Network Security Analysis Based on Consolidated Threat Resources

Oleg Garasym[0000-0001-6787-6937]1, Liliya Chyrun[0000-0003-4040-7588]2, Nadija Chernovol[0000-0001-9921-9077]3, Aleksandr Gozhyj[0000-0002-3517-580X]4, Victor Gozhyj[5], Irina Kalinina[0000-0001-8359-2045]6, Bohdan Rusyn[0000-0001-8654-2270]7, Liubomyr Pohreliuk[0000-0003-1482-5532]8, Maksym Korobchynskyi[0000-0001-8049-4730]9

[1]Volvo IT, Wrocław, Poland
[2-3]Lviv Polytechnic National University, Lviv, Ukraine
[4-6]Petro Mohila Black Sea National University, Nikolaev, Ukraine
[7-8]Karpenko Physico-Mechanical Institute of the NAS Ukraine
[9]Military-Diplomatic Academy named after Eugene Bereznyak, Kyiv, Ukraine

garasym-oleg@rambler.ru[1], lchirun21@gmail.com[2], nadija.m.chernovol@lpnu.ua[3], alex.gozhyj@gmail.com[4], gozhyi.v@gmail.com[5], irina.kalinina1612@gmail.com[6], rusyn@ipm.lviv.ua[7], liubomyr@inoxoft.com[8], maks_kor@ukr.net[9]

Abstract. The security of the network using the consolidated threat resources that have been identified and registered in the database is analyzed in the paper. A threat analysis chart has been compiled and the risks of their spread on the network are estimated, and weaknesses in the network have been identified.

Keywords - threat, network, risk, consolidation, e-governance, crypto algorithm, choice optimization

1 Introduction

The activities of any company or government agency are closely linked to the use of communications information networks, which are built using electronic technologies for the transmission, storage, processing, and use of corporate information [1-4]. The reliable functioning of these systems directly affects the economic activity and financial condition of the corporation [5-9]. Corporate governance along with financial risks should also take into account those related to the information systems use. Therefore, in order to manage the risks, the information of the accounting system should be consolidated and all events that cause losses should be consolidated, the probabilities of their occurrence, the risks of spreading, the ways of their prevention should be determined. This task is extremely important in modern corporate activity; its solution is of paramount importance. The corporate network information security management system (NISMS) is related to the various factors influence of activity of the network users and is the basis of economic stability and maintaining a high level

of corporate security. To protect corporate information, especially confidential information, administrators need to make timely and informed management decisions while processing consolidated information about threats and network weaknesses [10-16]. Consolidated corporate network security information allows you to obtain comprehensive network status information and effectively monitor events, identify attacks, faults and vulnerabilities, and isolate corporate information security threats. Based on the consolidated information, diagnostics, control and adaptation of information security management, direct security control are carried out. Adaptation of information security management is necessary to meet the desired results, despite changing corporate governance goals, technological conditions, or expanding corporate operations. Based on the consolidated information [1-2, 17-21], the network vulnerability assessment and prevention of possible intrusions are created, the corporate information security management strategy [3-4, 22-29] is adjusted accordingly, the methods and data protection methods are determined, and the appropriate decisions are made to identify hidden information threats.

2 Relate the highlighted issue to important practical and scientific work

The classification of functional elements of network security and the categorization of network security technologies of basic functional elements provide the basis for a structured approach to the study of heterogeneous technologies that are rapidly evolving [30-35]. An organized, hierarchical view is used to represent all traditional, modern and emerging network security technologies. Fig. 1 shows a structure that reflects an organized, hierarchical view of the technology of functioning of corporate communications information security systems [5-6].

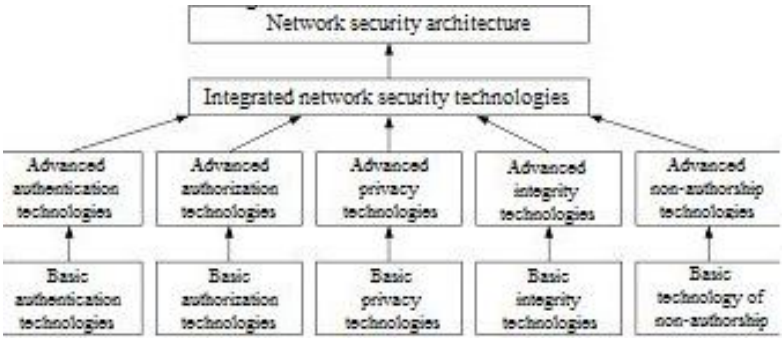

Fig. 1. Architecture of technologies of functioning of systems of protection of information of corporate communication networks

In order to maintain such architecture, the corporate communications information security system should be operated using consolidated security resources that arise throughout the system to prevent network attacks from progressing. By collecting all

the data from each security technology into a single consolidated resource, it is possible to identify the weaknesses of the security system and accordingly take timely measures to enhance the security of vulnerable sites and be able to predict events.

The resultant task of network security is to secure the application systems and information used at the input and generated at the output. As a result, you can identify the basic functional elements of a corporate network security that are necessary to build and operate a NISMS [36-42]:

- Confidentiality,
- Authentication,
- Authorization,
- The integrity of the message and the inability to opt out of authorship / receive the message [7-8].

These functional corporate network security elements are used in both hardware and software execution on network devices (switches, servers, etc.) within the path defined by the two endpoints of the communication connection (preferably a client PC or terminal and server) [9-10]. It is important to note that not all of these functional elements are always contained in separate elements of a corporate network security system. In addition, there are network security services that are difficult to attribute to these functional elements, but that work together with them to provide the desired network security capabilities [11-12]. The relevance of theme is due to the need for constant monitoring of network security and effective response to factors that disrupt the network [43-51]. For information security management, consolidation of data on threats that negatively affect the state of the network is a prerequisite for work. This approach provides an opportunity to solve management problems: forecasting damage from threats, identifying weak links of information protection and, accordingly, contributes to the creation of projects of management decisions to improve the protection system [52-59]. Consolidated threat accounting resources are created not only for operational and current management, but also for the purpose of making long-term decisions and predicting malicious actions of attackers. The aim of the work is to substantiate the theoretical concept of consolidation of data on threats of the corporate communication network and integration of the results into the information security management system based on the analysis of consolidated resources, effective planning, control and decision-making by the information security management system. To achieve the goal, the following tasks were set:

- To identify threats to the network;
- Determine the activities of the NISMS;
- To carry out the consolidation of identified threats;
- Assess the risks of proliferation and impact of threats;
- Research of weak links of a network.

3 Recent research and publications analysis

Consolidated information is obtained from multiple sources and systematically integrated multifaceted information resources, which are collectively endowed with the features of integrity, completeness, consistency and constitute an adequate information problem area model for its processing, analysis and effective use in decision support processes. A corporate communications network management system must have procedures in place to monitor and monitor the quality of its work. These procedures determine the compliance of the corporate network with the strategic plan of the corporation and the analysis of the impact of specific risks on its overall activity. In particular, they include checking the functions of electronic channels of information delivery, their compliance with the strategic plan of activity; the ability of electronic tools to process the intended amount of information [13-14].

The management system procedures determine whether the corporation's management and responsible units receive the information they need and examine the functioning of each electronic system implemented, analyze it, including:

- Determining whether various aspects of the functioning of electronic systems are taken into account, including analysis of critical cases, failures;
- Definition for each electronic system that cooperates with the main operating system of the corporation, databases their compatibility and security;
- Verification of the accuracy and intelligence of scheduling software, calculations, etc. available through the communications network;
- Determining whether a duplicate system is in place for users in the event that e-services systems do not operate for an extended period;
- Check for the developed procedures existence for notification of the management of the management system in case of technical problems of the network;
- Checking for the distribution of physical access to computer equipment, software, communications equipment and communication lines with clearly identified personnel, depending on their functions and positions within the corporation [10].

The organization of the corporation's activities must be tailored to the conditions of use of electronic means, so incompetence of management or imperfect technology used can affect the economic condition of the institution. Also, an existing organization of activities may not provide sufficient protection for sensitive electronic information. Existing procedures and procedures may not take into account the speed of transactions and the extended reach of electronic channels that transmit corporate information. Therefore, the management system includes:

1. Observation of operating procedures and procedures, which is to determine their suitability in the conditions of use of electronic channels of information transmission. Determines whether the applicable work organization procedures for the applicable personnel meet the requirements of implementation in new corporate products and services; how electronic technologies affect information transmission channels. A corporation must have a proper security system that includes the following elements:

- Control access and protection of confidential information of clients;
- The methods for determining the right of request of each participant in electronic data transmission systems;
- Highlighting information that may be accessible to third parties.

2. Determination of the ability to improve procedures and procedures in accordance with the use of electronic technologies to ensure access and change of confidential information:
- What information and how it is allowed to be transmitted to third parties;
- Whether confidential information is part of contracts and agreements with third parties that are hired by the corporation.

3. Determining the existence of mandatory authorization procedures. The presence of protection of tracking and prevention of duplicate transactions in each electronic system is confirmed. The quality of client training regarding security and safety when using electronic corporate systems is checked. Periodically, according to the established schedule, the entire spectrum of transactional corporate capabilities is checked, the resources of activity of each segment of the secure corporate communication network are consolidated, the operational procedures and procedures for conducting transactions and compliance with the requirements of protection and security of corporate information [15].

Effective management of information security requires understanding of network attacks. As a rule, attacks are carried out in several steps.

The first is research or network intelligence. The attacker collects information about the use of the target database and documents, the availability of monitoring tools for the corporate network. Then the attacker tries to identify vulnerabilities in the hardware, software or organizational information security, continues additional research and looks for a tool that can disrupt the work. Attack detection systems classify scans as low threat because they do not harm servers or corporation activity.
Scanning is a prerequisite for attacks. If the port is found open or unsecured, then the attacker usually goes into the pre-attack phase. Some services and applications are targets for attack. Despite the use of security technology, network administrators must address the challenge of protecting systems from malicious attacks and accidental failures. One method called intelligence is used by hackers to select networks and domains to search for targets. Intelligence allows a hacker to identify targets for attack or use them for attack [16].

4 Statement of a problem

The assessment of the risks associated with a breach of protection must identify, quantify and decide on their prevention. The results should guide and determine the appropriate management action and the risk management priorities associated with the breach of information security, as well as the implementation priorities of the selected management tools, to protect against these risks. The risk assessment and management selection process can be performed several times to cover different parts of the organization or individual NISMS.

The risk assessment should include a systematic assessing the magnitude method for the risks (risk analysis) and a process of comparing the predicted risks against the risk criteria in order to determine the significance of the risks. Risk assessments should also be undertaken periodically to take account of changes in security requirements and risk situations, such as assets, threats, weaknesses, negative impacts, risk assessment, and when significant changes occur. These risk assessments should be carried out in a methodological manner capable of producing comparisons and reproducible results. The assessment of risks associated with a breach of information security should have a clearly defined scope in order to be effective, and should include a linkage to risk assessments in other areas, where appropriate. In accordance with the requirements of ISO / IEC 27002: 2007, which defines the basic directions and general principles of development, implementation, support and improvement of management of information security of the organization, we will present the diagram of analysis of threats to the corporation network (Fig. 2) for their consolidation and definition information security management strategies (Fig. 3).

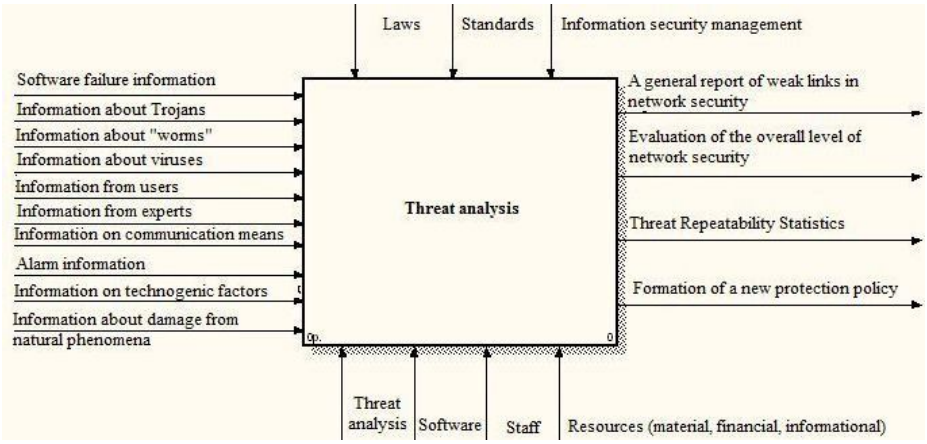

Fig. 2. Network Threat Analysis Chart

Monitoring the use of corporate electronic information systems, in particular their technical components, is an extremely important factor in ensuring the reliability and efficiency of modern corporation activities. Electronic systems monitoring data, consolidation of primary data in the areas we define is one of the main sources of information for management decisions and risk management programs in corporate activities. The source [13] presents the stages of risk analysis and forecasting:

In the general case, the average over a certain period of time the combined risk of a dangerous event A can be calculated by the formula:

$$R(A)=P(A)Y(A), \tag{1}$$

where $P(A)$ is a statistical probability of event A (or event risk), $Y(A)$ is a one-time loss is possible (or, if $P(A) = 1$, cost risk). In turn, the event risk is equal:

$$P(A) = \frac{v(t)}{T}, \tag{2}$$

where $v(t)$ is the number of occurrences of events of A over time t; T is the observation period.

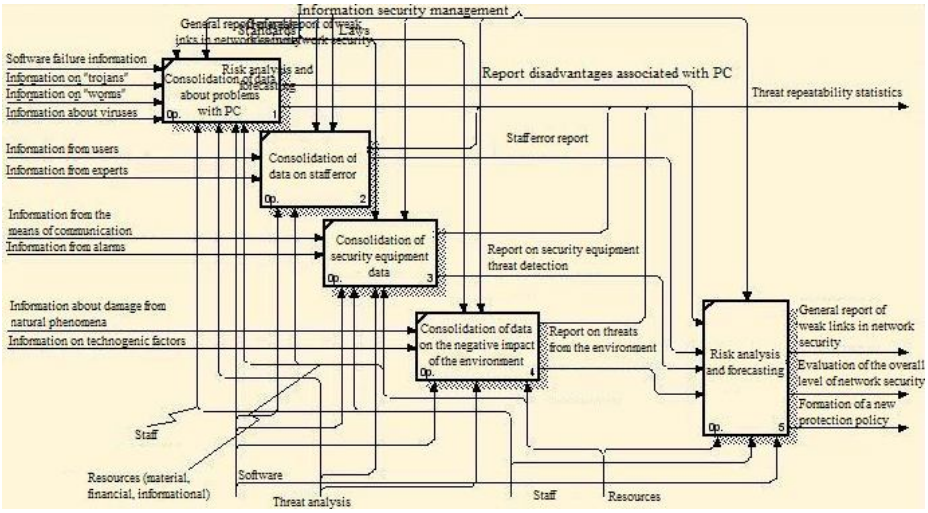

Fig. 3. Control elements of the threat analysis process

That is, the physical content of $R(A)$ is the number or cost of risk during the element study period. We introduce a new characteristic - the degree of vulnerability to the impact of event A:

$$C_y(A) = \frac{M_t}{M_a}, \tag{3}$$

where M_t is a number of affected elements, M_a is a total number of items, the total number of items that were in the affected area. Then a possible one-time loss $Y(A)$ can be determined by the following formula:

$$Y(A) = C_y(A) Y_n(A), \tag{4}$$

where $Y_n(A)$ is a conditional total loss, which is numerically equal to the number or value of all elements of the computer technology (or all elements that are in the area of damage). Thus, taking into account expression (2) and (4), formula (1) becomes:

$$R(A) = \frac{v(t)}{T} |_A \, C_y(A) Y_n(A). \tag{5}$$

This is a general formula for calculating risk. When considering the partial risks inherent in a particular type of network threat element (viruses, malware, trojans,

worms), the necessary modifications should be made. Then this formula looks like this:

$$R_f(A) = \frac{v(t)}{T}|_A \, P(H)C_c(A)H\,, \tag{6}$$

where $R_f(A)$ is a partial risk, P(H) is a probability of being of elements of a certain type in the affected area, H is their number, $C_c(A)$ is a degree of affection of this group of elements.

5 Analysis of the results

Consolidation of network threats was carried out at ISN department. The study period covers 18 days. The network consists of 3 computers on which 5 software products are installed. During the study, the following threats were identified:

- 18 computers (network 5);
- unauthorized access to information - 3;
- malicious intent or mistakes of staff - 5;
- external threats - 2.

A program for assessing the risks of threats (Fig. 4) was written, using formulas 1-6.

- Four events (problems) were investigated:
- Event I (technique) - failure, malfunctions, failures;
- Event II (Interception / access to information) - Interception of information or obtained in a sociotechnical way;
- Event III (malicious intent of the staff) - intentional or incorrect handling of information;
- Event IV (technogenic threat) is a negative impact of the environment.

The results are listed in the table (Fig. 4), where R is the average risk of an event; C is a degree of damage to the network elements; R_o is simultaneous losses; C_a is a partial degree of equipment damage; C_p is a partial degree of software vulnerability; R_a is a partial risk of an event for the hardware; R_p is a partial risk from event for the software.

As a result of calculations by formulas (1-6) the following results are obtained:

1. Average risks:
   (a) I event = 3.18
   (b) II event = 0.54
   (c) 3rd event = 0.9
   (d) IV event = 0.36

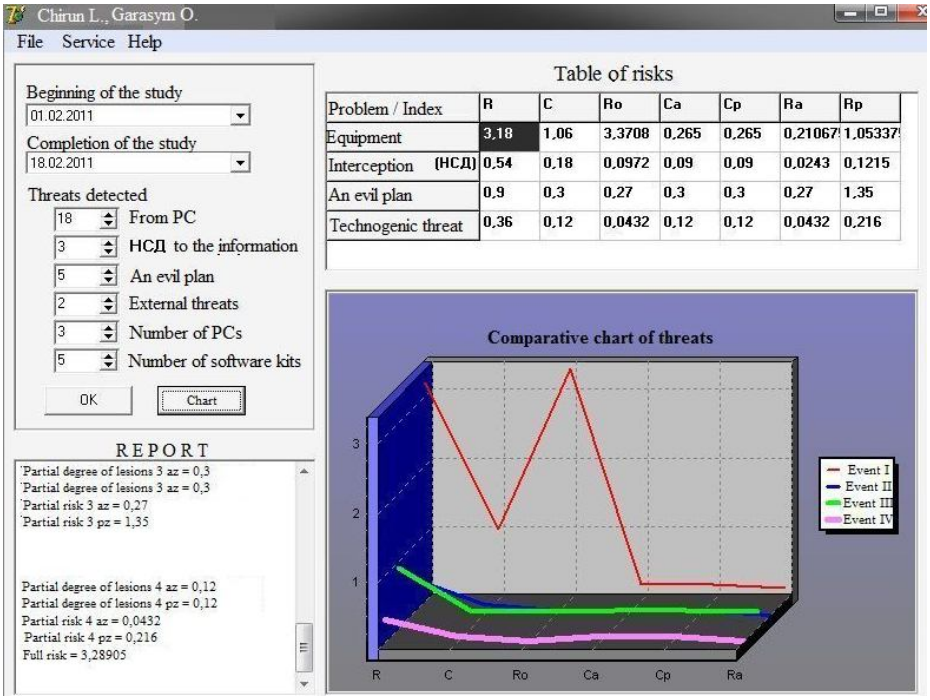

Fig. 4. The threat evaluationt program

2. Degree of involvement:
   (a) I event = 1.06
   (b) II event = 0.18
   (c) 3rd event = 0.3
   (d) IV event = 0.12
3. One-time losses:
   (a) I event = 3.3708
   (b) II event = 0.0972
   (c) 3rd event = 0.27
   (d) IV event = 0.0432
4. Combined losses = 3.7812
5. Combined average loss = 4.98
6. Partial degree of involvement 1 AZ = 0,265

- Partial severity of 1 software = 0.265
- Partial risk 1 AZ = 0.210675
- Partial risk 1 software = 1.053375

7. Partial severity of 2 AZ = 0,09

- Partial severity of 2 software = 0.09
- Partial risk 2 AZ = 0.0243
- Partial risk 2 software = 0.1221

8. Partial severity of 3 AZ = 0.3

- Partial severity of 3 software = 0.3
- Partial risk 3 AZ = 0.27
- Partial risk 3 software = 1.35

9. Partial degree of involvement 4 AZ = 0,12

- Partial severity of 4 software = 0.12
- Partial risk 4 AZ = 0.0432
- Partial risk 4 software = 0.216

10. Total risk = 3.28905

For certain risks, it is noticeable that the level of protection of the ISN department network is insufficient and the greatest threat to the network is the event I. Therefore, let us investigate in this aspect the threat using the system of finding logical rules. WithWhy (Demo, which has a limit on the number of records only), we derive logical rules based on the consolidated data about detected threats of event I (Fig. 4).

Virus

Cod	Name_vir	Size_kb	Dll_infect	Com_infect	Exe_infect	Resident	Polymorphi	Slowing_do	Unauthorize	streng_mes
1	Virus.Win32	20	☑	☐	☑	☑	☑	☑	☐	☐
2	Virus.Multi.I		☐	☐	☑	☐	☐	☑	☐	☐
3	Virus.Boot-[		☐	☑	☑	☑	☐	☑	☑	☐
4	Virus.Win32	36	☐	☐	☑	☐	☐	☐	☐	☑
5	Virus.Win32	18	☐	☐	☑	☐	☐	☐	☐	☐
6	Virus.Win32	41	☐	☐	☑	☑	☐	☐	☐	☐
7	Email-Worm		☑	☐	☑	☑	☑	☐	☐	☑
8	Virus.Win32	36	☐	☐	☑	☑	☐	☐	☐	☐
9	Virus.Win32		☐	☐	☑	☑	☐	☐	☐	☑
10	Virus.Win32	36	☐	☐	☑	☐	☑	☐	☐	☐
11	Virus.Win32	9	☐	☐	☑	☑	☐	☑	☐	☐
12	Virus.Win32	17	☑	☐	☑	☑	☐	☑	☑	☐
13	Virus.DOS. A	1	☐	☑	☑	☑	☐	☐	☐	☑
14	Email-Worm	53	☐	☐	☑	☑	☐	☑	☑	☐
15	Virus.Win32	31	☐	☑	☑	☑	☐	☑	☑	☐
16	Virus.Win32	16	☑	☐	☑	☑	☐	☑	☑	☐
17	Virus.Win32	8	☐	☐	☑	☐	☐	☑	☐	☐
18	Win32.Killis.	2	☐	☐	☑	☐	☐	☐	☐	☐

Fig. 5. Table for accounting for virus attacks

We use the following rules, which revealed deficiencies in the security system, namely the distribution of access to the local network and the Internet in software products, which overloaded the operating system and spread viruses:

1. *If* **Unauthorized_address_to_net** *is* **No** *Then* **Slowing_down_PC** *is not* **Yes**
Rule's probability: **0,692**
The rule exists in **9** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers): ***4, 5, 6, 7, 8, 9, 10, 13, 18***
Negative Examples (records' serial numbers): ***1, 2, 11, 17***

2. *If* **Unauthorized_address_to_net** *is* **Yes** *Then* **Slowing_down_PC** *is* **Yes**
Rule's probability: **1,000**
The rule exists in **5** *records.*
Significance Level: Error probability < 0,1
Positive Examples (records' serial numbers): ***3, 12, 14, 15, 16*** *(Fig. 6)*

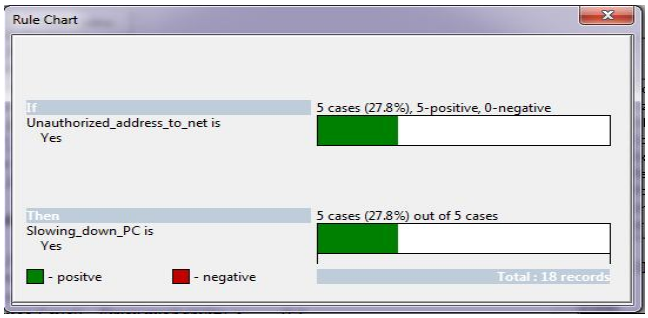

Fig. 6. Graph the rule based on an analysis of consolidated threat resources.

The information security management system aims to counter attacks from the outside and promote secure communication within the organization as well as beyond. The essence of the management system includes the need to consolidate information about the state of the computer system and effective ways of its use, and therefore the main task of the information security management system is the ability to solve problems with consideration of a number of specific limitations of the corporation, as well as to quickly and correctly diagnose and best troubleshoot systems.

It should be remembered that any measures taken to protect the information should not cost more than the information itself. Setting up physically isolated secure communication channels for secure information exchange between remote nodes is an extremely expensive and not always justifiable measure. Therefore, consolidated information resources on the state of corporate communications are the basis for the information security management system.

6 Conclusion

In order to coordinate the NISMS to address the problems of weak links in the communication network, it is necessary to distinguish from the general system of threats

consolidation as an integral part of information security, which is the basis for preparing the necessary information for acquiring new knowledge. An important way to improve network security is to assess the risks of threats that are generated by consolidated threat resources. Using this approach creates the prerequisites for making optimal decisions at the SMIB planning stage and improving it. In order to organize the totality of threats according to the ISMS objectives, it is advisable to use consolidated resources, which forms the methodological basis of ISMS and allows obtaining the necessary information to solve specific problems. Quite often, security personnel are responsible for monitoring and analyzing the data presented in one system. Security personnel only periodically review the data and do not report in a timely manner the results of the analysis of the security management reports to all concerned.

References

1. Rzheuskyi, A., Matsuik, H., Veretennikova, N., Vaskiv, R.: Selective Dissemination of Information – Technology of Information Support of Scientific Research. Advances in Intelligent Systems and Computingб 871, 235-245 (2019)
2. Rzheuskiy, A., Veretennikova, N., Kunanets, N., Kut, V.: The information support of virtual research teams by means of cloud managers. International Journal of Intelligent Systems and Applications, 10(2), 37-46 (2018)
3. Rzheuskyi, A., Kunanets, N., Kut, V.: Methodology of research the library information services: The case of USA university libraries. Advances in Intelligent Systems and Computing, 689, 450-460 (2018)
4. Rzheuskyi, A., Kunanets, N., Kut, V.: The analysis of the United States of America universities library information services with benchmarking and pairwise comparisons methods. In: Computer Sciences and Information Technologies, 417-420 (2017).
5. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C (second Edition. N.Y. : John Wiley & Sons, Inc. (1996)
6. Draft, E.: Authentication Policy for Federal Agencies. In: Federal Register, 68. (2003)
7. Advanced Encryption Standart (AES) http://www.intuit.ru/department/security/networksec/4/5.html. (2012)
8. Horton, M., Mugge, C.: Network Security - Portable Reference. In: McGraw-Hill, (2003).
9. Atkinson, R.: IETF RFC 1825: Security Architecture for the Internet Protocol. (1995).
10. Saaty, T. L.: An eingenvalue allocation model for prioritization and planning. In: Energy Management and Policy Center. University of Pennsylvania (1972)
11. Saadat, M.: Network Security Principles and Practices. In: Cisco Press. (2003)
12. Lytvyn, V., Vysotska, V., Rzheuskyi, A.: Technology for the Psychological Portraits Formation of Social Networks Users for the IT Specialists Recruitment Based on Big Five, NLP and Big Data Analysis. In: CEUR Workshop Proceedings, Vol-2392, 147-171. (2019)
13. Khribi, M. K., Jemni, M., Nasraoui, O.: Automatic recommendations for e-learning personalization based on web usage mining techniques and information retrieval. In: International Conference on Advanced Learning Technologies, 241-245. (2008).
14. Vysotska, V., Fernandes, V.B., Emmerich, M.: Web content support method in electronic business systems. In: CEUR Workshop Proceedings, Vol-2136, 20-41 (2018)
15. Demchuk, A., Lytvyn, V., Vysotska, V., Dilai, M.: Methods and Means of Web Content Personalization for Commercial Information Products Distribution. In: Lecture Notes in Computational Intelligence and Decision Making, 1020, 332–347. (2020)

16. Yu, P. L.: Multiple Criteria Decision Making: Concepts, Techniques, and Extensions. Plenum Press, N.Y. (1985)
17. Saaty, T. L.: Multicriteria Decision Making. The Analytic Hierarchy Process: Planning. Priority Setting. Resource Allocation. University of Pittsburgh, RWS Publications (1990)
18. Antonyu,k N., Medykovskyy, M., Chyrun, L., Dverii, M., Oborska, O., Krylyshyn, M., Vysotsky, A., Tsiura, N., Naum, O.: Online Tourism System Development for Searching and Planning Trips with User's Requirements. In: Advances in Intelligent Systems and Computing IV, Springer Nature Switzerland AG 2020, 1080, 831-863. (2020)
19. Lozynska, O., Savchuk, V., Pasichnyk, V.: Individual Sign Translator Component of Tourist Information System. In: Advances in Intelligent Systems and Computing IV, Springer Nature Switzerland AG 2020, Springer, Cham, 1080, 593-601. (2020)
20. Rzheuskyi, A., Kutyuk, O., Voloshyn, O., Kowalska-Styczen, A., Voloshyn, V., Chyrun, L., Chyrun, S., Peleshko, D., Rak, T.: The Intellectual System Development of Distant Competencies Analyzing for IT Recruitment. In: Advances in Intelligent Systems and Computing IV, Springer, Cham, 1080, 696-720. (2020)
21. Rusyn, B., Pohreliuk, L., Rzheuskyi, A., Kubik, R., Ryshkovets Y., Chyrun, L., Chyrun, S., Vysotskyi, A., Fernandes, V. B.: The Mobile Application Development Based on Online Music Library for Socializing in the World of Bard Songs and Scouts' Bonfires. In: Advances in Intelligent Systems and Computing IV, Springer, 1080, 734-756. (2020)
22. Lytvyn, V., Vysotska, V., Mykhailyshyn, V., Peleshchak, I., Peleshchak, R., Kohut, I.: Intelligent system of a smart house. In: 3rd International Conference on Advanced Information and Communications Technologies, 282-287. (2019)
23. Lytvyn, V., Peleshchak, I., Peleshchak, R., Vysotska, V.: Information Encryption Based on the Synthesis of a Neural Network and AES Algorithm. In: 3rd International Conference on Advanced Information and Communications Technologies, AICT, 447-450. (2019)
24. Kravets, P., Burov, Y., Lytvyn, V., Vysotska, V.: Gaming method of ontology clusterization. In: Webology, 16(1), 55-76. (2019)
25. Gozhyj, A., Kalinina, I., Gozhyj, V., Vysotska, V.: Web service interaction modeling with colored petri nets. In: Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019, 1,8924400, pp. 319-323 (2019)
26. Shu, C., Dosyn, D., Lytvyn, V., Vysotska V., Sachenko, A., Jun, S.: Building of the Predicate Recognition System for the NLP Ontology Learning Module. In: Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, 802-808 (2019)
27. Lytvyn, V., Gozhyj, A., Kalinina, I., Vysotska V., Shatskykh, V., Chyrun, L., Borzov, Y.: An intelligent system of the content relevance at the example of films according to user needs. In: CEUR Workshop Proceedings 2516, pp. 1-23 (2019)
28. Antonyuk N., Vysotsky A., Vysotska V., Lytvyn V., Burov Y., Demchuk A., Lyudkevych I., Chyrun L., Chyrun S., Bobyk I.: Consolidated Information Web Resource for Online Tourism Based on Data Integration and Geolocation. In: 14th International Scientific and Technical Conference on Computer Science and Information Nechnologies, 15-20. (2019)
29. Lytvyn V., Vysotska V., Peleshchak I., Basyuk T., Kovalchuk V., Kubinska S., Chyrun L., Rusyn B., Pohreliuk L., Salo T.: Identifying Textual Content Based on Thematic Analysis of Similar Texts in Big Data. In: 2019 IEEE 14th International Scientific and Technical Conference on Computer Science and Information Nechnologies (CSIT), 84-91. (2019)
30. Vysotsky A., Lytvyn V., Vysotska V., Dosyn D., Lyudkevych I., Antonyuk N., Naum O., Vysotskyi A., Chyrun L., Slyusarchuk O.: Online Tourism System for Proposals Formation to User Based on Data Integration from Various Sources. In: 14th International Scien-

tific and Technical Conference on Computer Science and Information Nechnologies (CSIT), 92-97. (2019)
31. Vysotska V., Lytvyn V., Kovalchuk V., Kubinska S., Dilai M., Rusyn B., Pohreliuk L., Chyrun L., Chyrun S., Brodyak O.: Method of Similar Textual Content Selection Based on Thematic Information Retrieval. In: 2019 IEEE 14th International Scientific and Technical Conference on Computer Science and Information Nechnologies (CSIT'2019), 1-6. (2019)
32. Lytvyn, V., Vysotska, V., Shakhovska, N., Mykhailyshyn, V., Medykovskyy, M., Peleshchak, I., Fernandes, V. B., Peleshchak, R., Shcherbak, S.: A Smart Home System Development. In: Advances in Intelligent Systems and Computing IV, 1080, 804-830. (2020)
33. Lytvyn, V., Kowalska-Styczen, A., Peleshko, D., Rak, T., Voloshyn, V., Noennig, J. R., Vysotska, V., Nykolyshyn, L., Pryshchepa, H.: Aviation Aircraft Planning System Project Development. In: Advances in Intelligent Systems and Computing IV, Springer, Cham, 1080, 315-348. (2020)
34. Lytvyn, V., Vysotska, V., Shatskykh, V., Kohut, I., Petruchenko, O., Dzyubyk, L., Bobrivetc, V., Panasyuk, V., Sachenko, S., Komar, M.: Design of a recommendation system based on Collaborative Filtering and machine learning considering personal needs of the user. In: Eastern-European Journal of Enterprise Technologies, 4(2-100), 6-28. (2019)
35. Vysotska, V., Chyrun, L.: Methods of information resources processing in electronic content commerce systems. In: Proceedings of 13th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2015-February. (2015)
36. Andrunyk, V., Chyrun, L., Vysotska, V.: Electronic content commerce system development. In: Proceedings of 13th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2015-February. (2015)
37. Alieksieieva, K., Berko, A., Vysotska, V.: Technology of commercial web-resource processing. In: Proceedings of 13th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2015-February. (2015)
38. Lytvyn V., Burov Y., Kravets P., Vysotska V., Demchuk A., Berko A., Ryshkovets Y., Shcherbak S., Naum O.: Methods and Models of Intellectual Processing of Texts for Building Ontologies of Software for Medical Terms Identification in Content Classification. In: CEUR Workshop Proceedings, of the 2nd International Workshop on Informatics & Data-Driven Medicine (IDDM 2019), Vol-2362, 354-368. (2019)
39. Lytvyn, V., Sharonova, N., Hamon, T., Cherednichenko, O., Grabar, N., Kowalska-Styczen, A., Vysotska, V.: Preface: Computational Linguistics and Intelligent Systems (COLINS-2019). In: CEUR Workshop Proceedings, Vol-2362. (2019)
40. Emmerich, M., Lytvyn, V., Yevseyeva, I., Fernandes, V. B., Dosyn, D., Vysotska, V.: Preface: Modern Machine Learning Technologies and Data Science (MoMLeT&DS-2019). In: CEUR Workshop Proceedings, Vol-2386. (2019)
41. Lytvyn, V., Vysotska, V., Mykhailyshyn, V., Rzheuskyi, A., Semianchuk, S.: System Development for Video Stream Data Analyzing. In: In Advances in Intelligent Systems and Computing, 1020, 315-331. (2020)
42. Zdebskyi, P., Vysotska, V., Peleshchak, R., Peleshchak, I., Demchuk, A., Krylyshyn, M.: An Application Development for Recognizing of View in Order to Control the Mouse Pointer. In: CEUR Workshop Proceedings, Vol-2386, 55-74. (2019)
43. Vysotska, V., Burov, Y., Lytvyn, V., Oleshek, O.: Automated Monitoring of Changes in Web Resources. In: Advances in Intelligent Systems and Computing, 1020, 348–363. (2020)
44. Burov, Y., Vysotska, V., Kravets, P. Ontological approach to plot analysis and modeling. CEUR Workshop Proceedings, Vol-2362, 22-31 (2019)

45. Lytvyn, V., Vysotska, V., Demchuk, A., Demkiv, I., Ukhanska, O., Hladun, V., Kovalchuk, R., Petruchenko, O., Dzyubyk, L., Sokulska, N.: Design of the architecture of an intelligent system for distributing commercial content in the internet space based on SEO-technologies, neural networks, and Machine Learning. In: Eastern-European Journal of Enterprise Technologies, 2(2-98), 15-34. (2019)
46. Lytvyn, V., Peleshchak, I., Vysotska, V., Peleshchak, R.: Satellite spectral information recognition based on the synthesis of modified dynamic neural networks and holographic data processing techniques, 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT, 330-334 (2018)
47. Gozhyj, A., Vysotska, V., Yevseyeva, I., Kalinina, I., Gozhyj, V.: Web Resources Management Method Based on Intelligent Technologies, Advances in Intelligent Systems and Computing, 871, 206-221 (2019)
48. Lytvyn, V., Vysotska, V., Dosyn, D., Burov, Y.: Method for ontology content and structure optimization, provided by a weighted conceptual graph, Webology, 15(2), 66-85 (2018)
49. Lytvyn, V., Vysotska, V., Dosyn, D., Lozynska, O., Oborska, O.: Methods of Building Intelligent Decision Support Systems Based on Adaptive Ontology, Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 145-150 (2018)
50. Gozhyj, A., Kalinina, I., Vysotska, V., Gozhyj, V.: The method of web-resources management under conditions of uncertainty based on fuzzy logic, 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018 – Proceedings 1, 343-346 (2018)
51. Rusyn, B., Lytvyn, V., Vysotska, V., Emmerich, M., Pohreliuk, L.: The Virtual Library System Design and Development, Advances in Intelligent Systems and Computing, 871, 328-349 (2019)
52. Rusyn, B., Vysotska, V., Pohreliuk, L.: Model and architecture for virtual library information system, 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018 – Proceedings 1, 37-41 (2018)
53. Su, J., Sachenko, A., Lytvyn, V., Vysotska, V., Dosyn, D.: Model of Touristic Information Resources Integration According to User Needs, 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018 – Proceedings 2, 113-116 (2018)
54. Vysotska, V., Lytvyn, V., Burov, Y., Gozhyj, A., Makara, S.: The consolidated information web-resource about pharmacy networks in city. In: CEUR Workshop Proceedings, 239-255 (2018)
55. Vysotska, V., Chyrun, L.: Analysis features of information resources processing. In: Computer Science and Information Technologies, Proc. of the Int. Conf. CSIT, 124-128 (2015)
56. Vysotska, V., Chyrun, L., Chyrun, L.: Information Technology of Processing Information Resources in Electronic Content Commerce Systems. In: Computer Science and Information Technologies, CSIT'2016, 212-222 (2016)
57. Vysotska, V., Rishnyak, I., Chyrun L.: Analysis and evaluation of risks in electronic commerce, CAD Systems in Microelectronics, 9th International Conference, 332-333 (2007).
58. Lytvyn, V., Vysotska, V., Peleshchak, I., Rishnyak, I., Peleshchak, R.: Time Dependence of the Output Signal Morphology for Nonlinear Oscillator Neuron Based on Van der Pol Model. In: International Journal of Intelligent Systems and Applications, 10, 8-17 (2018)
59. Lytvyn, V., Vysotska, V., Veres, O., Rishnyak, I., Rishnyak, H.: The Risk Management Modelling in Multi Project Environment.. In: Computer Science and Information Technologies, Proc. of the Int. Conf. CSIT, 32-35 (2017)