Method of Forming a Logical Conclusion about Legal Responsibility in the Cybersecurity Domain

Tetiana Hovorushchenko [1[0000-0002-7942-1857]], Alla Herts [2[0000-0002-3310-3159]] and Olga Pavlova [3[0000-0003-2905-0215]]

[1, 3] Khmelnytskyi National University, Instytutska str., 11, Khmelnytskyi, Ukraine
[2] Ivan Franko National University of Lviv, Universytetska str., 1, Lviv, Ukraine
[1] tat_yana@ukr.net
[2] agerc@ukr.net
[3] olya1607pavlova@gmail.com

Abstract. Cyber attacks on critical infrastructure's objects can have dire consequences, as our entire lives depend on the working capacity of such systems. In Ukraine, cybercrime provides for criminal and civil liability under the Criminal and Civil Codes of Ukraine, and under the Law of Ukraine "On the Fundamental Principles of Cyber Security in Ukraine". A successfully implemented decision-making support system that can provide a conclusion of legal responsibility in the cybersecurity domain, namely, propose sanctions recommended in the case of an offence or multiple offences, can significantly improve the productivity of the Ukrainian cyber police. This paper explores the legal and organizational principles of cybersecurity in today's information society, and first time develops the method and production rules of forming a logical conclusion about legal responsibility in the cybersecurity domain, that are used to form the conclusion about legal responsibility, namely for the selection of a sanction or set of sanctions recommended in the event of a particular offence or multiple cyber-security offences.

Keywords: cybersecurity, cyberattacks, cybersecurity offences, sanctions, legal responsibility in the cybersecurity domain, logical conclusion about legal responsibility in the cybersecurity domain.

1 Introduction

The modern development of an information society is directly linked to the need to collect, process and transmit vast amounts of information. The main criteria of the information society are the amount and quality of available information, the efficiency of its transmission and processing, the accessibility of information for everyone. So, information management is becoming a business-critical function. So the main strategic goal of the development of the information society in Ukraine is providing the security and protection of information. The issue of information security becomes more acute [1].

Cyber-attacks on critical infrastructure's systems pose real threats to the safety of the human community, lead to human casualties, environmental disasters, and significant financial losses.

Today, on a monthly basis, Ukraine undergoes cyber attacks 3000-3500 times. In the last 12 months, every second industrial company in the world has experienced one to five cyber incidents. The loss of the world economy as a result of cyber-attacks is 445 billion USD. Losses to Ukrainian businesses caused by the cyber-attacks amount to 25 million USD [2]. Every 4 seconds an unknown malware is downloaded – Fig. 1 [3].

Fig. 1. An Average Day at an Enterprise Organization [3].

So *the actual problem* with using computer systems is the robust protection of information against cyber threats.

Therefore, most countries in the world carry out comprehensive measures to ensure national cybersecurity. These measures relate, first and foremost, to the development and improvement of regulations, as well as to the establishment of departmental and state structures that regulate and be responsible for ensuring the security in the cyberspace [4].

In 2001, the European Commission presented the first document entitled "Network and Information Security: A Proposal for A European Policy Approach" [5]. The European Union Agency for Network and Information Security (ENISA) was established on 10 March 2004 [6]. In May 2007, the European Commission presented the document "Towards a general policy on the fight against cybercrime" [7]. European Commission policy on cybercrime opposition encourages the signing by the EU Member States and other countries of the Convention on Cybercrime. The message of the European Commission “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” [8] was published in March 2009. On February 7, 2013, the European Commission approved the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [9]. The European CyberCrime Center was

established in Europol (European Police Office), which started its operations in January 2013 in The Hague (Netherlands). On 6 July 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [10] was adopted. On 13 September 2017, the European Commission presented the document "Resilience, Deterrence and Defense: Building strong cybersecurity for the EU" [11]. Every year, the European Cybercrime Center publishes an Internet Organised Crime Threat Assessment (IOCTA) [12]. On December 14, 2016, Ukraine signed an Agreement between Ukraine and the European Police Office on operational and strategic cooperation [13].

In Ukraine, cybercrime provides for criminal and civil liability under the Criminal Code [14] and the Civil Code [15] of Ukraine (Articles 277, 278, 280), as well as under the Law of Ukraine "On the Fundamental Principles of Cyber Security in Ukraine" [16].

2 Problem Statement

A successfully implemented decision-making support system that can provide a conclusion about legal responsibility in the cybersecurity domain, namely, propose sanctions recommended in the case of an offence or multiple offences, can significantly improve the productivity of the Ukrainian cyber police. For developing this decision support system, a method and production rules of forming a logical conclusion about legal responsibility in the cybersecurity domain should be developed, which is *the purpose of this research*.

Such a decision support system, like any decision support system (DSS), can be represented as a formal system:

$$C = <A, PR, M>, \quad (1)$$

where *C* is the set of alternatives (conclusions) that are generated by DSS; *A* is the set of the basic elements (set of actions (offences), which entail certain sanctions under the current legislation of Ukraine); *PR* is the set of rules by which alternatives are generated for objects with *A*; *M* are methods used in data processing.

The DSS inputs (set *A*) are actions (offences), which entail certain sanctions under the current legislation of Ukraine. The outputs of the DSS (set *C*) are the results of the data analysis, on the basis of which the decisions are generated, as well as the decisions (conclusions about the sanction(s), which recommended in the case of committing an action (offence) or a few actions (offences)). Then the relationship between the input and output parameters is a mathematical description of DSS:

$$C=M(A), \quad (2)$$

where *M* is a method that allows to parameters of *A* to match an alternative of *C* using the production rules of *PR*.

In order to achieve the purpose of this research, *the following tasks* must be solved:

- developing the production rules (set *PR*) and method (*M*) of forming a logical conclusion about legal regulations in the cybersecurity domain;

- design of decision support system for forming a logical conclusion about legal regulations in the cybersecurity domain, for the selection of sanctions, which are recommended in the case of the cybersecurity offence or multiple offences.

3 Production Rules and Method of Forming a Logical Conclusion about Legal Responsibility in the Cybersecurity Domain

First of all, we will develop production rules of forming a logical conclusion about legal responsibility in the cybersecurity domain (set *PR = {pr1,…, pr13}*) based on the norms of the Criminal [14] and the Civil [15] codes of Ukraine (Articles 277, 278, 280), and the norms of the Law of Ukraine "On the Fundamental Principles of Cyber Security in Ukraine" [16].

For this purpose, we will form a set of actions (offences), which entail certain sanctions under the current legislation of Ukraine: *A = {a1,…, a10}*, where *a1* – unauthorized interference with the operation of computers, automated systems, computer networks or telecommunication networks, that have led to leakage, loss, tampering, blocking of information, distortion of the information processing process or disruption of established routing order; *a2* – re-committing; *a3* – preliminary conspiracy of a group of persons; *a4* – causing significant damage (damage that exceeds the tax-free minimum income of citizens 100 times or more); *a5* – creation for the purpose of use, distribution or sale, as well as distribution or sale of malicious software or hardware, which intended for unauthorized interference with the operation of computers, automated systems, computer networks or telecommunication networks; *a6* – unauthorized sale or distribution of restricted information, which stored in computers, automated systems, computer networks or on special media of such information; *a7* – unauthorized modification, destruction or blocking of information, that is processed in computers, automated systems or computer networks or stored on special media of such information; *a8* – unauthorized interception or copying of information, that is processed in computers, automated systems, computer networks or stored on special media of such information, which led to information leakage; *a9* – violation of the rules of operation of computers, automated systems, computer networks, telecommunication networks or of the order or rules of protection of the processed information, which caused significant damage; *a10* – intentional mass distribution of messages, which was made without the prior consent of the addressees, that has led to the disruption or termination of the operation of computers, automated systems, computer networks or telecommunication networks.

Given the set of actions (offences) *A, the production rules of forming a logical conclusion about legal regulations in the cybersecurity domain* are the set *{pr1,…,pr13}*:

pr1="if the person has committed action *a1*, then and only then such person shall be punished by a fine of six hundred to one thousand tax-free minimum incomes, or by restriction of liberty for a term of two to five years, or imprisonment for up to three years, with deprivation of the right to occupy certain positions or engage in certain activities for a term up to two years";

pr2="if the person has committed action *a1* and action *a2* and/or action *a3* and/or action *a4*, then and only then such person shall be punished by imprisonment for a

term of three to six years, with deprivation of the right to occupy certain positions or engage in certain activities for up to three years";

pr3="if the person has committed action *a5*, then and only then such person shall be punished by a fine of five hundred to one thousand tax-free minimum incomes, or by correctional labour for a term up to two years, or imprisonment for the same term";

pr4="if the person has committed action *a5* and action *a2* and/or action *a3* and/or action *a4*, then and only then such person shall be punished by imprisonment for a term up to five years";

pr5="if the person has committed the action *a6*, then such person shall be punished by a fine of five hundred to one thousand tax-free minimum incomes, or imprisonment for a term up to two years";

pr6="if the person has committed action *a6* and action *a*2 and/or action *a3* and/or action *a4*, then and only then such person shall be punished by imprisonment for a term of two to five years";

pr7="if the person has committed action *a7*, then and only then such person shall be punished by a fine of six hundred to one thousand tax-free minimum incomes or corrective labour for a term up to two years";

pr8="if the person has committed action *a7* and action *a2* and/or action *a3* and/or action *a4*, then and only then such person shall be punished by imprisonment for a term of three to six years, with deprivation of the right to occupy certain positions or engage in certain activities for up to three years";

pr9="if the person has committed the action *a8*, then and only then such person shall be punished by imprisonment for a term up to three years, with deprivation of the right to occupy certain positions or engage in certain activities for the same term";

pr10=" if the person has committed action *a8* and action *a2* and/or action *a3* and/or action *a4*, then and only then such person shall be punished by imprisonment for a term of three to six years, with deprivation of the right to occupy certain positions or engage in certain activities for up to three years";

pr11="if the person has committed action *a9*, then and only then such person shall be punished by a fine of five hundred to one thousand tax-free minimum incomes, or a restriction of liberty for a term up to three years, with deprivation of the right to occupy certain positions or engage in certain activities for the same term";

pr12="if the person has committed action *a10*, then and only then such person shall be punished by a fine of five hundred to one thousand tax-free minimum incomes, or by restriction of liberty for a term up to three years";

pr13="if the person has committed action *a10* and action *a2* and/or action *a3* and/or action *a4*, then and only then such person shall be punished by restriction of liberty for a term up to five years, with deprivation of the right to occupy certain positions or engage in certain activities for up to three years".

On the basis of the developed production rules, we will develop the *method of forming a logical conclusion about legal regulations in the cybersecurity domain*:

1. the set of actions (offences) $A_{real} = \{a1_{real}, \ldots, an_{real}\}$, which are committed by the offender, is formed, where n is the number of offences committed by a concrete offender;

2. by the method of searching in the breadth in the forward direction, in the set of production rules *{pr1,…,pr13}*, a rule(s) is(are) searched for each of the elements of the set $\{a1_{real},\ldots,an_{real}\}$;
3. according to the selected rules, the conclusion is drawn about the sanction(s), which recommended in the case of committing an action (offence) or a few actions (offences); if the rule is not found, then there is no sanction(s) accordance with the modern legislation of Ukraine.

The scheme of the developed method of forming a logical conclusion about legal regulations in the cybersecurity domain is represented on Fig. 2.

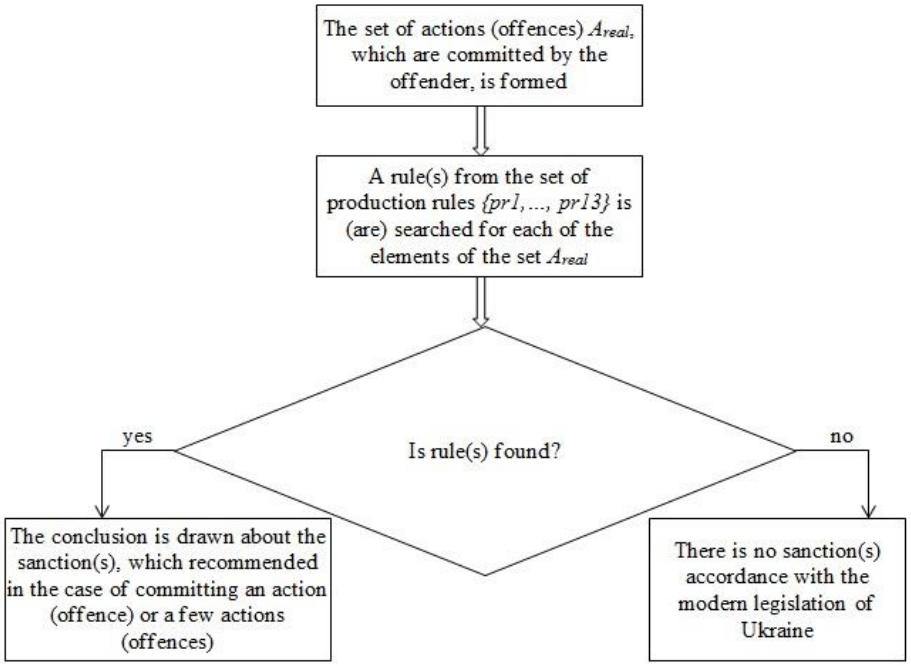

Fig. 2. The scheme of the developed method of forming a logical conclusion about legal regulations in the cybersecurity domain.

4 Results & Discussions

Examples of forming a logical conclusion about legal regulations in the cybersecurity domain. Person1 has created and distributed a new computer virus *V1*, which is designed for unauthorized interference with the operation of the computer network of Enterprise1. Then for this case the set A_{real} = {"creation for the purpose of use, distribution or sale, as well as distribution or sale of malicious software or hardware, which intended for unauthorized interference with the operation of computers, automated systems, computer networks or telecommunication networks"}. In the set of production rules, the search of rule for the action (offence) from the set A_{real} is

executed – this is *pr3*. According to this rule, the conclusion about the sanction, which recommended in the case of committing this action (offence), has the form: "*Person1 shall be punished by a fine of five hundred to one thousand tax-free minimum incomes, or by correctional labour for a term up to two years, or imprisonment for the same term*".

Person2 perefromed unauthorized modification of information, that is processed in automated system of Enterprise2. Then for this case the set A_{real} = {"unauthorized modification, destruction or blocking of information, that is processed in computers, automated systems or computer networks or stored on special media of such information"}. In the set of production rules, the search of rule for the action (offence) from the set A_{real} is executed – this is *pr7*. According to this rule, the conclusion about the sanction, which recommended in the case of committing this action (offence), has the form: "*Person2 shall be punished by a fine of six hundred to one thousand tax-free minimum incomes or corrective labour for a term up to two years*".

Discussions. The authors analyzed the materials of 20 cases initiated against persons who committed cybersecurity offences, in which the court decided to return for revision to the cyber police due to incorrectly formulated requests for sanctions. Analysis of the data from these cases using the developed rules method of forming a logical conclusion about legal regulations in the cybersecurity domain showed that if the developed method was used before the case was sent to court, all correct decisions on the necessary sanction would be made. Therefore, the use of developed rules and methods can increase the level of correctness of decisions on the required sanction to 100%. Thus, the decision support system for the selection of sanctions, which are recommended in the case of cybersecurity offences or multiple offences, will provide rapid and automatic verification of all cases against perpetrators of cybersecurity offences, in terms of the choice of sanctions for such persons.

5 Conclusions

At present, in the age of the information society, cyber weapons in terms of efficiency and impact can be equated with weapons of mass destruction. The faster humanity develops information technologies, the greater is the need to protect them, to ensure their cybersecurity. Today, no state can say with certainty that its networks are fully secure and able to withstand multi-vector cyberattacks, so cybersecurity has become a priority in many countries. At first glance, it may seem that cyberattacks cannot do much harm or take lives, but attacks on critical infrastructure's objects can have dire consequences, since our entire lives depend on the working capacity of such systems.

A successfully implemented decision-making support system that can provide a conclusion of legal responsibility in the cybersecurity domain, namely, propose sanctions recommended in the case of an offence or multiple offences, can significantly improve the productivity of the Ukrainian cyber police.

This paper first time develops the method and production rules of forming a logical conclusion about legal responsibility in the cybersecurity domain, that are used to form the conclusion about legal responsibility, namely for the selection of a sanction(s) recommended in the event of a particular offence or multiple cyber-security offences.

The perspective directions of future authors' work are the designing, developing and implementing the decision support system for the selection of sanctions, which are recommended in the case of the cybersecurity offence or multiple offences. The basis of such the system will be developed in this paper production rules and method of forming a logical conclusion about legal responsibility in the cybersecurity domain.

References

1. Hovorushchenko, T., Pomorova, O.: Information Technology of Evaluating the Sufficiency of Information on Quality in the Software Requirements Specifications. CEUR-WS. 2104. 555-570 (2018).
2. 33 Alarming Cybercrime Statistics You Should Know in 2019, https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/, last accessed 2020/03/09.
3. Check Point's 2019 Security Report, https://blog.checkpoint.com/2019/03/04/check-points-2019-security-report/, last accessed 2020/03/09.
4. Voytsikhovskyi, A.: Cybersecurity as an important component of the national security system of European countries. Journal of Eastern European Law. 53. 26-37 (2018). (in Ukrainian)
5. Network and Information Security: Proposal for A European Policy Approach, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298, last accessed 2020/03/09.
6. About ENISA, https://www.enisa.europa.eu/about-enisa, last accessed 2020/03/09.
7. Towards a general policy on the fight against cybercrime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560, last accessed 2020/03/09.
8. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149, last accessed 2020/03/09.
9. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667, last accessed 2020/03/09.
10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, last accessed 2020/03/09.
11. Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN, last accessed 2020/03/09.
12. Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment, last accessed 2020/03/09.
13. Agreement between Ukraine and the European Police Office on operational and strategic cooperation: international agreement of 14.12.2016, URL:http://zakon3.rada.gov.ua/laws/show/984_001-16/paran2#n2, last accessed 2020/03/09.
14. Criminal Code of Ukraine – Information of the Verkhovna Rada of Ukraine. 25-26 (2001).
15. Civil Code of Ukraine – Information of the Verkhovna Rada of Ukraine. 40-44 (2003).
16. Law of Ukraine "On the Fundamental Principles of Cyber Security in Ukraine" – Information of the Verkhovna Rada of Ukraine. 45 (2017).