System for Determination of Legal Responsibility/Penalty for a Cybersecurity Breach

Tetiana Hovorushchenko[a], Alla Herts[b], Artem Boyarchuk[c] and Olga Pavlova[a]

[a] *Khmelnytskyi National University, Institutska str., 11, Khmelnytskyi, 29016, Ukraine*
[b] *Ivan Franko National University of Lviv, Universytetska str., 1, Lviv, 79000, Ukraine*
[c] *Tallinna Tehhnikaülikool, Ehitajate tee 5, Tallinn, 12616, Estonia*

Abstract

The conducted state-of-the-art on known solutions and decision support systems for cybersecurity domain showed that none of the known solutions are intended for determination of legal responsibility/penalty for a cybersecurity breach, although the need for such an automated tool in cyber structures and cyber organizations is considerable. Therefore, it is necessary to design and implement system for determination of legal responsibility/penalty for a cybersecurity breach. The paper simulates the process of determination of legal responsibility/penalty for a cybersecurity breach, which is the theoretical basis for developing the system for determination of legal responsibility/penalty for a cybersecurity breach. The authors have developed the system for determination of legal responsibility/penalty for a cybersecurity breach, which forms a decision as to whether a person has committed a cybersecurity breach(es). If the system establishes that a person has committed a cybersecurity breach(es), the system forms a conclusion on legal responsibility/penalty for the committed cybersecurity breach(es).

Keywords

Cybersecurity, cyber threat, cybersecurity breach, set of possible cybersecurity breaches, responsibility/penalty for a cybersecurity breach.

1. Introduction

The peculiarity of digitalization of society is that the main type of activity is the collection, accumulation, processing, production, storage, transfer and use of information. The main criteria for the effectiveness of digitalization of society are: efficiency of information transfer and processing, quality and quantity of available information, availability of information. So, to meet the requirements of the time and information society, companies are forced to use a huge number of sources of information in order to improve the results of their work [1-4].

The rapidly changing digital world requires the formation of a more balanced and effective cybersecurity system that can flexibly adapt to changes in the security environment, guaranteeing the safe functioning of cyberspace, foreseeing new opportunities for digitalization of all spheres of public life.

Today, the amount of information is constantly growing, effective and safe information management is becoming a critically important function, therefore the issue of information security is extremely acute and relevant. Cyber weapons are currently weapons of mass destruction in terms of consequences and effectiveness of use, so cybersecurity is currently a priority for many countries. The spread of cyber threats to all spheres of life and the improvement of tools for their implementation necessitates a change

ITTAP'2022: 2nd International Workshop on Information Technologies: Theoretical and Applied Problems, November 22–24, 2022, Ternopil, Ukraine

EMAIL: tat_yana@ukr.net (T. Hovorushchenko); agerc@ukr.net (A. Herts); a.boyarchuk@taltech.ee (A. Boyarchuk); olya1607pavlova@gmail.com (O. Pavlova)
ORCID: 0000-0002-7942-1857 (T. Hovorushchenko); 0000-0002-3310-3159 (A. Herts); 0000-0001-7349-1371 (A. Boyarchuk), 0000-0003-2905-0215 (O. Pavlova)

in the strategy and tactics of combating them. The fastest possible detection of vulnerabilities and cyberattacks, response and dissemination of information about them to minimize possible damage is gaining importance.

The technical level of implementing cyber threats is increasing, new tools and mechanisms of cyberattacks are constantly being improved and developed. No state today can be sure that its digital infrastructure is fully protected and can withstand cyberattacks. Cyberattacks on digital resources of critical infrastructure cause real threats to public safety, lead to human casualties, significant financial losses, and significant reputational damage. The tendency to use cyberattacks as a tool for special information operations, manipulation of public opinion, and influence on election processes is increasing.

The specific weight of cyber threats is growing, and this trend will intensify in the next decade as information technologies develop and converge with artificial intelligence technologies. The growth of such influence on the functioning of both national and transnational management structures creates a new security situation. The spheres of influence in cyberspace are being divided between the world's power centers, and their desire to ensure the realization of their own geopolitical interests is increasing due to such a division.

Today, when Russia's full-scale war against Ukraine is going on, Ukraine's cyber war with Russia is going on in parallel, during which Ukraine has turned into a testing ground for Russian hackers. Cyberspace, along with other physical spaces, is recognized as one of the theaters of war. According to the State Service of Special Communications and Information Protection of Ukraine, in the first 4 months of the war, 796 cyberattacks were carried out on the digital infrastructure of Ukraine (179 cyberattacks on the digital resources of the government and local authorities, 104 cyberattacks on the digital resources of the security and defense sector, 55 cyberattacks on digital resources of the financial sector, 54 cyberattacks on digital resources of commercial organizations, 54 cyberattacks on digital resources of the energy sector and 350 attacks on digital resources of other sectors). The most common methods of cyberattacks were: collection of information by an attacker (242 cyberattacks), malicious software code (192 cyberattacks), interference (92 cyberattacks), attempted interference (82 cyberattacks), accessibility violations (56 cyberattacks) [5].

So, at this moment, *the actual task* when using digital infrastructure is ensuring the cybersecurity, which is one of the priorities in the national security system of Ukraine. Most of the countries of the world apply complex measures to ensure cybersecurity – creation of structures responsible for ensuring cybersecurity, development and improvement of normative legal acts in the field of cybersecurity [6].

In Ukraine, criminal and civil responsibility is provided for cybercrimes according to the Criminal and Civil Codes of Ukraine, as well as according to the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine". In addition, on December 14, 2016, Ukraine signed the Agreement between Ukraine and the European Police Office on operational and strategic cooperation in cybersecurity domain. In the paper [7], the authors researched the legal and organizational principles of ensuring cybersecurity in the modern conditions of the development of the information society, and also developed a method and rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity.

The system for determination of legal responsibility/penalty for a cybersecurity breach can significantly increase the productivity of the cyber structures of Ukraine, which, based on the rules and method proposed by the authors in [7], will determine the sanctions recommended for this or that cybersecurity breach or a set of cybersecurity breaches. Designing such a system is *the goal of this study*.

2. State-of-the-Art

Let's conduct the state-of-the-art on known solutions and decision support systems for cybersecurity domain.

Cybersecurity requirements are influenced by the range of stakeholders: board members and Chief Information Security Officers (CISOs), managers, legal professionals. The paper [8] explores the effect that different experience has on the quality of a team's cybersecurity decision-making.

Assuring an organization's cybersecurity posture requires the active involvement of decision makers at all levels, particularly strategic level decision makers. These leaders have the responsibility of initiating security programs and are responsible for the security policy implementation. It is necessary that such leaders being provided with the tools for strategic and security management responsibilities [9].

Companies need to be cautious about confidence form consumers. The presence or absence of a previous cybersecurity breach had a large impact on confidence to company, but a minimal impact on intentions to be more secure [10].

International legal control of cyber operations emerges and develops through the optics of the law of war. The paper [11] analyses three key dimensions of the relationship between the law of war and general international law: systemic, conceptual, and teleological.

The study [12] employed Situational Crisis Communication Theory to address vulnerabilities and capabilities when data breaches take effect at hospitality organizations.

The purpose of the study [13] is to examine and overcome the risks to take advantage of opportunities through the Risky-Opportunity Analysis Method to increase the resilience of the system.

In [14] a structure for ensuring appropriate security, safety and privacy built into systems is proposed. In this structure, enforcement can be achieved by incentives or penalties. Determining the rules for optimization of the mix of penalties and incentives is a major goal of the paper [14].

The decision support system provides agility decisions for shortening the time a network is insecure in the event of a cyberattack. In the paper [15] decision support system "Cyber Fighter Associate (CyFiA)" is described for selecting the agility maneuvers with the purpose of containing and eliminating a malicious infection in a mobile network.

In [16] the decision support system is represented aimed at suggesting to operators of critical infrastructure the optimal configuration in terms of deployed security functions Ali ties. The decision support system has an optimization framework on the basis of genetic algorithm for exploring the solution space.

In the paper [17] the Information Security Maturity Model was proposed, that has four maturity level – None, Initial, Basic and Capable. The model provides the guideline for better management of information security and forms the best strategy for improving the overall information security state.

The information object cybersecurity operational management system is developed in [18] which is based on the morphological approach. The developed system provides reducing the cost of development of information security system and shortening the time for informing about information security incidents.

The goal of [19] is the development of basis from which can be attack a realistic networking environment where the intruder can bypass security measures thus exposing a vulnerability in the environment.

In [20] the web-based multi-perspective decision support system is developed on the basis of the multi-criteria decision framework with security and decision theory, which captures the complexity in a multi-criteria security control selection decision problem.

In [21] the FUSE-IT project is developed intending to propose a new paradigm: the convergence of monitoring on building and facilities, energy, cyber and physical security, and information technologies for leveraging the critical sites activities and detection of threats.

The paper [22] provides the analysis of mathematical models for choosing the investment strategies in cybersecurity systems of informatization objects in educational information systems. It is proposed to use the models on the basis of game theory as a basic mathematical model for such cybersecurity system.

In [23] a Nature-inspired Decision Support System for Secure Clustering (NIDSC), which classifies each node as either legitimate or attacker, is proposed for overcoming the security issues with minimum consumptions of resources and minimal computational overhead.

Authors of [24] developed a board game that simulates real-life environment and shows the challenges of organizations’ decision-making processes driving cyber-security strategy.

In [25] software is developed intending for supporting the cyber risks and cyber threats analysis of the information and communications technological infrastructure, and for support decision-making about prevention measures.

The conducted state-of-the-art on known solutions and decision support systems for cybersecurity domain showed that none of the known solutions are intended for determination of legal responsibility/penalty for a cybersecurity breach, although the need for such an automated tool in cyber structures and cyber organizations is considerable. Therefore, it is necessary to design and implement system for determination of legal responsibility/penalty for a cybersecurity breach.

3. Modeling of the Process of Determination of Legal Responsibility/Penalty for a Cybersecurity Breach

Let *CSB* is the set of cybersecurity breaches committed by a person (such a set can consist of one element or be empty).

In order to form a conclusion on the commitment of a cybersecurity breach and determining the responsibility/penalty for it, it is necessary to check whether a person has committed cybersecurity breaches, that is, whether there are elements in the set of cybersecurity breaches committed by a person, therefore *the criterion for the presence of a cybersecurity breach* will be as follows:

- if $CSB = \varnothing$, then the person did not commit cybersecurity breaches;
- if $CSB \neq \varnothing$, then the person has committed a cybersecurity breach(es). In this case, the legal responsibility/penalty for the committed cybersecurity breach(es) should be determined according to the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity, developed by the authors in [7].

Taking into account the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity developed by the authors in [7], *the set of possible cybersecurity breaches* that involve legal responsibility/penalty has the following form:

$$PCSB = \{ uai, ri, pcg, csd, cds, udi, ucdb, uci, vor, dmdm \}, \tag{1}$$

where *uai* – "unauthorized intervention in the operation of computers, their systems and networks, which led to the loss, leakage, blocking, falsification of information", *ri* – "repeat commission of the breach", *pcg* – "prior conspiracy of a group of persons", *csd* – "causing significant damage (100 or more times greater than the tax-free minimum)", *cds* – "creation, distribution, sale of malicious tools for unauthorized interference in the operation of computers, their systems and networks", *udi* – "unauthorized distribution of information with limited access (according to the current legislation), which is stored in computers, their systems and networks", *ucdb* – "unauthorized change, blocking, destruction of information", *uci* – "unauthorized copying, interception of information, which led to information leakage", *vor* – "violation of the rules of operation of computers, their systems and networks or the rules of information protection", *dmdm* – "deliberate mass distribution of messages that led to the failure or termination of the operation of computers, their systems and networks".

Taking into account the developed criterion for the presence of a cybersecurity breach and the set of possible cybersecurity breaches that involve legal responsibility/penalty (equation (1)), let's perform *modeling of the process of determination of legal responsibility/penalty for a cybersecurity breach*.

If *CSB* is the set of cybersecurity breaches committed by a person (such a set can consist of one element or be empty), then:

$$CSB = PCSB \cap RCSB, \tag{2}$$

where *RCSB* is the set of breaches committed by a person.

The general rule for making a decision on the determination of responsibility/penalty for a cybersecurity breach is as follows:

$$\begin{array}{c} \mathit{If}\ CSB = \varnothing \\ \mathit{then}\ "\mathit{person\ didn't\ commit\ cybersecurity\ breaches}" \\ \mathit{else}\ "\mathit{person\ has\ committed\ cybersecurity\ breach(es)\ and\ should\ be\ held\ legally\ responsible/punished}" \end{array}. \tag{3}$$

The conducted modeling of the process of determination of legal responsibility/penalty for a cybersecurity breach is the theoretical basis for developing the system for determination of legal responsibility/penalty for a cybersecurity breach.

4. System for Determination of Legal Responsibility/Penalty for a Cybersecurity Breach

Taking into account the results of the analysis of the legal and organizational foundations of cybersecurity provided by the authors in [7], as well as the modeling of the process of determination of legal responsibility/penalty for a cybersecurity breach carried out in chapter 3 of this paper, let's develop the system for determination of legal responsibility/penalty for a cybersecurity breach – Fig. 1.

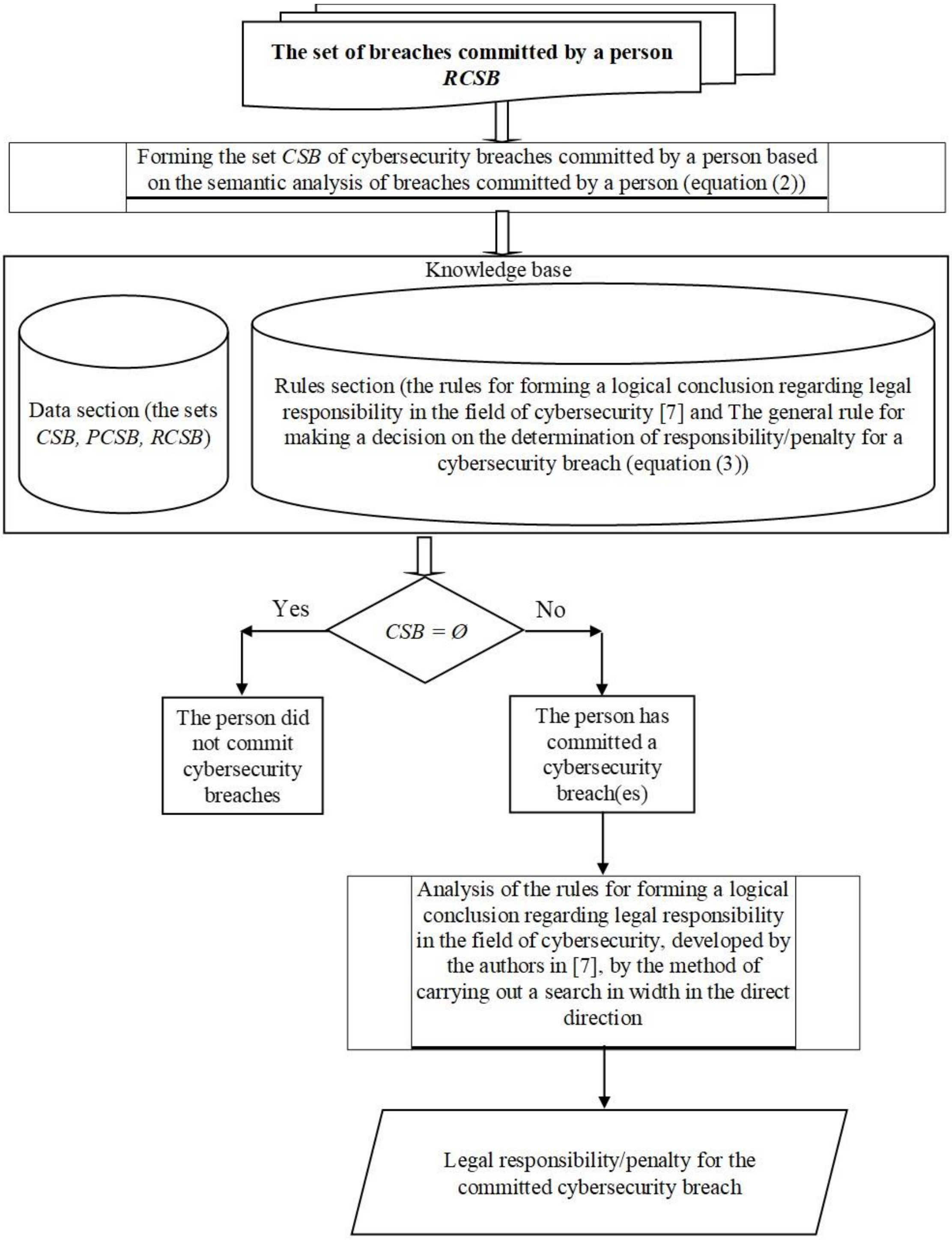
The set of breaches committed by a person *RCSB*
Forming the set *CSB* of cybersecurity breaches committed by a person based on the semantic analysis of breaches committed by a person (equation (2))
Knowledge base
Data section (the sets *CSB, PCSB, RCSB*)
Rules section (the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity [7] and The general rule for making a decision on the determination of responsibility/penalty for a cybersecurity breach (equation (3))
Yes
CSB = Ø
No
The person did not commit cybersecurity breaches
The person has committed a cybersecurity breach(es)
Analysis of the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity, developed by the authors in [7], by the method of carrying out a search in width in the direct direction
Legal responsibility/penalty for the committed cybersecurity breach

Figure 1: Structure of the system for determination of legal responsibility/penalty for a cybersecurity breach

The main source of information is a set *RCSB* of breaches committed by a person. Breaches committed by a person are analyzed by the system for the purpose of searching for cybersecurity breaches (for the purpose of searching for the values of the elements of the set *PCSB* of possible cybersecurity breaches). On the basis of this semantic analysis, a set *CSB* of cybersecurity breaches committed by a person is formed (such a set can consist of one element or be empty), according to equation (2) – if the value of an element of the set *PCSB* of possible cybersecurity breaches is found among the values of the elements of the set *RCSB* of breaches committed by a person, then this value is entered in the set *CSB* of cybersecurity breaches committed by the person.

All sets (*RCSB*, *PCSB*, *CSB*) are entered in the data section of the knowledge base. The rule section of the knowledge base contains the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity developed by the authors in [7], as well as the general rule for making a decision on the determination of responsibility/penalty for a cybersecurity breach (equation (3)).

Taking into account the presence/absence of elements in the set CSB of cybersecurity breaches committed by the person, a decision is made whether the person has committed a cybersecurity breach(es). If $CSB = \varnothing$, then the person did not commit cybersecurity breaches. If $CSB \neq \varnothing$, then the person has committed a cybersecurity breach(es). In this case, one should perform the analysis of the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity, developed by the authors in [7], using the method of carrying out a search in width in the direct direction, on the basis of which to determine the legal responsibility/penalty for the committed cybersecurity breach(es).

So, the system for determination of legal responsibility/penalty for a cybersecurity breach is developed, which forms a decision as to whether a person has committed a cybersecurity breach(es). If the system establishes that a person has committed a cybersecurity breach(es), the system forms a conclusion on legal responsibility/penalty for the committed cybersecurity breach(es).

5. Results & Discussion

Let's consider examples of the operation of the proposed system for determination of legal responsibility/penalty for a cybersecurity breach.

For *the first example*, we have the following set of breaches committed by the Person1 $RCSB_1$ = *{"unauthorized copying, interception of information, which led to information leakage", "repeat commission of the breach", "breach of hunting rules", "breach of traffic rules"}*. Breaches committed by a person are analyzed by the system for the purpose of searching for cybersecurity breaches (for the purpose of searching for the values of the elements of the set *PCSB* of possible cybersecurity breaches). On the basis of such semantic analysis, a set of cybersecurity breaches committed by a person is formed – for the first example CSB_1 = *{"unauthorized copying, interception of information, which led to information leakage", "repeat commission of the breach"}*.

Given the presence/absence of elements in the set *CSB* of cybersecurity breaches committed by the person, a decision is made whether the person has committed a cybersecurity breach(es). Since $CSB_1 \neq \varnothing$, then the Person1 has committed a cybersecurity breach(es). In this case, the system, as a result of the analysis of the rules for forming a logical conclusion regarding legal responsibility in the field of cybersecurity, developed by the authors in [7], using the method of carrying out a search in width in the direct direction, determined the legal responsibility/penalty for the committed cybersecurity breach(es) – according to rule 10, Person1 should be punished with deprivation of liberty for a period of three to six years with deprivation of the right to hold certain positions or engage in certain activities for a period of up to three years.

For the second example, we have the following set of breaches committed by the Person2 $RCSB_2$ = *{"violation of public order", "violation of curfew", "drinking alcoholic beverages on the playground"}*. Breaches committed by a person are analyzed by the system for the purpose of searching for cybersecurity breaches (for the purpose of searching for the values of the elements of the set PCSB of possible cybersecurity breaches). On the basis of such semantic analysis, a set of cybersecurity breaches committed by a person is formed – for the second example $CSB_2 = \varnothing$.

Given the presence/absence of elements in the set CSB of cybersecurity breaches committed by the person, a decision is made whether the person has committed a cybersecurity breach(es). Since $CSB_2 = \varnothing$, then the Person2 did not commit cybersecurity breaches.

The considered examples of the operation of the proposed system for determination of legal responsibility/penalty for a cybersecurity breach showed that the proposed system can significantly increase productivity and facilitate the work of cyber structures of Ukraine by determining whether a person has committed a cybersecurity breach, as well as determining the sanctions recommended by the current legislation of Ukraine this or that cybersecurity breach(es), if the system has determined that a cybersecurity breach(yi) has been committed.

6. Conclusions

At this moment, the actual task when using digital infrastructure is ensuring the cybersecurity, which is one of the priorities in the national security system of Ukraine. The system for determination of legal responsibility/penalty for a cybersecurity breach can significantly increase the productivity of the cyber structures of Ukraine, which will determine the sanctions recommended for this or that cybersecurity breach or a set of cybersecurity breaches.

The conducted state-of-the-art on known solutions and decision support systems for cybersecurity domain showed that none of the known solutions are intended for determination of legal responsibility/penalty for a cybersecurity breach, although the need for such an automated tool in cyber structures and cyber organizations is considerable. Therefore, it is necessary to design and implement system for determination of legal responsibility/penalty for a cybersecurity breach.

The paper simulates the process of determination of legal responsibility/penalty for a cybersecurity breach, which is the theoretical basis for developing the system for determination of legal responsibility/penalty for a cybersecurity breach.

The authors have developed the system for determination of legal responsibility/penalty for a cybersecurity breach, which forms a decision as to whether a person has committed a cybersecurity breach(es). If the system establishes that a person has committed a cybersecurity breach(es), the system forms a conclusion on legal responsibility/penalty for the committed cybersecurity breach(es).

7. References

[1] T. Hovorushchenko, O. Pavlova, D. Medzatyi. Ontology-Based Intelligent Agent for Determination of Sufficiency of Metric Information in the Software Requirements. Advances in Intelligent Systems and Computing 1020 (2020) 447-460. doi: 10.1007/978-3-030-26474-1_32.

[2] T. Hovorushchenko, O. Pomorova. Ontological Approach to the Assessment of Information Sufficiency for Software Quality Determination. CEUR-WS 1614 (2016) 332–348.

[3] O. Pomorova, T. Hovorushchenko. The Way to Detection of Software Emergent Properties, in Proceedings of the 2015 IEEE 8-th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015, vol. 2, p. 779-784. doi: 10.1109/IDAACS.2015.7341409.

[4] T. Hovorushchenko, O. Pomorova. Information Technology of Evaluating the Sufficiency of Information on Quality in the Software Requirements Specifications CEUR-WS 2104 (2018) 555-570.

[5] How russian cyberattacks changed during the war, 2022. URL: https://www.ukrinform.ua/rubric-technology/3518528-ak-zminilisa-rosijski-kiberataki-pid-cas-vijni.html.

[6] 33 Alarming Cybercrime Statistics You Should Know in 2019, 2019. URL: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/.

[7] T. Hovorushchenko, A. Herts, O. Pavlova. Method of Forming a Logical Conclusion about Legal Responsibility in the Cybersecurity Domain. CEUR-WS 2732 (2020) 128-135.

[8] B. Shreeve, J. Hallett, M. Edwards, K. Ramokapane, R. Atkins, A. Rashid. The Best Laid Plans or Lack Thereof: Security Decision-Making of Different Stakeholder Groups. IEEE Transactions on Software Engineering 48 5 (2022) 1515-1528. doi: 10.1109/TSE.2020.3023735.

[9] F. Garcia-Granados, H. Bahsi. Cybersecurity Knowledge Requirements for Strategic Level Decision Makers, in: Proceedings of 15th International Conference on Cyber Warfare and Security (ICCWS), Norfolk, 2020, pp. 559-568. doi: 10.34190/ICCWS.20.102.

[10] S. Curtis, J. Carre, D. Jones. Consumer security behaviors and trust following a data breach. Managerial Auditing Journal 33 4 (2018) 425-435. doi: 10.1108/MAJ-11-2017-1692.

[11] K. Macak. From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law, in: Proceedings of 9th International Conference on Cyber Conflict - Defending the Core (CyCon), Tallinn, 2017, pp. 135-148. doi: 10.23919/CYCON.2017.8240333.

[12] H. Chen, T. Jai. Cyber alarm: Determining the impacts of hotel's data breach messages. International Journal of Hospitality Management 82 (2019) 326-334. doi: 10.1016/j.ijhm.2018.10.002.

[13] A. Ardebili, E. Padoano, A. Longo, A. Ficarella. The Risky-Opportunity Analysis Method (ROAM) to Support Risk-Based Decisions in a Case-Study of Critical Infrastructure Digitization. Risks 10 3 (2022) No 48. doi: 10.3390/risks10030048.

[14] C. Axelrod. Enforcing Security, Safety and Privacy for the Internet of Things, in: Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT), Long Island, 2015, pp. 1-6. doi: 10.1109/LISAT.2015.7160214.

[15] C. Huber, P. McDaniel, S. Brown, L. Marvel. Cyber Fighter Associate: A Decision Support System for Cyber Agility, in: Proceedings of 50th Annual Conference on Information Science and Systems (CISS), Princeton, 2016, pp. 198-203. doi: 10.1109/CISS.2016.7460501.

[16] A. Tortorelli, A. Fiaschetti, R. Germana, A. Giuseppi, V. Suraci, A. Andreani, F. Delli Priscoli. A decision support tool for optimal configuration of critical infrastructures. International Journal of Critical Infrastructures 18 2 (2022) 105-127. doi: 10.1504/IJCIS.2022.10033792.

[17] S. Yulianto, C. Lim, B. Soewito. Information Security Maturity Model a Best Practice Driven Approach to PCI DSS Compliance, in: Proceedings of IEEE Region 10 Symposium (TENSYMP), 2016, Indonesia, pp. 65-70. doi: 10.1109/TENCONSpring.2016.7519379.

[18] V. Lakhno, A. Petrov, A. Petrov. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport. Advances in Intelligent Systems and Computing 656 (2018) 113-127. doi: 10.1007/978-3-319-67229-8_11.

[19] B. Sassani, R. Choque, B. Paul, F. Mehdipour. Commercial Security Scanning: Point-on-Sale (POS) Vulnerability and Mitigation Techniques, in: Proceedings of IEEE 17th International Conference on Dependable, Autonomy and Secure Computing / IEEE 17th International Conference on Pervas Intelligence and Computing / IEEE 5th International Conference on Cloud and Big Data Computing / IEEE 4th Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, 2019, pp. 493-498. doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00099.

[20] O. El-Gayar, B. Fritz. A web-based multi-perspective decision support system for information security planning. Decision Support Systems 50 1 (2020) 43-54. doi: 10.1016/j.dss.2010.07.001.

[21] H. Pouyllau, B. Istasse, S. Ahvar, N. Crespi, I. Praca, S. Garcia-Rodriguez, E. Mengusoglu. FUSE-IT: Enhancing Critical Site Supervision with Cross-Domain Key Performance Indicators, in: Proceedings of Global Information Infrastructure and Networking Symposium (GIIS), Porto, 2016, pp. 1-6. doi: 10.1109/GIIS.2016.7814850.

[22] B. Akhmetov, V. Lakhno, A. Adranova, L. Kydyralina, L. Pliska. Bulletin of The National Academy of Sciences of the Republic of Kazakhstan 1 (2020) 128-139. doi: 10.32014/2020.2518-1467.16.

[23] S. Qureshi, S. Shandilya. Nature-inspired adaptive decision support system for secured clustering in cyber networks. Multimedia Tools and Applications (2022). doi: 10.1007/s11042-022-13336-7.

[24] S. Zeijlemaker, E. Rouwette, G. Cunico, S. Armenia, M. Von Kutzschenbach. Decision-Makers' Understanding of Cyber-Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers. Systems 10 2 (2022) No 49. doi: 10.3390/systems10020049.

[25] G. Roldan-Molina, M. Almache-Cueva, C. Silva-Rabadao, I. Yevseyeva, V. Basto-Fernandes. A Decision Support System for Corporations Cybersecurity Management, in: Proceedings of 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, 2017, pp. 1-6. doi: 10.23919/CISTI.2017.7975826.