Oleksandr MILOV[1], Stanislav MILEVSKYI[2], Volodymyr ALEKSIYEV[3]

CREATION OF A METHODOLOGY FOR BUILDING SECURITY SYSTEMS FOR MULTIMEDIA INFORMATION RESOURCES IN SOCIAL NETWORKS

Summary: The report presents an approach to the creation of a methodology for building security systems for the exchange of multimedia content in social networks through the development of conceptual foundations, methods and technologies for detecting, assessing and countering information security threats.

Keywords: cybersecurity, social networks, multimedia content, threats classifier

OPRACOWANIE METODOLOGII TWORZENIA SYSTEMÓW BEZPIECZEŃSTWA DLA ZASOBÓW INFORMACJI MULTIMEDIALNYCH W SIECIACH SPOŁECZNOŚCIOWYCH

Streszczenie: W artykule omówiono ideę metodologii budowy system bezpieczeństwa dla wymiany zasobów multimedialnych w sieciach społecznościowych. Elementami takiej ogólnej metodologii są podstawy konceptualne, odpowiednie metody oraz technologie do wykrywania, oceny oraz przeciwdziałania zagrożeniom bezpiecznego przesyłu informacji.

Słowa kluczowe: cyberbezpieczeństwo, sieci społecznościowe, zawartość zasobów multimedialnych, klasyfikator zagrożeń

1. Introduction

The constant improvement of the communication and information environment has turned social networks into the dominant segment of information exchange and communication of citizens in the virtual space. Modern means of supporting the functioning of social networks are constantly improving means of forming and exchanging content of various types, which in the final form are an integral part of

[1] Prof., PhD, Simon Kuznets Kharkiv National University of Economics, Professor of Department of Cyber Security and Information Technology oleksandr.milov@hneu.net

[2] Associate Prof., PhD, Simon Kuznets Kharkiv National University of Economics, Associate Professor of Department of Cyber Security and Information Technology stanislav.milevskiy@hneu.net

[3] Prof., PhD, Simon Kuznets Kharkiv National University of Economics, Professor of Department of Cyber Security and Information Technology aleksiyev@gmail.com

not only the national, but also the global information space.

The popularity of personal digital cameras and online communities for photo / video sharing has led to an explosion in the amount of multimedia information that circulates on social media. In contrast to text information, for the processing of which there are a huge number of tools and methods, ranging from content analysis to text-mining, allowing to structure, annotate, extract knowledge from unstructured data, determine the semantic proximity of texts [1]. For processing multimedia data (audio, video, graphics) such a variety of tools and methods is not observed. Although it should be noted that unlike traditional multimedia data, many new multimedia data sets are organized in a structured manner, including rich information such as semantic ontology, social interaction, social media, geographic maps, in addition to multimedia content. Research on such structured multimedia data has led to the emergence of a new area of research called multimedia information networks [2]. Multimedia information networks are closely related to social networks, but primarily focused on understanding the themes and semantics of multimedia files in the context of the network structure.

In parallel with the increase in the volume of generated, stored and transmitted multimedia information in social networks, the number and variety of attacks carried out on information resources of the multimedia type is increasing. Such attacks have features associated with the fact that multimedia information networks have not yet been formed, have turned into a source of threats to the information security of both individual citizens and the state as a whole. As a result of the dissemination of inaccurate, incomplete or biased content in combination with the technologies of information and psychological impact on the individual, collective and mass consciousness in society, manifestations of national and religious enmity, calls for a violent change of the constitutional order or violation of the sovereignty and territorial integrity of the state may take place [3, 4].

2. Literature survey

Analysis of publications devoted to ensuring the security of the functioning of social networks, countering attacks on information resources and, first of all, of multimedia type, showed that at the present stage of development of information technologies, there is a contradiction between the need to increase the level of information security of the functioning of social networks and the imperfection of the multimedia content files control system . The consequence of this is the lack of a methodology for constructing security systems for multimedia information resources in social networks. Given the complex nature of security threats in the information sphere, the role of social networks in the formation and development of civil society, the problem of developing effective approaches to building a system for ensuring information security of social networks in the context of globalization and free circulation of information is especially urgent [5].

The analysis also showed that today there is still no scientifically grounded methodology for assessing the most likely threats to information security, based on economic estimates of the cost of an attack and the damage caused. Therefore, a radical revision of the existing methodologies for building security systems for multimedia information resources in social networks is required.

3. Research materials

The basic assumption of the proposed methodology for constructing a security system for social networks with multimedia content is the assumption about the influence of the behavior of both individual members of a social network and the behavior of the entire social network community in the process of posting, searching, accessing and using multimedia content of social networks.

However, the theory lacks a holistic, scientifically grounded methodology for modeling the behavior of individual members of a social network and the network as a whole, which is due to the complexity of the modeling object and the lack of appropriate methods and tools for modeling such complex processes as the behavior of individual elements of a social network and the network as a whole.

In modern conditions, practice requires the theory to search for new approaches to ensuring protection against threats in all components of security: cybersecurity, information security and information security in the context of hybridity and synergy of modern threats [6].

To develop a methodology for constructing security systems for multimedia information resources in social networks, the concept of modeling the behavior of members of a social network is proposed, which is implemented at three levels.

At the first level, an element of a social network (agent or actor) is determined, the behavior of which forms the behavior of the social network as a whole, and is decisive for the study and construction of a security system. At this level:

1. A set of actions of an individual element of a social network is determined, which together form behavior.
2. The probabilities of the implementation of certain actions are determined.
3. Information multimedia resources associated with a particular action are determined.
4. Possible attacks aimed at the corresponding information resources are determined.
5. Cost indicators of the corresponding information resources are determined.

At the second level, models of collective behavior (group dynamics) are built. At this level:

1. Models of influence in the group are determined.
2. The dynamic characteristics of the group's behavior are determined – stability, coordination of actions, self-organization of the group, temporal characteristics of the dynamics of behavior.
3. Characteristics of openness, isolation or closedness of the group are determined.

At the third level, threats are identified that are directed at the platform of the functioning of the social network as a whole. At this level:

1. A classifier of threats specific to social networks and their multimedia content is formed (or modified).

The formed complex of tasks, separated by levels, makes it possible to form an economically grounded methodology for constructing a security system for multimedia information resources of social networks (Fig. 1).

The methodology construction process consists of 5 stages:

1. Analysis of a social network and possible attacks on it.
2. Analysis of a social network and possible attacks on it.

3. Development of models of the social network group level.
4. Development of platform-level models for the functioning of a social network.
5. Development of methods for determining the most likely threats and assessment of their cost indicators.

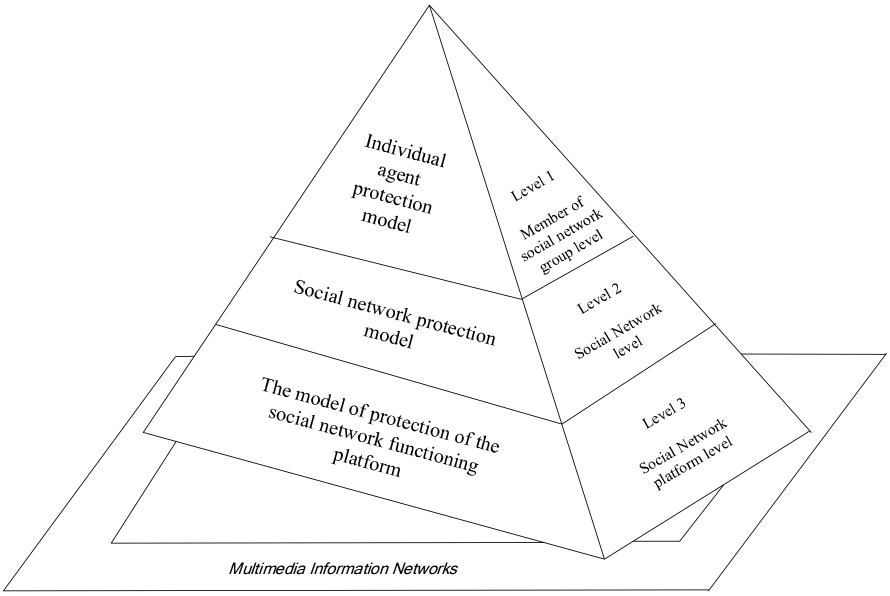
Individual agent protection model
Level 1
Member of social network group level
Social network protection model
Level 2
Social Network level
The model of protection of the social network functioning platform
Level 3
Social Network platform level
Multimedia Information Networks

Figure 1. Levels of the concept of forming a methodology for building a security system

The analysis of a social network and possible attacks on it should start with improving the threat classifier [7]. It is proposed to introduce a new platform into the threat classifier - the platform of cost indicators of attacks. This will make it possible to assess threats from the point of view of economic efficiency of their implementation and counteraction to them (Fig. 2).

In the threat classifier, which was used as a basic one, 4 platforms were implemented, namely.

The first platform is the classification of threats according to the components of the security circuit: information security (IS) (01), security of information (SI) (02), cybersecurity (CS) (03).

The second platform is classification of threats by the nature of orientation: regulatory (01), organizational (02), engineering (03).

The third platform – classification of threats according to the main features of information: confidentiality (01), integrity (02), accessibility (03), authenticity (04).

The fourth platform - classification of threats by business processes contou rinfrastructure hierarchy levels: FL - physical level (01), NL - network level (02), OSL - operating systems-level (OS) (03), DBL - level of management systems of databases (04), BL - level of technological applications and services (05).

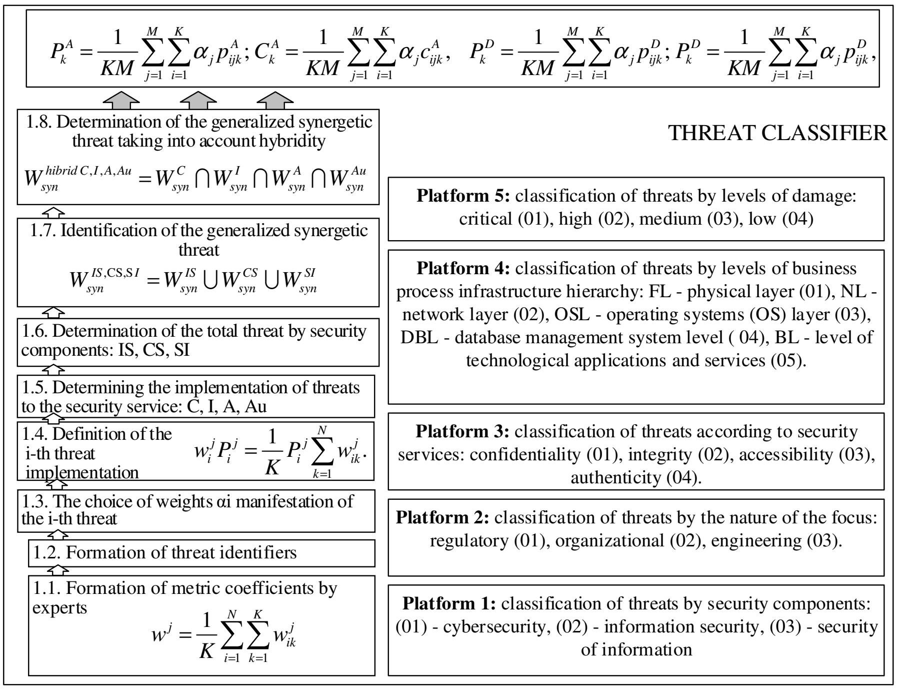
$P_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^A;\ C_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^A,\ P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D;\ P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D,$
THREAT CLASSIFIER
1.8. Determination of the generalized synergetic threat taking into account hybridity
$W_{syn}^{hibrid\,C,I,A,Au} = W_{syn}^C \cap W_{syn}^I \cap W_{syn}^A \cap W_{syn}^{Au}$
1.7. Identification of the generalized synergetic threat
$W_{syn}^{IS,CS,SI} = W_{syn}^{IS} \cup W_{syn}^{CS} \cup W_{syn}^{SI}$
1.6. Determination of the total threat by security components: IS, CS, SI
1.5. Determining the implementation of threats to the security service: C, I, A, Au
1.4. Definition of the i-th threat implementation
$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j.$
1.3. The choice of weights αi manifestation of the i-th threat
1.2. Formation of threat identifiers
1.1. Formation of metric coefficients by experts
$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$
Platform 5: classification of threats by levels of damage: critical (01), high (02), medium (03), low (04)
Platform 4: classification of threats by levels of business process infrastructure hierarchy: FL - physical layer (01), NL - network layer (02), OSL - operating systems (OS) layer (03), DBL - database management system level (04), BL - level of technological applications and services (05).
Platform 3: classification of threats according to security services: confidentiality (01), integrity (02), accessibility (03), authenticity (04).
Platform 2: classification of threats by the nature of the focus: regulatory (01), organizational (02), engineering (03).
Platform 1: classification of threats by security components: (01) - cybersecurity, (02) - information security, (03) - security of information

Figure 2. Platforms of the classifier of threats and the formation of their characteristics

The analysis of the classifier of existing threats allowed to formulate the relationship between hybridity and synergy of threats depending on their type and direction. A platform for cost indicators of attacks has been introduced into the threat classifier, which allows assessing threats to the economic efficiency of their use and counteraction to them. The scale of measuring the value of losses for expert evaluation proposed in the form of: {*insignificant, low, medium, high, critical*}. Let's assign: *i* current threat number $(\{i\}_1^N)$, *k* – the current number of the expert who performed the assessment $(\{k\}_1^K)$. The average value of the assessment of the cost of losses by experts for all threats to a specific contour of business processes can be recorded as:

$$P_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^A;\ C_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^A,$$

$$P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D;\ P_k^D = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^D,$$

where K – number of experts, M – the number of business transactions that may be targeted, α_j – the criticality ratio of the business process to which the relevant business transaction belongs.

The fifth platform has been introduced into the classifier of threats aimed at information resources of the multimedia plan of social networks.

The fifth platform is the classification of threats by the cost of their protection and implementation: (01) – insignificant, (02) – small, (03) – medium cost, (04) – large and (05) – significant cost. These indicators refer to both the cost of protection and the cost of realizing the threat.

The use of the proposed classifier is implemented as a sequence of next steps.

Step 1. Formation of metric coefficients of threats by experts.

We estimate the weights of each of the N threats presented in the classifier. K experts take part in determining the weights of each threat to the information resources of the social network. In addition, to determine the possible harm, each threat is classified according to the criterion of critical damage to the social network as a whole.

According to the ISO / IEC15408 standard, experts choose the quality level of damage: critical, high, medium, low. With the help of CRAMM or FAIR risk assessment methods, it is possible to assess the qualitative level in quantitative terms. Thus, at the first stage, the weights of the metric of modern hybrid cyber threats are formed, which allows to use them within the SIEM (Security Information and Event Management) system in order to simplify the audit and correlation of information from different sources.

Denote by *i* current threat number $(\{i\}_1^N)$, as *k* – the current number of the expert who performed the assessment $(\{k\}_1^K)$. The average value of the expert assessment of all threats to a particular security service can be recorded as:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j \ , \qquad (1)$$

where w_{ik}^j – the value of the metric coefficient set by *k*-th expert for *i*-th threat for *j*-th information resource of the social network; *N* – number of threats; *K* – number of experts.

Step 2. Formation of threat identifiers by components of the classifier. In this step, the experts generate a digital value (code) of the threat identifier for the relevant components of the classifier.

Step 3. Selection of weights α_i, determining the conditions of display of *i*-th threat (table 1) [5].

Table 1. Table of weights α_i selection of i-th threat depending on the condition of its manifestation

Weights α_i	Terms of threat
0,067	the threat appears no more than once every 5 years
0,133	the threat appears no more than once a year
0,2	the threat appears no more than once a month
0,267	the threat appears no more than once a week
0,333	the threat is manifested daily

Step 4. Determining the implementation of each *i*-th threat, taking into account the probability of an attack (its occurrence) is carried out by expression:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j . \qquad (2)$$

where w_i^j – expert weights.

Improving the threat classifier through the introduction of cost indicators of threats allows to implement an algorithm for building a rating of potential threats and the importance of information resources to be protected.

Step 5. Determining the summary threat by security components:

$$W_{synerg}^{IB} = \sum_{i=1}^{N} \left(w_i^R \cap w_i^P \cap w_i^T \cap w_i^I \right) \alpha_i ,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N} \left(w_i^R \cap w_i^P \cap w_i^T \cap w_i^I \right) \alpha_i ,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^R \cap w_i^P \cap w_i^T \cap w_i^I \right) \alpha_i . \qquad (3)$$

Step 6. Determining the generalized synergetic threat:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} . \qquad (4)$$

Step 7. Determination of the generalized synergetic threat taking into account its hybridity is calculated as:

$$W_{synerg}^{\text{hybrid } R,P,T,I} = W_{synerg}^{R} \cap W_{synerg}^{P} \cap W_{synerg}^{T} \cap W_{synerg}^{I} . \qquad (5)$$

4. Conclusions

Creating a methodology for building security systems for information resources in social networks is a complex problem, the difficulties of which are explained by the following reasons.

1. All types of activities to ensure the security of resources in social networks are fundamentally multidisciplinary cooperative and highly dynamic. Separate consideration of security issues can lead to attempts to address them in one area that can lead to a sharp increase in tensions in another. To resolve this contradiction, qualitatively new ways of comprehensive research and forecasting the results of actions are needed.
2. Stochasticity and uncertainty permeate all levels of society and lead to ambiguous reflection of ongoing processes in the minds of people and, consequently, to subjective and irrational reactions to changes in the world around them.
3. The organization of a social network as a reflection of the organization of society as a whole is largely a consequence of the manifestation of subjective interests of both the individuals and their groups.

REFERENCES

1. MOLODETSKA-HRYNCHUK K. V.: Identification of information influences in social Internet services based on intellectual analysis of textual content", III International. scientific-practical conf. Current issues of cybersecurity and information security, Kyiv, 2017, p. 120–121.
2. Social Network Data Analytics - Charu C. Aggarwal (eds.). Springer Science+Business Media, LLC. 2011. – 500 p.
3. MOLODETSKA K. V.: Threats to information security of the state in social Internet services, International. scientific-practical conf. Information Security and Computer Technologies, Kirovograd, 2016, p. 55.
4. HRYSHCHUK R. V., MOLODETSKA-HRYNCHUK K. V.: Statement of the problem of ensuring information security of the state in social Internet services, Modern information protection, 3(2017)31, 86–96.
5. MILOV O., YEVSEIEV S.: Methodology of modeling the behavior processes of antagonistic agents in security systems. Ukrainian Scientific Journal of Information Security, 25(2019)3, 150-161.
6. MILOV O., KAZAKOVA N., MILCZARSKI P., KOROL O.: Mechanisms of cyber security: the problem of conceptualization. Ukrainian Scientific Journal of Information Security, 25(2019)2, 110-116.
7. YEVSEIEV S.: Classifier of cyberthreats of information resources of automated banking systems, Cybersecurity: education, science, technology, 2(2018)2, 47-67.