad (13)$$

whence one can find the limit on the duration of control ΔT_{ki} (at a certain value p_i)

$$\Delta T_{ki} = \Delta t_{ki} + \Delta t_{ni} p_{di} < F_i T_{ki} p_{di} / \left[p_i C_i - F_i (1 - p_i) \right] \quad (14)$$

or on the probability p_{di} (taking into account that $\Delta T_{ki} < T_{ki}$)

$$p_{di} > \Delta T_{ki} / (T_{ki} - \Delta T_{ki}) - \Delta T_{ki} (C_i / F_i) \quad (15)$$

Since protection systems are used in practice, in which the value of the probability of detecting and further countering a threat of the *i*-th type approaches unity, expression (14) can be simplified.

$$\Delta T_{ki} = \Delta t_{ki} + \Delta t_{ni} p_{di} < T_{ki} (F_i / C_i) \quad (16)$$

It should be noted that the values ΔT_{ki} and p_{di} obtained from inequalities (10) – (16) are limited to those values when the application of control gives a gain that exceeds the losses of the network due to its downtime during control, that is, the system becomes efficient and its application is cost effective.

In other words, expressions (15), (16) are conditions for the expediency of using a system of protection against threats of this type.

3. Conclusions

1. The values of the probabilities should be chosen the greater, the more significant the losses in case of failure to detect the fact of a successful implementation of the threat compared to the losses due to network downtime during the control (the greater the value of the ratio F_i / C_i).

On the contrary, the more operative the control is (with a shorter duration of the control procedure Δt_{ki}, for example, integrity and a shorter duration of the further update procedure Δt_{ni}) the smaller this probability may be. Moreover, the more significant the losses due to failure to detect the fact of a successful implementation of the threat compared to the losses due to network downtime during monitoring (the greater the value of the ratio F_i / C_i) and the greater the values of the required or acceptable monitoring durations ΔT_{ki} and the probabilities of detecting and countering the threat of the *i*-th type p_{di}, the more perfect, and therefore, longer should be the control.

2. The considered generalized model makes it possible to obtain a number of conditions, restrictions and optimal values of the most general parameters of the protection system, which are most important for solving the problem of protecting audiovisual content, but do not allow formulating more specific requirements for the composition and parameters of the protection system or its components.

References

[1] Al-Mukaddim K. P., Rajkumar B.: A Taxonomy and Survey of Content Delivery Networks. Australia, 2007.
[2] Andreev V. I., Kozlov V. S., Horoshko V. A.: Kolychestvennaya otsenka zashishennosti tekhnicheskikh obektov s uchetom ikh funktsionirovaniya. Zakhyst informatsiyi 2, 2004, 47–51.
[3] Ayankoya F., Otushile O., Ohwo B.: A Review on Content Delivery Networks and Emerging Paradigms. International Journal of Scientific & Engineering Research 9, 2018, 211–217.
[4] Bohush V. M., Kudin A. M.: Monitorynh system informatsiinoi bezpeky. DUIKT, Kyiv 2006.
[5] Charles D. C. et al.: Enhanced Streaming Services in a Content Distribution Network. IEEE Computing Society, 2001, 66–75.
[6] Dmitrenko A. P., Sirchenko G. A., Horoshko V. A.: Modeli bezopasnogo soedineniya s udalennymi obektami. Zakhyst informatsiyi 1, 2010, 53–57.
[7] Dmitrenko A.P., Sirchenko G.A., Horoshko V.A.: Statisticheskoe modelirovanie dlya ocenki zashhishhennosti lokalnoj seti. Visnyk DUIKT 1, 2010, 62–67.
[8] Ingmar P. et al.: Improving Content Delivery with Provider-aided Distance Information System (PaDIS). IEEE Computer Society, 2012, 44–52.
[9] Jaeyeon J., Balachander K., Rabinovich M.: Flash crowds and denial of service attacks: Characterization and implications for CDNs and Web sites. 11th International World Wide Web Conference Hawaii: ACM, 2002, 293–304.
[10] Kirichek R., Kulik V., Koucheryavy A.: False clouds for Internet of Things and methods of protection. 18th International Conference on Advanced Communication Technology, Pyeongchang, South Korea 2016, 201–205.
[11] Moroz S. et al.: Methods for ensuring data security in mobile standards. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS, 1, 2022, 4–9 [http://doi.org/10.35784/iapgos.2877].
[12] Nikolaienko B., Vasylenko S.: Application of the threat intelligence platform to increase the security of government information resources. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS 4, 2021, 9–13 [http://doi.org/10.35784/iapgos.2822].
[13] Politanskyi R., Politanskyi L., Hres O., Lesinskyi V. Statistical estimation of pseudorandom number sequences. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018, 873–876.
[14] Rusyn V. et al.: Computer Modelling of the Information Properties of Hyper Chaotic Lorenz System and Its Application in Secure Communication System. Journal of Physics: Conference Series 1764, 2021, 012205 [http://doi.org/10.1088/1742-6596/1764/1/012205].
[15] Rusyn V., Sambas A., Mujiarto: Information security system based on chaotic signals. CEUR Workshop Proceedings 3039, 2021, 294–299.
[16] Rusyn V., Subbotin S., Sambas A.: Simple autonomous security system based on Arduino UNO platform and fingerprint scanner module: A study case. CEUR Workshop Proceedings 2864, 2021, 262–271.
[17] Shirochin V. P., Muhin V. E., Kramar D. I.: Analiz riskov v zadachah monitoringa bezopasnosti kompyuternyh sistem i setej. Zakhyst informatsii 1, 2003, 28–34.
[18] Shoroshev V. V., Ilnytskyi A. Yu.: Informatsiino-analitychna model bazovoho pervynnoho zakhystu PEOM vid zahroz NSD. Byznes y bezopasnost 3–5, 1999, 32–39.
[19] Shushura O. M. et al.: Simulation of information security risks of availability of project documents based on fuzzy logic. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS 3, 2022, 64–68 [http://doi.org/10.35784/iapgos.3033].
[20] Sirchenko H. A.: Zadachi zabezpechennia tsilisnosti ta dostupnosti informatsiinykh obiektiv v komunikatsiinykh merezhakh. Zakhyst informatsii 2, 2010, 49–54.
[21] Vasilenko V. S., Korolenko M. P.: Celostnost informacii v avtomatizirovannyh sistemah. Korporativnye sistemy 3, 1999, 52–58.
[22] Vyshnivskyi V. V., Sribna I. M., Zinchenko O. V.: Analysis of technical solutions for identification of internet things in modern communication networks. Electronics and Control Systems 1, 2021, 33–39 [http://doi.org/10.18372/1990-5548.67.15583].

D.Sc. Heorhii Rozorinov
e-mail: grozoryn@gmail.com

National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute" Department of Acoustic Multimedia Electronic Systems. D.Sc. (Engineering Sciences) Professor of Department of Audiotechnic and Information Registration.
Research interests: pseudorandom sequence generators; encryption information, acoustics.
Author of nearly 135 publications.

http://orcid.org/0000-0002-6095-7539

Ph.D. Oleksandr Hres
e-mail: o.hres@chnu.edu.ua

Yuriy Fedkovych Chernivtsi National University Department of Radio Engineering and Information Security. Ph.D. (Engineering Sciences) Assistant Professor of Department of Radio Engineering and Information Security.
Research interests: pseudorandom sequence generators; encryption information. Author of nearly 42 publications.

http://orcid.org/0000-0002-8465-193X

Ph.D. Volodymyr Rusyn
e-mail: rusyn_v@ukr.net

Yuriy Fedkovych Chernivtsi National University Department of Radio Engineering and Information Security. Ph.D. (Engineering Sciences) Assistant Professor of Department of Radio Engineering and Information Security.
Research interests: modeling of nonlinear equations and chaotic generators; control of chaotic oscillations. Author of nearly 85 publications.

http://orcid.org/0000-0001-6219-1031