Intellectual analysis and basic modeling of complex threats

Nikolai Korneev
Faculty of Integrated Security of Fuel and Energy Complex
Gubkin Russian State University of Oil and Gas (National Research University)
Department of Data Analysis, Decision-Making and Financial Technology
Financial University under the Government of the Russian Federation
Moscow, Russia
niccyper@mail.ru

Vyacheslav Merkulov
Faculty of Integrated Security of Fuel and Energy Complex
Gubkin Russian State University of Oil and Gas (National Research University)
Moscow, Russia
niccyper@mail.ru

***Abstract*—The paper describes the basic principles of complex threats modeling, and the task of complex threats detection is formalized. The proposed modeling principles are based on the idea of identifying the links between elementary threats as part of a complex one. As an example, the process of constructing a complex threat model based on the proposed modeling rules is given. Based on the examples presented in the work, the paper includes the description of tasks while working with complex threats: the tasks of complex threats detection, the identification of their inner structure and purposes of the implementation. Based on the formulated principles of basic modeling, the paper also gives a formal statement of complex threats detection problem, which explains the possibility for applying data mining algorithms and big data processing technologies in the construction of protection systems against complex threats and developing the neurographic theory of complex security.**

Keywords— complex threats; complex threat model ; complex security; hybrid threats; complex threats detection; complex threats detection method ; data mining algorithms; big data processing, neurographic theory of complex security

TERMS USED

Protected system – a system in the conventional sense, consisting of many security objects, not necessarily located in one space.

Complex threat – a threat consisting of several different elementary threats, connected by means of certain synchronized mechanisms and not necessarily existing in one space.

Hybrid threat – a variation of a complex threat, which necessarily contains elementary threats that affect different areas of the protected system.

Exploited threat vulnerability – a factor based on the properties of the protected system or methods of protection, which is used in the implementation of a specific elementary threat.

Threat implementation mechanism – a set of actions, which actively use available exploited vulnerabilities and are aimed at the threat implementation.

Consequences of threat implementation – a factor that is caused by a specific threat implementation; it can have a negative impact on the protected system or it can be an exploited vulnerability for another threat.

I. INTRODUCTION

Scientific publications of both domestic and foreign scientists [1-3, 7, 11-13, 15-20] show that in domestic and foreign literature and practice in this area, rigorous mathematical models with criteria of control support efficiency in the field of comprehensive security generally do not exist, and the existing comprehensive security systems do not solve the task of automated building a component-based model of a facility as part of comprehensive facility safety control support [9].

In the case where the finite number of states of the controlled facility at each moment of time is unknown, it is advisable to use a more sophisticated model similar neurographic model [9].

In retrospect, security threats were considered as atomic units unconnected to each other. This approach has led to the fact that elementary threats are currently well studied and classified [5, 6], effective hardware and software solutions have been developed to ensure security against them, also organizational and legal methods, general principles of security are widely used.

In practice, when analyzing security incidents and risks, it often becomes obvious that there are internal links between a set of elementary threats, which form a system.

The presence of certain properties in this system allows us to consider the constituent elements of the system not as atomic (elementary) threats, but as a complex security threat.

The paper contains an example of the formation and implementation of a complex threat consisting of several elementary threats connected in a certain way.

It is also worth noting that the existence of hybrid threats is closely related to the term “hybrid war” [4, 8, 10]. These are subtypes of complex threats and characterized by the property

of forming and implementing the threat components not in a single space (for example, only in the physical) and in several spaces simultaneously (for example, in physical and information space).

Complex threats, as a separate type of threat, require the creation of theoretical foundations for security; on their basis, it is possible to ensure the development of appropriate integrated security systems.

II. BASIC MODEL OF COMPLEX THREAT

As an object of research, complex threats require certain methods of formalization, i. e. principles and tools for modeling, which are currently missing. The following are the rules for basic models formation of complex threats.

The complex threat C can be represented as a combination of a set (1) of the elementary threats T and a set R of interconnections between them:

$$C = <T, R>; \quad |T| > 1; \quad |R| > 1. \tag{1}$$

The elementary threat $t_i \in T$ consists of (2) (3) non-empty sets of exploited vulnerabilities V, mechanisms for implementing M and consequences of implementing threat A:

$$t_i = < V_{t_i}, M_{t_i}, A_{t_i} >, \tag{2}$$

$$V_{t_i} = \{v_1, v_2, \dots, v_n\};$$

$$M_{t_i} = \{m_1, m_2, \dots, m_k\}, \tag{3}$$

$$A_{t_i} = \{a_1, a_2, \dots, a_p\}.$$

To avoid further conglomeration of indexes, we consider records of the form v_1 equivalent to $v^{(1)}$.

A link $r_{i,j} \in R$ between elementary threats t_i and t_i exists, if at least, one consequence of the threat implementation t_i ($a_p \in A_{t_i}$) is an exploited threat vulnerability ($v_n \in V_{t_j}$), i. e. between a_p and v_n there is some equivalence relation.

Thus, the set R can be represented as a two-dimensional matrix, the rows and columns of which contain elements of the set T, and at the intersection of i row and j column there is an element $r_{i,j}$, showing the existence of a connection between threats t_i and t_j.

The nature of such a connection is an open question for further research, however, in a simplified version it is proposed to use binary values for elements of the set R (there is either a connection, then $r_{i,j} = 1$, or not, in this case $r_{i,j} = 0$) (4).

$$r_{i,j} = \begin{Bmatrix} 1, \exists\, a_p \in A_{t_i}, (a_p \sim v_n) \wedge (v_n \in V_{t_j}) \\ 0, \text{otherwise} \end{Bmatrix}. \tag{4}$$

The above-mentioned modeling principles allow you to make a formalized model of a complex threat, which has a minimum set of parameters for further research.

III. EXAMPLE OF BUILDING A BASIC MODEL OF A COMPLEX THREAT

Let us consider an example of the formation and implementation of a complex threat, which can be called hybrid, as elementary attacks in its composition exist in different spaces.

Example: a group of intruders implements a hybrid threat against a FEC enterprise. The purpose of the attack is to cause economic and reputational damage to the enterprise; the subject of the attack – confidential information of loyalty cards of end-use customers; the protected system is directly a FEC enterprise. In this example, the hybrid threat is implemented in several stages:

1. Exploiting software vulnerability in corporate PACS, inaccurate data is added to the identification code database.

2. Having the ability to pass the perimeter of physical protection freely, since there are false entries in PACS database, the intruder penetrates into the protected area.

3. While in the protected area, the intruder detects a storage medium, which contains confidential data and creates its physical copy.

4. Copied confidential information distributes to public sources, which causes economic and reputational damage to the protected system.

Reputational damage involves the reduction of the consumer trust to the company's ability to ensure the protection of personal customer data.

The economic damage involves loyalty cards usage without the need for their legal acquisition and participation in the loyalty program, as you can purchase stolen data from the intruder.

We formalize this example of a hybrid threat into a basic model. Its general view (5):

$$C = <T, R>; \quad |T| = 4; \quad |R| = 4. \tag{5}$$

Let us consider the structure of elementary threats t_1, t_2, t_3, t_4 and correlations r between them.

To simplify the model, the power of the sets V, M, A of every elementary threat is equal to one, i. e. $|V| = 1$, $|M| = 1$, $|A| = 1$ for all $t \in T$.

Further, we consider the problem of modeling non-obviousness and threat implementation, especially hybrid threats, that depends on the power of the sets V, M, A.

In this example, the elementary threat t_1 arises, implements and generates consequences only in the information space, as it is based in the PACS software vulnerability and implements by the intruder distantly, changing the reliability and accuracy of the confidential database (6):

$$t_1 = < V_{t_1}, M_{t_1}, A_{t_1} >, \tag{6}$$

$$V_{t_1} = \begin{Bmatrix} \text{software vulnerability} \\ \text{in the identifier store PACS} \end{Bmatrix};$$

$$M_{t_1} = \{\text{exploiting a software vulnerability}\};$$

$$A_{t_1} = \begin{Bmatrix} \text{violation of data reliability} \\ \text{in the identifier store} \end{Bmatrix}.$$

The elementary threat t_2 arises in the information space, as it is based on unreliable data in the identifier store; implemented in the physical space by penetration of the intruder into the protected area; also produces consequences in physical space, providing the intruder with access to physical storage media (7):

$$t_2 = < V_{t_2}, M_{t_2}, A_{t_2} >, \quad (7)$$

$$V_{t_2} = \begin{Bmatrix} \text{violation of data reliability} \\ \text{in the identifier store} \end{Bmatrix};$$

$$M_{t_2} = \begin{Bmatrix} \text{penetration into the protected} \\ \text{area via PACS} \\ \text{without being detected} \end{Bmatrix};$$

$$A_{t_2} = \{\text{access to physical storage media}\}.$$

The elementary threat t_3 arises in the physical space, because it is based on access factor of the intruder to physical storage media; it also implements in the physical space, using the media copy mechanism; generates consequences in the information space, that is characterized by the possession of confidential information (8):

$$t_3 = < V_{t_3}, M_{t_3}, A_{t_3} >, \quad (8)$$

$$V_{t_3} = \{\text{access to physical storage media}\};$$

$$M_{t_3} = \{\text{copying of the physical storage media}\};$$

$$A_{t_3} = \{\text{access to confidential data}\}.$$

The elementary threat t_4 arises and is implemented in the information space, it means that an intruder has a confidential access and has the ability to distribute the confidential data to general public; however, threat implementation generates consequences in the economic and social spaces, damaging the company's reputation and the financial performance of the company (9):

$$t_4 = < V_{t_4}, M_{t_4}, A_{t_4} >, \quad (9)$$

$$V_{t_4} = \{\text{access to confidential data}\};$$

$$M_{t_4} = \{\text{confidential data distribution}\};$$

$$A_{t_4} = \begin{Bmatrix} \text{image and economic} \\ \text{damage to the enterprise} \end{Bmatrix}.$$

As the sets V, M, A were presented in a simplified form, the elements of the set R are also easy to model (10):

$$V_{t_2} \sim A_{t_1} \rightarrow r_{1,2} = 1;$$
$$V_{t_3} \sim A_{t_2} \rightarrow r_{2,3} = 1; \quad (10)$$
$$V_{t_4} \sim A_{t_3} \rightarrow r_{3,4} = 1.$$

For clarity, we also give the matrix form, representing the set R in this case (Fig. 1).

	t_1	t_2	t_3	t_4
t_1	0	1	0	0
t_2	0	0	1	0
t_3	0	0	0	1
t_4	0	0	0	0

Fig. 1. Mapping elements of the set R in the matrix form

In fact, the represented matrix is a connectivity matrix for a directed graph (Fig. 2).

Fig. 2. Representation of the C model as a directed graph

The construction of such kind of graphs allows you to visualize the investigated complex threats and the correlation of elementary threats.

As illustrated in the considered example, the proposed system of complex threats modeling can be used as a theoretical basis for constructing formalized descriptions of complex threats for their further analysis.

IV. PROBLEMATICS OF COMPLEX THREATS

The assumption about the sets V, M, A power is made to simplify the understanding of the example. In practice, as it was shown (2) (3), these sets are strictly non-empty, and their power can be quite large. We give an example of a complete composition of these sets based on t_2 (11):

$$V_{t_2} = \left\{ \begin{array}{c} \text{violation of data reliability} \\ \text{of the identifier store;} \\ \text{PACS is unequipped by} \\ \text{supplementary power supply;} \\ \text{recruitment of a company employee;} \\ \text{blackmailing a company employee;} \\ \text{presence of weaknesses in the} \\ \text{physical guard band (obstacles);} \\ \text{the possibility of a power outage.} \end{array} \right\};$$

$$M_{t_2} = \left\{ \begin{array}{c} \text{penetration into the} \\ \text{protected area via PACS} \\ \text{without being detected;} \\ \text{penetration into the territory} \\ \text{during the PACS shutdown;} \\ \text{using ID of recruited} \\ \text{agent to evade PACS;} \\ \text{penetration through the} \\ \text{weak point of physical obstacles.} \end{array} \right\}; \quad (11)$$

$$A_{t_2} = \left\{ \begin{array}{c} \text{access to physical storage media;} \\ \text{physical access to workstations;} \\ \text{physical access to servers;} \\ \text{physical access to internal} \\ \text{computer communication;} \\ \text{physical access to internal} \\ \text{electric service lines;} \\ \text{physical access to the} \\ \text{fire protection system.} \end{array} \right\}.$$

A deeper analysis of vulnerabilities can give the full composition of the sets V, M, A, however, we will focus on the above example and make a few remarks:

Comment 1. It is obvious that between the elements of sets V and M must also be a certain connection. In this example, the presence of the intruder inside the protected system (vulnerability $v_{t_2}^{(3)}$ or $v_{t_2}^{(4)}$) allows not only to use its ID to deceive the PACS (mechanism $m_{t_2}^{(3)}$), but also to break the power supply of the PACS (vulnerability $v_{t_2}^{(6)}$), then penetrate the area while PACS' inoperability (mechanism $m_{t_2}^{(2)}$).

According to the authors, this connection can be defined as follows: for an intruder to be able to use this mechanism $m_i \in M$ to implement the elementary threat, this mechanism m_i must be based on at least one exploited vulnerability $v_i \in V$. At the same time, the increase of vulnerabilities v_i, upon which the mechanism m_i depends, have to increase the probability that intruders will use the m_i mechanism when implementing an elementary threat.

Comment 2. Adding elements to all the sets V, M, A for the remaining elementary threats t_1, t_3 and t_4, and having done an additional analysis of the received model, the content of the set R requires clarification, since one cannot rule out the possibility of additional connections that will be modeled on the basis of the data added to the model.

Let us consider another example of mapping the set R into a matrix form, without reference to the previously considered problem, and make an appropriate graph (Fig. 3, Fig. 4).

	t_1	t_2	t_3	t_4
t_1	-	1	0	0
t_2	0	-	1	1
t_3	0	0	-	1
t_4	1	0	0	-

Fig. 3. Mapping an example of the set R into a matrix

The connection $r_{2,3}$ and $r_{2,4}$ (Fig. 4) means, that the threat t_2 can be implemented in the way, that the threat implementation t_3 will no longer be necessary before implementation t_4, since required vulnerabilities (V_{t_4}) for t_4 will already exist as a result of the threat t_2 (A_{t_2}). However, such reasoning is true only if t_4 is accepted as the target of a complex attack.

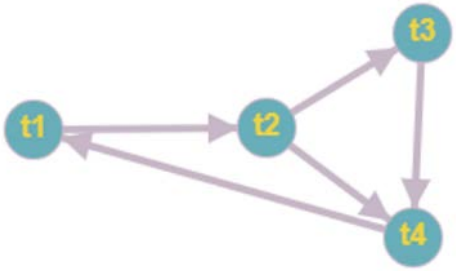

Fig. 4. Mapping an example of the set R as a graph

In the problem discussed above, the elementary threat t_1 was accepted as 'initial', i.e. implemented the first (in terms of the linear time flow). The connection $r_{4,1}$ means that there is a transition to the threat t_1 from t_4, i.e. literally 'threat implementation t_4 will make consequences A_{t_4}, which can be used in the threat t_1 as vulnerabilities V_{t_1}'.

Obviously, the connection may exist in the model, but it does not make practical sense at first glance, if t_1 is considered as 'initial' threat, to which there is no need to return.

In addition, with such a set of connections in R it becomes unclear which elementary threat among t_1-t_4 is an aim for the intruder, i.e. that one of them will allow him to achieve the goal of a complex attack.

Returning to the considered example of complex threat, the whole process of its formation and implementation was known, therefore it became possible to make a model and track the relation between threats. The tasks such as complex threat detection, the determination of its purpose and the order of elementary threats implementation as a part of it, did not require a solution – this information was contained in the initial data. However, as follows from all of the above, it is these tasks that are the main ones and the most difficult to solve.

V. COMPLEX THREATS DETECTION

In reality, for complex and hybrid threats protection, we can point out two the most important tasks:

1. Detection of a complex threat presence.
2. Determining the goal of a complex threat.

Ideally, the human thinking can assume the presence of a complex threat only after the implementation of at least two elementary attacks.

In the given example, if the security expert knows only the fact of the attack, implementing the threat t_1, it is quite complicated for him to make a conclusion about the presence of a complex threat based on such information.

If the expert knows about the threat implementation t_2 – he may already have certain assumptions and conjectures about the existence of a connection between t_1 and t_2, i.e. about the existence of $r_{1,2}$. We can make the following conclusions:

1. The task of detecting the presence of a complex threat can be kept to define the set of links R, if the content of the set

of elementary threats T is known (moreover, the full description of this set is required).

2. Attempts to detect complex and hybrid threats by humans will be "late" for at least two elementary attacks t, as this number allows to conclude that there is at least one link r. If a complex threat consists of three planned attacks – the 'human' detection system is almost useless.

Let us consider the question of determining the goal of a complex threat. Despite the fact that the complex threat includes many elementary threats T, which can cause some damage on their own, the real (main) purpose of a complex threat, in general, is only one – it is a deep systemic vulnerability in the protected system.

The main purpose of a well-planned and implemented complex threat is not obvious to the security service until the intruder reaches the target, in some cases – after, because the consequences of a complex threat implementation and the achievement of the main goal can be hidden and stretched over time.

The example considered above (Fig. 4) is a visual representation of the purpose of a complex threat uncertainty. The Elementary threats t_1-t_4 are occurred through vulnerabilities, which are the consequences of other threat. Neither goals of the complex threat nor the order of its implementation is obvious.

Fig. 5 presents a situational pattern, wherein the expert is aware of seven potential elementary threats and the existence of the connection of $r_{1,2}$:

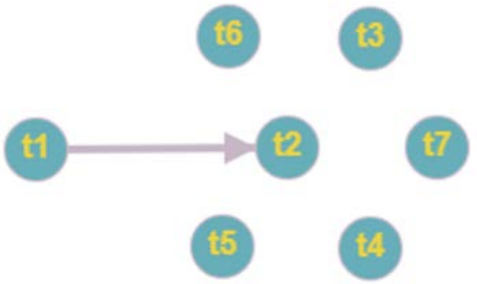

Fig. 5. An example of a lack of knowledge about a partially implemented complex threat

The task of predicting the next threat implementation, in this case, seems to be quite difficult for human thinking even for seven threats. In reality, the number of potential threats that can be implemented next, can be measured in hundreds.

VI. METHOD INTELLIGENT DETECTION METHOD OF COMPLEX THREATS

We introduce three main terms.

1. *Potential elementary threats* T_p – the set of all elementary threats existing within the considered protected system. In this case, the elements of the set T_p also satisfy (2), and the record (1) can be supplemented in the following way (12):

$$C = <T, R>;$$
$$|T| > 1; \quad (12)$$
$$|R| > 1;$$
$$T \subseteq T_p.$$

That is, for any complex threat C, the set of elementary threats T will always be formed from the elements of the set of potential elementary threats T_p.

2. *Current complex threat model* – an updated model in the form of C = <T, R>, created on the basis of information available at a discrete instant of time about the implemented complex threat C.

3. *Proposed complex threat model* – immutable model C = <T, R>, formed by an intelligent algorithm based on its operational internal rules and knowledge about possible complex threats models.

In fact, having extensive information about the components of the set of potential elementary threats T_p, to synthesize the rules of detection of a specific complex threat C you will have to create a set of assumed integrated threat models C, and then – compare the assumed models with the current model to identify the most reliable ones.

To detect complex threat C, let N putative models of complex threats <Ti, Ri> (i = 1..N) be synthesized, with each such model satisfying the rules (12) and (2). We introduce the set <Tc, Rc> to denote the current complex threat model C, which also satisfies (12) and (2).

As the complex threat C is implemented, its current model $<T_c, R_c>$ will be supplemented not only with new connections r, but also with the elements of the set T_c. Having calculated the evaluation function (13), where d (p, q) - is a certain measure of similarity, we obtain the closest to the current model $<T_c, R_c>$ the estimated model $<T_i, R_i>$, which can be considered the most likely case scenario at discrete time:

$$\min(d_{i=1}^{N}(< T_i, R_i >, < T_c, R_c >)). \quad (13)$$

Thus, it is proposed to reduce the complex threat detection to finding the most "similar" model among the set of pairs of proposed models $<T_i, R_i>$, which will be made by a special intelligent algorithm.

VII. CONCLUSION

The proposed rules for the complex threats formalization into a basic model can be used as a basis for further research in the direction of the theory of complex security and hybrid threats protection, neurographic theory of complex security [9].

The example of constructing a basic model, given in the work, shows its applicability. The basic model can be supplemented with various aspects that will improve the accuracy of the created models.

In addition, some aspects identified in the paper remain open for further research, for example, the nature of the links between elementary threats.

The second most important result of the work is the conclusion of a formalized task of complex threats detection

(13). The issue, in fact, directly leads to artificial intelligence algorithms usage and big data processing in the construction of integrated security systems, as there are three big tasks:

1. Potential modeling of complex threats. The problem can be solved by creating an artificial intelligence system that has decent knowledge about complex threats modeling, the structure of internal relationships, the features of the complex threats implementation, etc.

Such knowledge can only be obtained by processing large amounts of data, collected during the operation of security monitoring systems. In general, there arises a range of tasks typical for Big Data technologies, which are already widely used in many fields, including the fields of data security and cyber security systems [1, 9, 11, 13, 15, 16, 18].

2. Creation of rules for determining the most similar anticipated and current models of complex threats. The solution of this problem includes a wide range of possibilities for applying data mining algorithms (Data Mining).

Among the Data Mining algorithms used in relation to this problem can be noted clustering, classification and affinity analysis. It is possible to use regression analysis and genetic algorithms. Data Mining technologies are also widely used in many areas of activity, successfully solving assigned tasks, including the field of security [2, 3, 7, 9, 12, 17].

3. Tracking and current integrated threat modeling. According to the authors, this task can be solved by creating certain analysis and information system, which can be based on existing corporate information systems and security tools within specific enterprises. Integration and data flow monitoring [14], emphasis on critical deviations, events recording and relation determination by methods of intellectual analytics are the main assets, the totality of which will solve this problem.

The paper describes the basic principles of complex threats modeling, and the task of complex threats detection is formalized. The proposed modeling principles are based on the idea of identifying the links between elementary threats as part of a complex one. As an example, the process of constructing a complex threat model based on the proposed modeling rules is given. Based on the examples presented in the work, the paper includes the description of tasks while working with complex threats: the tasks of complex threats detection, the identification of their inner structure and purposes of the implementation. Based on the formulated principles of basic modeling, the paper also gives a formal statement of complex threats detection problem, which explains the possibility for applying data mining algorithms and big data processing technologies in the construction of protection systems against complex threats and developing the neurographic theory of complex security [9].

REFERENCES

[1] Anavangot, Vijay, Varun G. Menon, and Anand Nayyar. "Distributed Big Data Analytics in the Internet of Signals." 2018 International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE, 2018.

[2] Barceló-Rico, F., Esparcia-Alcázar, A. I., & Villalón-Huerta, A. (2016). Semi-supervised classification system for the detection of advanced persistent threats. In Recent Advances in Computational Intelligence in Defense and Security (pp. 225-248). Springer, Cham.

[3] Chan, K. Y., Kwong, C. K., Wongthongtham, P., Jiang, H., Fung, C. K., Abu-Salih, B., ... & Jain, P. (2018). Affective design using machine learning: a survey and its prospect of conjoining big data. International Journal of Computer Integrated Manufacturing, 1-19.

[4] Davis Jr, J. R. (2015). Continued evolution of hybrid threats. The Three Sword Magazine, 19(28).

[5] Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 301-306). IEEE.

[6] Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 295-300). IEEE.

[7] He, Z., Situ, H., Zhou, Y., Wang, J., Zhang, F., & Qiu, M. (2018, May). A Fast Security Evaluation of Support Vector Machine Against Evasion Attack. In 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 258-263). IEEE.

[8] Hunter, E., & Pernik, P. (2015). The challenges of hybrid warfare. International Centre for Defence and Security.

[9] Korneev, N. V. (2019, January). A Neurograph as a Model to Support Control Over the Comprehensive Objects Safety for BIM Technologies. In IOP Conference Series: Earth and Environmental Science (Vol. 224, No. 1, p. 012021). IOP Publishing.

[10] Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. European security, 27(3), 374-392.

[11] Mishra, A. D., & Singh, Y. B. (2016, April). Big data analytics for security and privacy challenges. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 50-53). IEEE.

[12] Mohammed, B., Awan, I., Ugail, H., & Younas, M. (2019). Failure prediction using machine learning in a virtualised HPC system and application. Cluster Computing, 22(2), 471-485.

[13] More, Rohit, et al. "Real time threat detection system in cloud using big data analytics." 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, 2017.

[14] Offia, C. E., & Crowe, M. (2019). A theoretical exploration of data management and integration in organisation sectors. International Journal of Database Management Systems, 11(1), 37-56.

[15] Petrenko, S. A., & Makoveichuk, K. A. (2017). Big data technologies for cybersecurity. In CEUR Workshop (pp. 107-111).

[16] Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. IEEE Transactions on Services Computing.

[17] Singh, J. (2014, March). Real time BIG data analytic: Security concern and challenges with Machine Learning algorithm. In 2014 Conference on IT in Business, Industry and Government (CSIBIG) (pp. 1-4). IEEE.

[18] Srivastava, Neha, and Umesh Chandra Jaiswal. "Big Data Analytics Technique in Cyber Security: A Review." 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2019.

[19] Stepanova, T., Pechenkin, A., Lavrova, D. Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems (2015) ACM International Conference Proceeding Series, 08-10-Sep-2015, DOI: 10.1145/2799979.2799995.

[20] Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.