Qualitative and Quantitative Characteristics Analysis for Information Security Risk Assessment in E-Commerce Systems

Aleksandr Gozhyj[a], Irina Kalinina[a], Victoria Vysotska[b], Svitlana Sachenko[c] and Roman Kovalchuk[d]

[a] *Petro Mohyla Black Sea National University, 68 Desantnykiv, 10, 54003, Mykolaiv, Ukraine*

[b] *Lviv Polytechnic National University, S,.Bandera street, 12, Lviv, 79013, Ukraine*

[c] *Ternopil National Economic University, Lvivska Street, 11, Ternopil, 46004, Ukraine*

[d] *Hetman Petro Sahaidachnyi National Army Academy, Heroes of Maidan street, 32, Lviv, 79012, Ukraine*

Abstract

The choice of security profile in e-commerce systems depends on the results of the analysis of quantitative and qualitative characteristics of information security risk assessment. The article analyses the concept of information in the aspect of property rights object and investigates threats to information security in electronic commerce systems based on systematic attacks series frequency analysis on the system.

Keywords

Information Security, E-Commerce System, Risk Assessment

1. Introduction

Considering information as an object of protection, it should note that information is the result of reflection and processing in the human consciousness of the diversity of the surrounding world [1]. Not only has a secret information needed a protection [2]. Modifying unclassified data can lead to leakage of classified information [3]. The destruction or disappearance of data that has accumulated with great difficulty can cause them to be lost. Depending on the scope of a particular data processing system, the loss or leakage of confidential information can lead to a variety of important consequences: from innocent jokes to the dramatic economic and political consequences. In particular, common are the crimes in automated systems that serve banking and trading structures.

Therefore, it is very important to solve the problems of creating, using and evaluating the effectiveness of information security systems (GIS) for the designed and existing electronic commerce systems (ECS).

ICT&ES-2020: Information-Communication Technologies & Embedded Systems, November 12, 2020, Mykolaiv, Ukraine

alex.gozhyj@gmail.com (A. Gozhyj); irina.kalinina1612@gmail.com (I. Kalinina); Victoria.A.Vysotska@lpnu.ua (V. Vysotska)

0000-0002-3517-580X (A. Gozhyj); 0000-0001-8359-2045 (I. Kalinina); 0000-0001-6417-3689 (V. Vysotska); 0000-0001-8225-1820 (S. Sachenko); 0000-0001-8337-8591 (R. Kovalchuk)

CEUR Workshop Proceedings (CEUR-WS.org)

2. Related Works Review

Considering the importance of the information systems protection the following specific feature should be taken into account [4]:

- Incompleteness and uncertainty of initial information on the composition of IP and specific threats;
- Multi-criterion of the task, related to the need to account for a large number of indicators (requirements) of GIS;
- Availability of quantitative and qualitative indicators that must be taken into account when solving the tasks of KIC development and implementation;
- Impossibility of applying classical optimization methods.

The model developed shall meet the following requirements [5]:

- Used as: A Guide to Creating a GIS; Methods of formation of indicators and requirements for GIS; Tool (methodology) for GIS assessment; GIS models for research (state matrix) [6];
- Have properties: Versatility; Complexity; Easy to use; Clarity; Practical orientation; Being self-educated (ability to increase knowledge); Operate in conditions of high uncertainty of the initial information [7];
- Allow: Establish a relationship between indicators (requirements); Set different levels of protection; To receive quantitative estimates; Monitor the status of GIS; Apply different assessment techniques; Respond promptly to changes in operating conditions; To unite the efforts of different specialists with a single plan [8].

The value of information is a criterion when making any decision to protect it. Although many different attempts have made to formalize this process using information theory and decision analysis methods, the assessment process remains highly subjective. To evaluate, it is necessary to divide the information into categories not only according to its value but also according to its importance. The following is the distribution of information by importance [9]:

- Vital, irreplaceable information, the availability of which is necessary for the functioning of the organization;
- Important information - information that can be replaced or restored, but the recovery process is very difficult and costly;
- Useful information - information that is difficult to retrieve, but an organization can function effectively without it;
- Irrelevant information - information that the organization no longer needs.

In practice, attributing information to one of these categories is quite a challenge, since the same information can used by many organizational units, each of which can be assigned to different categories of importance. The importance category, as well as the value of information, subsequently changes and depends on the attitude of different groups of consumers and potential violators [10]. There are definitions of groups of persons involved in the processing of information: the holder is the organization or the person who owns the information; source - the organization or person supplying the information; the offender is a person or organization who unlawfully seeks information. The attitude of these groups to the significance of the same information may be different [11]. Example:

- Important online information, such as a list of current week orders and production schedules, can be of high value to the user, while low to the source or offender;
- Personal information, such as medical information, is of much greater value to the source (the person concerned) than to its user or offender [12];
- The information used by management to develop and make decisions, such as market prospects, may be much more valuable to the offender than to the source or holder who has already completed the analysis of the data [13].

These categories of importance are noteworthy and can applied to any information. This is also consistent with the existing principle of the distribution of information by level of secrecy. A level of secrecy is an administrative or legislative measure adequate to the extent of a person's liability for the leakage or loss of specific classified information, which is regulated by a special document taking into account public, military, strategic, commercial, service or private interests. Such information may be state, military, commercial, official or personal secret [14]. Practice shows that not only secret information is protected. Unauthorized information subject to unauthorized changes (such as modifications to management commands) may result in leakage or loss of classified information associated with it, as well as failure to perform automated system assignments due to erroneous data that may not detected by the system user [15]. The total amount or statistics of non-classified data may be secret as a result. Similarly, aggregate data of one level of secrecy may generally be information of higher secrecy. Functional delimitation of access to information is widely used to protect against such situations. The equal importance, the information processed by the system is shared according to the functional responsibilities and authority of the users. Until recently, information security in automated systems (AUs) is interpreted solely as a risk of unauthorized receipt of information throughout the processing and storage of the AUs. Today, information security is also interpreted as security for actions that use information [16]. The fundamental differences of the extended interpretation, unlike the traditional one, are very important as computer technology is increasingly used for automated management of information systems and processes in which unauthorized changes to planned algorithms and technologies can have serious consequences. Historically, a traditional property object is a tangible object [17]. Information is not a material object, information is knowledge, that is, the reflection of reality in the mind of man (and the true or false representation is not essential, it is important that it is in the mind). In the future, information can translated into tangible objects of the world. As an intangible object, information is inextricably linked to the material medium [18]. This is the human brain or the alienated material, such as a book, floppy disk, and other types of "memory" (computer memory). From a philosophical point of view, it is possible to speak of information as an abstract substance existing in itself, but for us neither storing nor transmitting information without a tangible medium is impossible [19].

Risk analysis involves the study and systematization of threats to ECS, defining the requirements for security tools for information systems [20, 21]. The analysis clarifies the permissible residual risks and costs of information security measures, and then concludes on the permissible residual risk levels and the feasibility of applying specific security options.

Besides many recent references were dedicated by information security systems issues.

In the Reference [1] the complementary ISRA and MCDM methods are explored that could be used as a basis to create a new hybrid model for more efficient evaluation of critical IT solutions in information security(IS).

Authors of the Reference [2] are solving a problem of weighting the risk factors that lead to different risk values. The proposed metrics are classified and aggregated providing a unique risk metric.

The Reference [3] presents the qualitative and quantitative depictions of ECSs from a complex systems perspective, that provides a brand new idea of how to address the current issues of information security in ECS.

The Reference [22] present a Goal-driven Software Development Risk Management Model (GSRM) and its explicit integration into the requirements engineering phase as well as an empirical investigation result of applying GSRM into a project.

The Reference [23] describes the impact of criminal activities based on the nature of the crime, the victims of cybercrime in Internet. Authors proposed to utilize Fuzzy Inference Model (FIS) to produce risk assessment result based on the four risk factors in particular, vulnerability, threat, likelihood and impact as well as specify the range of risks and try to solve such issues.

Based on the hierarchical structure of e-commerce security system, the Reference [24] analyses the security requirements for e-commerce security and proposes a quantitative e-commerce risk assessment model based on cloud computing.

Authors of the Reference [25] designed a model that integrates fault tree analysis, decision theory and fuzzy theory to determine the current causes of cyberattack prevention failures and the vulnerability of a given cybersecurity system. The model was applied to evaluate the cybersecurity risks caused by attacks on a website as well as assess the possible consequences of such attacks.

In the Reference [26] a model, based on the opinions of e-commerce security experts, is designed and implemented by using fuzzy expert systems and MATLAB. A case study is conducted to validate the effectiveness of this model.

In the Reference [27] the data security in the systems of control of passenger flows in Smart City is investigated. The Reference [28] is dedicated by the analysis of DDOS attacks features on the basic machine learning. The Reference [29] describes the measurement instrument for information technology risk assessment towards a risk management strategy.

The Reference [30] explores the internal and external organizational factors and characteristics of information security for affecting the e-commerce systems.

The Reference [31] investigates the evaluation system of E-commerce specialty based on TOPSIS and analytic hierarchy process.

3. Proposed Methods and Materials

When solving many theoretical and engineering problems, it is often necessary to know the likelihood of a certain number of events occurring in a series. If the risk tests that form a series are considered to independent, then we can make the necessary predictions using the developed hypergeometric law. Consider this a simple example. Let N events be taken from the list of informational security threats, including n dangerous with serious consequences and m insignificant threats, and each of the events occurred at a certain interval of x_i times

$$i = \overline{1, k}, k = n + m, N = \sum_{i=1}^{k} x_i \tag{1}$$

the events took place without a certain interdependence, frequency and order.

Tests involving the analysis of these events over a period can investigated using two schemes. Under the terms of the first scheme, each completed event is considered to repetitive after a while, after the result of each trial is recorded in the protocol. In each subsequent study, the probabilities of the occurrence of a particular event remain unchanged and are, respectively, n/N and m/N.

A probabilistic threat experiment that operates with the effects of mutually independent trials, in each of which threat events retain their unconditional probabilities, is called repeated sampling. In the implementation of the second scheme, the completed events are considered to non-recurring. The probability of an event occurring in each subsequent trial depends on the results of the previous tests. Thus, we are dealing with dependent tests, and the probability of the result of each test is conditional. An experiment that runs on a sequence of dependent tests, each of which results in conditional probabilities, is called a non-repetitive (or non-return) sample. The real probabilistic threat experiment can carried out either by repeated or repeated sampling [26].

Let the event $B_x^{'}$ be that the threat of informational security A will appear at least a and not more than b times. Then the probability $P_N(a \leq x \leq b)$ of this event is

$$P_N(a \leq x \leq b) = P_N(a) + P_N(a+1) + ... + P_N(b-1) + P_N(b) = \sum_{x=a}^{b} P_N(x) = \sum_{x=a}^{b} C_N^x p^x q^{N-x}. \tag{2}$$

Graphically, the number of additives that need to be calculated can represented as follows (Fig. 1):

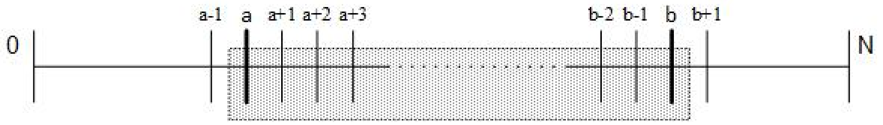

Figure 1: Graphically display the number of additions in the event probability $P_N(a \leq x \leq b)$

If the number of terms corresponding to the values of x from a to b is much greater than the total number of terms corresponding to the values of x from 0 to $a-1$ and from $b-1$ to N, then it is more convenient to summarize the probabilities for these two sequences. In this case, we obtain the probability of the opposite event $B_x^{'}$: $P(B_x^{'}) = \sum_{x=0}^{a-1} C_N^x p^x q^{N-x} - \sum_{x=b+1}^{N} C_N^x p^x q^{N-x}$. Now we calculate the required probability by the formula

$$P_N(a \le x \le b) = 1 - P(B_x^{'}) = 1 - \sum_{x=0}^{a-1} C_N^x p^x q^{N-x} - \sum_{x=b+1}^{N} C_N^x p^x q^{N-x} \tag{3}$$

Graphically, this approach can interpreted as follows (Fig. 2):

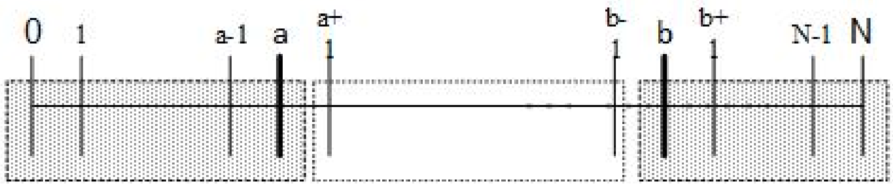

Figure 2: Representation of the number of additions in the likelihood of the opposite event

Consider some partial cases. Suppose that it is necessary to determine the probability that some unit of threat A will meet at least a times. Here

$$P_N(x \ge a) = \sum_{x=0}^{N} C_N^x p^x q^{N-x} \tag{4}$$

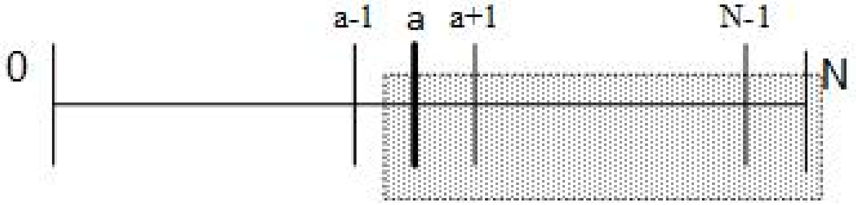

Figure 3: Graphic representation of the number of additions in the event probability

If the value of a is small, it is advisable to use the expression

$$P_N(x \ge a) = 1 - \sum_{x=0}^{a-1} C_N^x p^x q^{N-x}, \tag{5}$$

which is a partial case of formula (3).

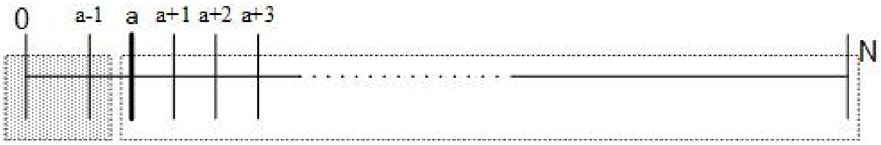

Figure 4: Graphic representation of the number of additions in the likelihood of opposite event

In the case when $a = 1$, we have

$$P_N(1 \le x \le N) = 1 - C_N^0 p^0 q^N = 1 - q^N. \tag{6}$$

The probability of occurrence of event A no more than b b times is also determined by summing the probabilities in which the event appears $0, 1, 2, ..., b$ times:

$$P_N(x \le b) = \sum_{x=0}^{b} C_N^x p^x q^{N-x} \tag{7}$$

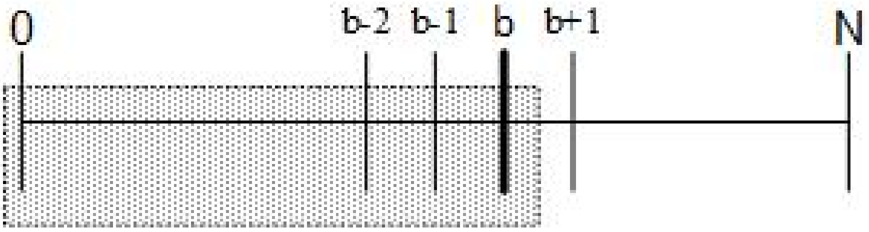

Figure 5: Graphic representation of the number of additions in the event probability

If the value of b is close to N , then this probability should calculated by the formula:

$$P_N(x \le b) = 1 - \sum_{x=b+1}^{N} C_N^x p^x q^{N-x} \tag{8}$$

which is also a partial case of formula (8).

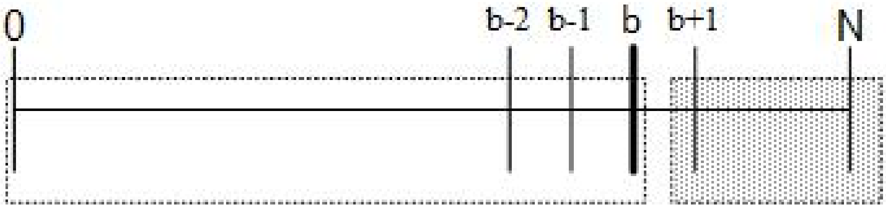

Figure 6: Graphic representation of the number of additions $P_N(x \le b)$

In informational security threat studies, and especially when designing information security systems in e-commerce systems, there is a constant need to determine the amount of potential threats needed to ensure that information and financial transactions are securely assigned. To do this, let's first transform the formula

$$P_N(1 \le x \le N) = 1 - q^N = 1 - (1 - p)^N \tag{9}$$

by the way $(1 - p)^N = 1 - P_N(1 \le x \le N)$.

We prologarify both parts of equality and after simple transformations we obtain

$$N = \frac{lg\,[1 - P_N(1 \le x \le N)]}{lg(1 - p)}, \tag{10}$$

where N indicates the required sample size.

The hypergeometric law can applied only to finite general populations, the volume of which is known. Since in security problems the volume of the general set of attacks is usually not a predictable finite value, the application of this law to predict the results of experiments in unique samples is unrealistic. However, under certain conditions, the hypergeometric probability is well approximated by the binomial probability. Therefore, without fear of violating the mathematical rigor, we will calculate the probabilities of occurrence of event A exactly x times in our unique sample as if it were a re-sample. In other words, we apply binomial law to unique samples.

We will consider the data of S attacks as S series or samples, each of which consists of N independent tests. The event A can appear x times in each series ($x = 0, 1, 2, ..., N$).It is easy to notice that there are groups of series in which A appears $x = 0, 1, 2, ..., N$ times. It follows that the relative frequency of event $A$is exactly x times in one series is determined by the ratio $f_N(x) = S_x/S$ where S_x is the number of series in which event A appears exactly x times.

The a priori probability of occurrence of event A in one random series is equal to

$$p \approx \frac{\sum xS_x}{NS}, \tag{11}$$

and therefore,

$$q \approx 1 - \frac{xS_x}{NS}. \tag{12}$$

In the obtained theoretical distribution, each value of x is correlated not by its probability, but by some theoretically expected number of series (samples) S_x^T , in which event A appears exactly x times. Because

$$S_x^T = SP_N(x) = SC_N^x p^x q^{N-x}, \tag{13}$$

it is not difficult to notice that the values S_x^T and $P_N(x)$ are related by coefficient of proportionality S.

Table 1
The frequencies of successful attacks

Number of occurrences of the event x	0	1	2	3	4	5	6	7	8	9	10	
Empirical frequencies of sampling S_x	0	1	4	15	33	27	11	4	2	1	0	$\sum S_x = 100$

4. Experimental Results and Discussions

For determine the characteristics of a period of systematic attacks on the ECS was randomly selected 100 time intervals of 10 attacks each. The frequencies of successful attacks in these series are given in Table 1. It is necessary to calculate the theoretical binomial distribution of probabilities of x successful attacks in one series.

Here $S = 100, N = 10$. Using the products of x and $S_x$given in the table, we find

$$p = \frac{\sum xS_x}{NS} = \frac{0 \cdot 0 + 1 \cdot 1 + 2 \cdot 4 + 3 \cdot 15...}{10 \cdot 100} = \frac{440}{1000} = 0.44$$

Let's take $p \approx 0.44$ and $q \approx 0.56$, then based on $Np + p - 1 \leq x_0 \leq Np + p$ we have

$$10 \cdot 0.44 - 0.56 < x_0 < 10 \cdot 0.44 - 0.56 + 1, or 3.84 < x_0 < 4.84$$

whence it follows that $x_0 = 4$. Then $P_N(x_0) = P_{10}(4) = C_{10}^4 \cdot 0.3^4 \cdot 0.7^6$. From here we find that $P_{10}(4) = 0.2001$. Therefore, $S_x^T = SP_{10}(4) = 100 \cdot 0.2001 \approx 20.01$. he remaining values of the expected number of samples are given in the table 2 and on Fig. 7-9.

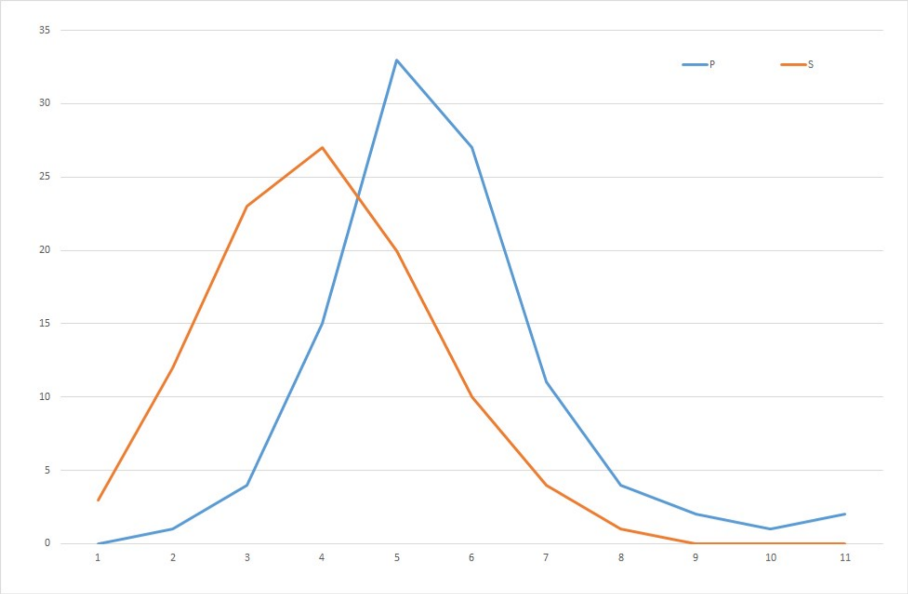

Figure 7: Graphic of the dependence of the values of the expected number of samples of attacks series

Table 2
The remaining values of the expected number of samples

x	S_x	$P_N(x)$	S_x^T
0	0	0.0282	3
1	1	0.1211	12
2	4	0.2335	23
3	15	0.2668	27
4	33	0.2001	20
5	27	0.1029	10
6	11	0.0368	4
7	4	0.0090	1
8	2	0.0014	0
9	1	0.0001	0
10	2	0.0	0
	100	1.0	100

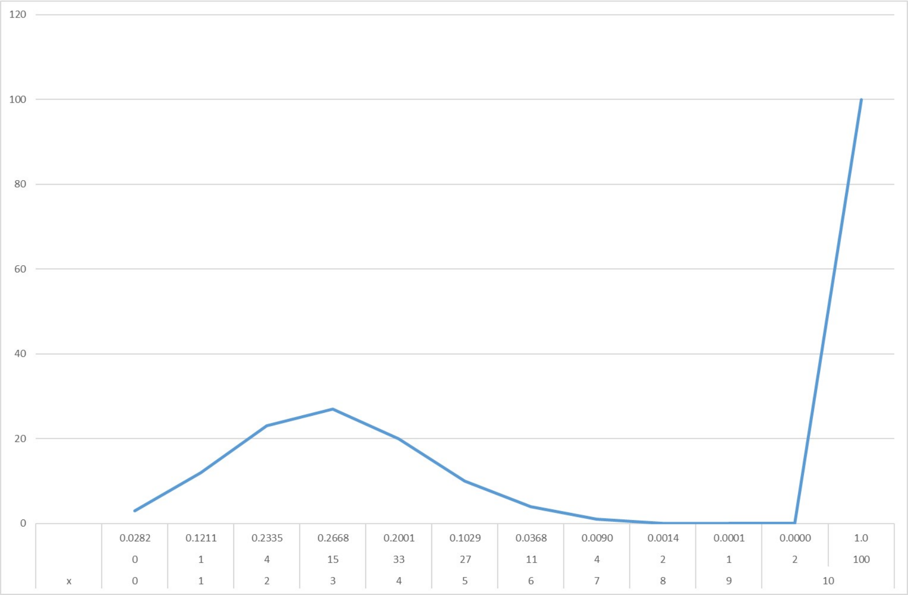

Figure 8: Graphic of the binomial probability distribution of a series of attacks

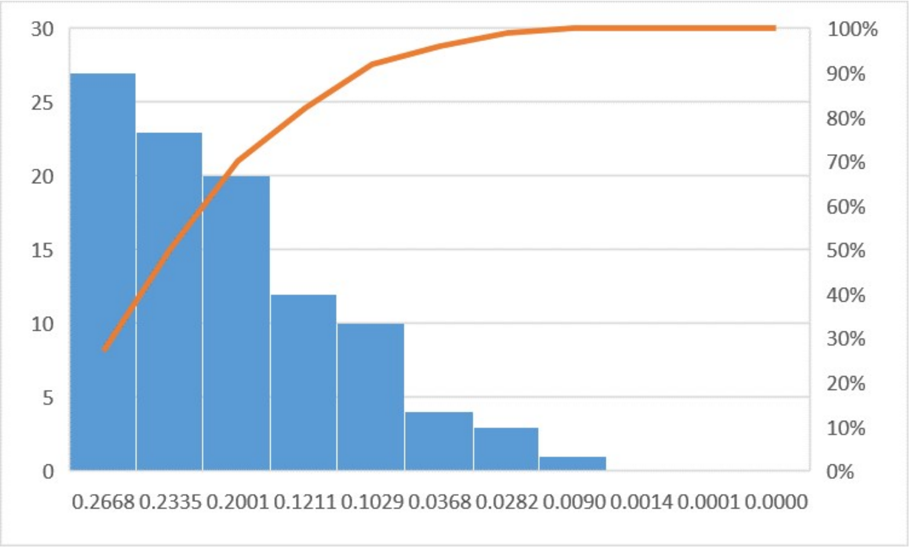

Figure 9: Pareto diagram of the distribution of a series of attacks in descending order, and on the auxiliary axis - the line of the set of values as a percentage of the total

Attacks of 9-10 in the series have almost no effect on the result. Therefore, we can neglect them. Here instead of determining, and then summing up the probabilities of 0, 1, 2, ..., 8 attacks (this is nine terms), let's determine the probability of 9 or 10 attacks (two terms):

$$P_{10}(9) + P_{10}(10) = 0.1493.$$

Then the required value is calculated by the formula (8)

$$P_{10}(x \leq 8) = 1 - (P_{10}(9) + P_{10}(10)) = 1 - 0.1493 = 0.8507.$$

In other words, if we take 10,000 samples of 10 attacks, then in 8507 samples we can expect the appearance of no more than 8 attacks and the greatest load on the security system goes to 2-5 attacks series. By systematizing the statistics of periods of such attacks, it is possible to predict the following system loads and improve security levels in ECS.

5. Conslusions

The authors developed an approach to the analysis of qualitative (absolute frequency of attacks series on the system per a certain period) and quantitative (relative frequency of attacks series on the system per a certain period) characteristics to assess the information security risks in e-commerce systems. It is proposed to use the method of the sequential monitoring to study information security threats and conduct risk assessments. In this case, the mathematical model of risk, which provides the results of the test for the hypergeometric law, is the basis for the construction of other probabilistic models, including those that are widely used in the study of threats to information security.

Qualitative and quantitative characteristics of one event from a series of attacks are analyzed. The analysis clarifies the priority of information security, allowable residual risks and costs of information security measures. Then it concludes on the allowable residual levels of risk and the feasibility of using the specific security options. It has been experimentally confirmed on 10,000 samples out of 10 attacks that in 8507 samples, no more than 8 attacks can be expected, and the greatest load on the security system falls on 2-5 series of attacks.

In the future, it is expected to investigate the attacks series on information systems depending on period (day, week, month and season).

References

[1] D. Maček, I. Magdalenić, N.Ređep, A systematic literature review on the application of multicriteria decision making methods for information security risk assessment, International Journal of Safety and Security Engineering 10 (2020) 161–174. URL: https://doi.org/10.18280/ijsse.100202. doi:10.18280/ijsse.100202.

[2] K. Karoui, Security novel risk assessment framework based on reversible metrics: a case study of DDoS attacks on an e-commerce web server, International Journal of Network Management 26 (2016) 553–578. URL: https://doi.org/10.1002/nem.1956. doi:10.1002/nem.1956.

[3] Z. Song, Y. Sun, J. Wan, L. Huang, J. Zhu, Smart e-commerce systems: current status and research challenges, Electronic Markets 29 (2017) 221–238. URL: https://doi.org/10.1007/s12525-017-0272-3. doi:10.1007/s12525-017-0272-3.

[4] M. Loosemore, E. Cheung, Implementing systems thinking to manage risk in public private partnership projects, International Journal of Project Management 33 (2015) 1325–1334. URL: https://doi.org/10.1016/j.ijproman.2015.02.005. doi:10.1016/j.ijproman.2015.02.005.

[5] R. J. Chapman, The rules of project risk management: Implementation guidelines for major projects, Routledge, 2019.

[6] A. Elzamly, B. Hussin, A comparison of fuzzy and stepwise multiple regression analysis techniques for managing software project risks: Implementation phase, International Management Review 10 (2014) 43–54.

[7] A. G. Kravets, N. Salnikova, K. Dmitrenko, M. Lempert, Industrial cyber-physical systems: Risks assessment and attacks modeling, in: Cyber-Physical Systems: Industry 4.0 Challenges, Springer International Publishing, 2019, pp. 197–210. URL: https://doi.org/10.1007/978-3-030-32648-7_16. doi:10.1007/978-3-030-32648-7_16.

[8] O. Trach, S. Fedushko, Determination of measures of counteraction to the social-oriented risks of virtual community life cycle organization, in: Advances in Intelligent Systems and Computing IV, Springer International Publishing, 2019, pp. 680–695. URL: https://doi.org/10.1007/978-3-030-33695-0_46. doi:10.1007/978-3-030-33695-0_46.

[9] R. Yurynets, Z. Yurynets, D. Dosyn, Y. Kis, Risk assessment technology of crediting with the use of logistic regression model, in: CEUR Workshop Proceedings, volume 2362, 2019.

[10] Z. Wu, L. Wang, Trustworthiness measurement of e-commerce systems using fuzzy hybrid multi-criteria analysis, in: 2015 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2015. URL: https://doi.org/10.1109/trustcom.2015.433. doi:10.1109/trustcom.2015.433.

[11] A. P. H. de Gusmão, L. C. e Silva, M. M. Silva, T. Poleto, A. P. C. S. Costa, Information security risk analysis model using fuzzy decision theory, International Journal of Information Management 36 (2016) 25–34. URL: https://doi.org/10.1016/j.ijinfomgt.2015.09.003. doi:10.1016/j.ijinfomgt.2015.09.003.

[12] L. Chyrun, I. Turok, I. Dyyak, Information model of the tendering system for large projects, in: CEUR Workshop Proceedings, volume 2604, 2020, pp. 1224–1236.

[13] A. Berko, K. Aliekseyeva, Quality evaluation of information resources in web-projects, Actual Problems of Economics (2012) 226–234.

[14] O. Chereshnyuk, V. Panasyuk, S. Sachenko, A. Banasik, I. Golyash, Fuzzy-multiple approach in choosing the optimal term for implementing the innovative project, in: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE, 2017. URL: https://doi.org/10.1109/idaacs.2017.8095138. doi:10.1109/idaacs.2017.8095138.

[15] V. V. Morozov, O. V. Kalnichenko, O. O. O. M. Mezentseva, The method of interaction modeling on basis of deep learning the neural networks in complex it-projects, International Journal of Computing 19 (2020) 88–96.

[16] B. Rusyn, R. Tors'ka, M. Kobasyar, Application of the cellular automata for obtaining pitting images during simulation process of their growth, in: Advances in Intelligent Systems and Computing, Springer International Publishing, 2014, pp. 299–306. URL: https://doi.org/10.1007/978-3-319-02309-0_32. doi:10.1007/978-3-319-02309-0_32.

[17] M. F. Ak, M. Gul, Ahp–topsis integration extended with pythagorean fuzzy sets for information security risk analysis, Complex & Intelligent Systems 5 (2019) 113–126.

[18] T. I. Buldakova, D. A. Mikov, Comprehensive approach to information security risk management, in: CEUR Workshop Proceedings, volume 2081, 2017, pp. 21–26.

[19] Z. Li, Z. Li, Y. Shen, G. Zhang, Application of combined evaluation method based on comprehensive weight and gray-fuzzy theory in network security risk assessment, in: The International Conference on Computing Technology, Information Security and Risk Management (CTISRM2016), 2016, p. 38.

[20] H. D. Tsague, B. Twala, Investigation of carrier mobility degradation effects on mosfet leakage simulations, International Journal of Computing 15 (2016) 237–247.

[21] M. Dyvak, N. Porplytsya, V. Brych, N. Halysh, O. Tulai, Y. Shpak, Modeling of dynamics of the company's share in the solid fuel market, in: 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), IEEE, 2019. URL: https://doi.org/10.1109/acitt.2019.8779973. doi:10.1109/acitt.2019.8779973.

[22] S. Islam, H. Mouratidis, E. R. Weippl, An empirical study on the implementation and evaluation of a goal-driven software development risk management model, Information and Software Technology 56 (2014) 117–133. URL: https://doi.org/10.1016/j.infsof.2013.06.003. doi:10.1016/j.infsof.2013.06.003.

[23] M. Alali, A. Almogren, M. M. Hassan, I. A. Rassan, M. Z. A. Bhuiyan, Improving risk

assessment model of cyber security using fuzzy logic inference system, Computers & Security 74 (2018) 323–339. URL: https://doi.org/10.1016/j.cose.2017.09.011. doi:10.1016/j.cose.2017.09.011.

[24] Y. Li, H. Zhao, L. Zhu, Research on the construction of e-commerce security risk assessment model based on cloud computing, in: 2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), IEEE, 2019. URL: https://doi.org/10.1109/icmtma.2019.00135. doi:10.1109/icmtma.2019.00135.

[25] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C. e Silva, A. P. C. S. Costa, Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory, International Journal of Information Management 43 (2018) 248–260. URL: https://doi.org/10.1016/j.ijinfomgt.2018.08.008. doi:10.1016/j.ijinfomgt.2018.08.008.

[26] H. Beheshti, M. Alborzi, Using fuzzy logic to increase the accuracy of e-commerce risk assessment based on an expert system, Engineering, Technology & Applied Science Research 7 (2017) 2205–2209. URL: https://doi.org/10.48084/etasr.1479. doi:10.48084/etasr.1479.

[27] Y. Matseliukh, V. Vysotska, M. Bublyk, Intelligent system of visual simulation of passenger flows, in: CEUR Workshop Proceedings, volume 2604, CEUR-WS, 2020, pp. 906–920.

[28] R. Lynnyk, V. Vysotska, Y. Matseliukh, Y. Burov, L. Demkiv, A. Zaverbnyj, A. Sachenko, I. Shylinska, I. Yevseyeva, O. Bihun, DDOS attacks analysis based on machine learning in challenges of global changes, in: CEUR Workshop Proceedings, volume 2631, CEUR-WS, 2020, pp. 159–171.

[29] Y. Priyadi, The designing of measurement instrument for information technology risk assessment as a risk management strategy recommendation at sbupe bandung (2019).

[30] A. A. Al-Bakri, M. I. Katsioloudes, The factors affecting e-commerce adoption by jordanian SMEs, Management Research Review 38 (2015) 726–749. URL: https://doi.org/10.1108/mrr-12-2013-0291. doi:10.1108/mrr-12-2013-0291.

[31] Y. Liu, H. Ma, Z. Liu, H. Hui, Research on the evaluation system of e-commerce specialty based on topsis and analytic hierarchy process, Revista de la Facultad de Ingenieria 32 (2017) 626–632.