UDC 004.853:007.2
https://doi.org/10.31891/csit-2023-1-3

Sergii BOZHATKIN, Viktoriia GUSEVA-BOZHATKINA,
Tetyana FARIONOVA, Volodymyr BURENKO, Bohdan PASIUK
Admiral Makarov National University of Shipbuilding

EMERGENCY NOTIFICATION COMPUTER SYSTEM VIA TELECOMUNICATION EQUIPMENT OF THE ORGANIZATION'S LOCAL NETWORK

In the event of an emergency, there are still actions that people must take to save themselves. Currently, everyone has a mobile phone. Almost all establishments have an open Wi-Fi network. A model of the system that, when connected to the network, informs about the threats that have arisen and the actions that citizens must take to avoid damage. The alert system works around the clock. It complements the existing fire alarm and security systems. In the course of the work, an analysis of the existing models of cybersecurity threats for warning systems in emergencies was carried out, which showed that the requirements for the civil protection warning system currently need to be modernized. Therefore, the purpose of the work is to design and develop an extended cybersecurity threat model. The key aspects of the cybersecurity threat model are identified. A model of an intruder of such a warning system is presented. An extended cybersecurity threat model has been built using the Cyber Kill Chain.

At this stage of the study, data were obtained that allow us to conclude about the use of the Cyber Kill Chain model. When applied to a typical threat model, the result gives a broader view of the threats to the information system (including actors, typical hacker software, devices that may eventually become hacker tools when the system is hacked).

The use of modeling to study each of the structural components of the warning system is determined to be appropriate. This is justified by the fact that it is impractical to conduct a real experiment, especially with the reproduction of cyber incidents, due to significant financial and labor costs. This approach is also effective when it is necessary to conduct an analysis of the designed system, which does not yet physically exist in this organization.

Keywords: emergency, notification computer system, public wireless access point, alert nodes, organization's local network, cybersecurity, model of cybersecurity threats, Cyber Kill Chain

Сергій БОЖАТКІН, Вікторія ГУСЄВА-БОЖАТКІНА,
Тетяна ФАРІОНОВА, Володимир БУРЕНКО, Богдан ПАСЮК
Національний університет кораблебудування імені адмірала Макарова

КОМП'ЮТЕРНА СИСТЕМА ОПОВІЩЕННЯ ПРО НАДЗВИЧАЙНІ СИТУАЦІЇ ЗА ДОПОМОГОЮ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

У разі надзвичайної ситуації необхідно вжити всіх необхідних заходів, щоб врятувати людей. Майже всі заклади мають відкриту мережу Wi-Fi для співробітників. На теперішній час у кожного з них є мобільний телефон. На основі телекомунікаційного обладнання корпоративної мережі та смартфонів у якості хостів такої мережі можливо побудувати систему оповіщення, яка працює цілодобово. Така системі також може бути доповнена існуючими системами пожежної сигналізації та охорони.

Моделювання системи оповіщення полегшує вивчення поведінки об'єктів з метою покращення функціональності та зменшення вартості такої системи під час її створення, подальшого перетворення і розвитку. До того ж, в такій моделі системи має бути враховано не тільки інформування про загрози, але й дії, які громадяни мають виконати, щоб уникнути небезпеки та мінімізувати збитки на виробництві. У ході роботи також проведено аналіз існуючих моделей загроз кібербезпеці для систем оповіщення про надзвичайні ситуації.

Комплексний підхід до моделювання всіх зазначених складових комп'ютерної системи оповіщення про надзвичайні ситуації за допомогою телекомунікаційного обладнання локальної мережі організації (ЛОМ) показав, що вимоги до системи оповіщення цивільного захисту наразі потребують модернізації. Тому у роботі розглянуті питання проєктування такої системи. Також розроблено розширену модель загроз кібербезпеці системі оповіщення через обладнання ЛОМ. Визначено ключові аспекти моделі загроз кібербезпеці. Представлено модель порушника такої системи оповіщення. Розширену модель загроз кібербезпеці було створено за допомогою Cyber Kill Chain.

Використання моделювання для дослідження кожної зі структурних складових системи оповіщення визначається як доцільне, тому що реальний експеримент, особливо з відтворенням кіберінцидентів, проводити недоцільно через значні фінансові і трудові витрат, а також при необхідності проведення аналізу проектованої системи, яка ще фізично не існує в даній організації.

Ключові слова: надзвичайна ситуація, комп'ютерна система сповіщень, публічна бездротова точка доступу, вузли сповіщень, локальна мережа організації, кібербезпека, модель загроз кібербезпеці, Cyber Kill Chain

Introduction

One of the main ways of protecting the population from emergencies is a timely notification of the danger in the situation that has arisen as a result of its development, as well as informing about the procedure and rules of behavior in the context of the emergency.

Today there is a revision of the requirements regarding modern alert systems (AS), which were created for civil protection tasks using automated systems of centralized notification, communication networks, radio broadcasting. There is a transition to new structures of organization of such systems, taking into account the current

state of technical means of communication, protection against unauthorized access, and distribution of malicious software.

Emergency alert systems serve as a critical link in the chain of crisis communication, and they are essential to minimize loss during emergencies. Acts of terrorism and violence, chemical spills, amber alerts, nuclear facility problems, weather-related emergencies, flu pandemics, and other emergencies all require those responsible such as government officials, building managers, and university administrators to be able to quickly and reliably distribute emergency information to the public [1, 2].

Loudspeaker in such places attracts attention and may provide the necessary information for further action but at the same time the presence on the screen of a smartphone, tablet, laptop clear scheme using microservices, evacuation plan and instructions for actions of the population especially with hearing impairments, which will minimize the time to make decisions about an emergency response or mitigation measures [3].

Therefore, the danger must be notified first via calls, howls, sirens, etc. But currently, everyone has a mobile phone, and almost all establishments have a Wi-Fi network. Consequently, a system that, when connected to the network, informs about the threats that have arisen and the actions that citizens must take to avoid damage, is necessary important at this time.

Modern AS and information support are created to solve the assigned tasks based on automated centralized warning systems, communication networks, and broadcasting [4]. Also, when building notification systems, it is necessary to take into account the security of access points (AP) and system servers from hacking by intruders, preventing DDoS attacks, etc. [5].

The security system of information systems (such like AS) is not built by itself. It is based on threat models and intruder models. The threat model itself is a document that lists and describes possible threats to the information security of the organization/enterprise, the probability of implementation, and the consequences of their action.

The idea of creating a public alert system via Wi-Fi is quite new and interesting for research and implementation. Since we are talking about APs of wireless connection, there is a threat of various kinds of attacks. To determine the cybersecurity of such a system, it is proposed to develop an extended threat model based on the Cyber Kill Chain model and to study the difference with a typical threat model [6, 7].

Research interests – cybersecurity, models of hacker attacks.

The aim of the present study is to increase the accuracy of the threat model on the example of the development of a wireless alert system by developing an extended threat model through detail using the Cyber Kill Chain model.

Objectives of the study.

- Identify typical models on which typical final threat models and violator models are based
- Analyze the type of connection between digital network points
- Identify typical attack methods for this type of connection
- Develop assessment criteria in an extended threat model based on Cyber Kill Chain items
- Develop and present the results of the study of the alarm system via wireless communication

The relevance of the study is based on the fact that the rapid acceleration of the development of computer technology entails more complex and diverse attacks, which are difficult to describe with existing typical models of threats. Therefore, there is a need to develop a more accurate and detailed model with expert assessments for each stage of the security system being tested for hacking.

The object of the study Methods of extending a typical threat model using the Cyber Kill Chain model.

The subject of the study is the properties of the information system cybersecurity violator model after the implementation of key points of the Cyber Kill Chain model.

The relevance of the study is to find new, more detailed, more effective models for building a threat model of information systems. At present, not every business or government organization in Ukraine is thinking about the problems of creating a model of threats to their information systems. Often it is due to the negligence or ignorance of the system administrator that vulnerabilities remain in the systems, which an attacker can exploit at his own discretion without any problems. His actions can result in the complete destruction of information, as well as its theft or sale on the black market.

In this regard, it should be noted that the most effective description tools are the model of intruder and the model of threats to the information system, which simultaneously provides a representation of two key issues: identifying the system actor that can harm the information system and attack vectors.

Existing standard approaches and models are quite general and do not describe at what stage the actor (employee or attacker) can perform intentional or unintentional actions that may harm the information system. This research is based on the development of a wireless warning system for students of the Admiral Makarov National University of Shipbuilding.

Problem statement

The threat itself is a security flaw or omission that can be exploited by attackers. The presence of a threat does not mean the inevitable possible leakage of information: this suggests that attackers have a theoretical possibility of unauthorized access to the personal data of the enterprise.

Like any normative document, the threat model is built on a certain model: the title page, a list of terms, definitions, and abbreviations, content, main part, and appendices [8].

To create a model, it is necessary to analyze the data obtained during the audit of the information system (IS). This will help identify system weaknesses; understand what will threaten it; where the threat may come from and by what means it will be possible to neutralize it or prevent its detection in advance [9].

Sources of threats – a section that also needs to be reflected in the model. These can be external or internal intruders, viruses, or software and hardware bookmarks.

When compiling a threat model, the level of initial security is determined. This is a global parameter that is determined once and does not change depending on the threat. Then the actual threats are highlighted and unnecessary ones are excluded – those that do not harm the system. Threats that have not been ruled out are included in the model with a description.

Threat modeling is still in some ways an art as much as a science, and there is no single canonical threat modeling process. The practice of threat modeling draws from various earlier security practices, most notably the idea of "attack trees" that were developed in the 1990s. In 1999, Microsoft employees Loren Kohnfelder and Praerit Garg circulated a document within the company called "The Threats to Our Products" which is considered by many to be the first definitive description of threat modeling [10].

In [11, 12] present threat models in the form of a list of possible IP vulnerabilities (such as DoS, DDoS, sniffing, packet header substitution, etc.), but objects like an alarm system are subject to much more thorough inspection and the developed model should be to some extent more detailed.

The need for a Wi-Fi network is that the marketing policy of the center provides visitors and employees of the center and shops the opportunity to access the Internet. There are many times when you need to access the Internet not only from your computer or laptop, but also from portable devices that allow you to optimize your workflow at the expense of modern network infrastructures – video conferencing, IP telephony, e-mail, server management, and network devices.

The high level of security of Wi-Fi indicates its advantages when used in public places where information security is one of the main criteria of the network. To protect against unauthorized access to the alert node and save the database of connected subscribers the RADIUS Protocol is the most common AAA (Authentication, Authorization, and Accounting) protocol now developed to transmit information between application programs (Fig. 1).

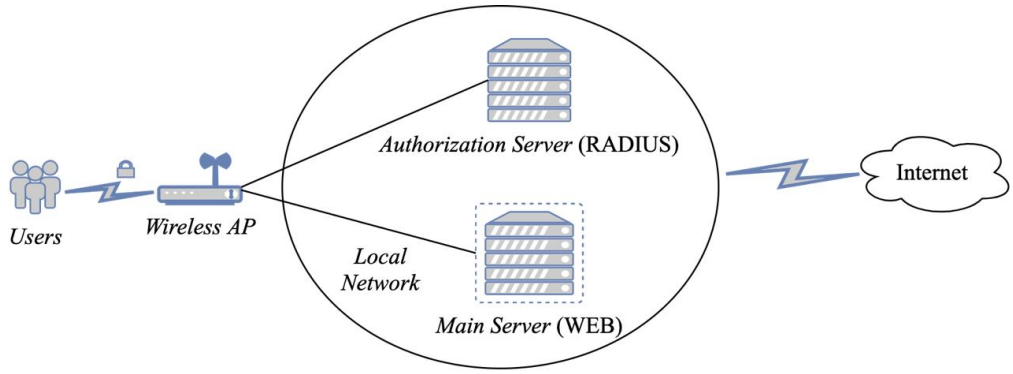

Fig. 1. Alert node scheme

It should be noted that this model can be applied to employees of the *Local Network* of the enterprise, who are granted access to the Wi-Fi network with a RADIUS server (*Authorization Server*) and a notification server (*Main Server*). This means, that the connection between *Wireless AP* and *Users* (employees) has an encrypted connection [13].

To describe a problem, we need to understand what is typical cybersecurity threats exist for such systems. There are many specific types of attacks on Wi-Fi networks [14]:

- Hacking WPA/WPA2 passwords (handshake catching);
- WEP attack;
- Hacking WPS Pin;
- WPA downgrade;
- Replacing a true AP with a fake (for catching login and password to connect to the AP and compromised it);
- Attack on Wi-Fi access points from the global and local networks;
- Denial of Service Attacks (Wi-Fi DoS);
- Attacks on specific services and functions of routers;
- Keyloggers on mobile devices;
- Hijacking;

– Social Engineering.

First, let's define the model of information security violator. For this purpose, the typical model shown in Fig. 2 will approach.

This typical model of cybersecurity violator of the notification system in the enterprise reflects only general information and carries almost no semantic load for a cybersecurity specialist or system administrator. In this case, the next step is to build a threat model for the notification system by using the so-called "CIA Triad": Confidentiality, Integrity, and Availability [15]. Details of the implementation of this approach in different types of activities have shown in Fig. 3.

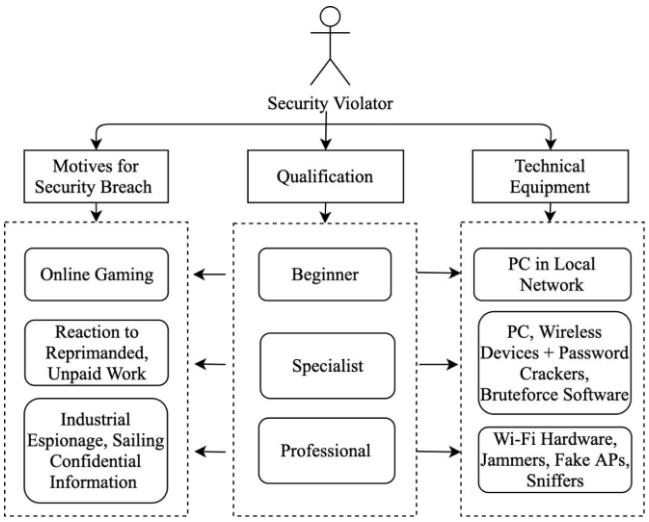

Fig. 2. Typical model of information security violator

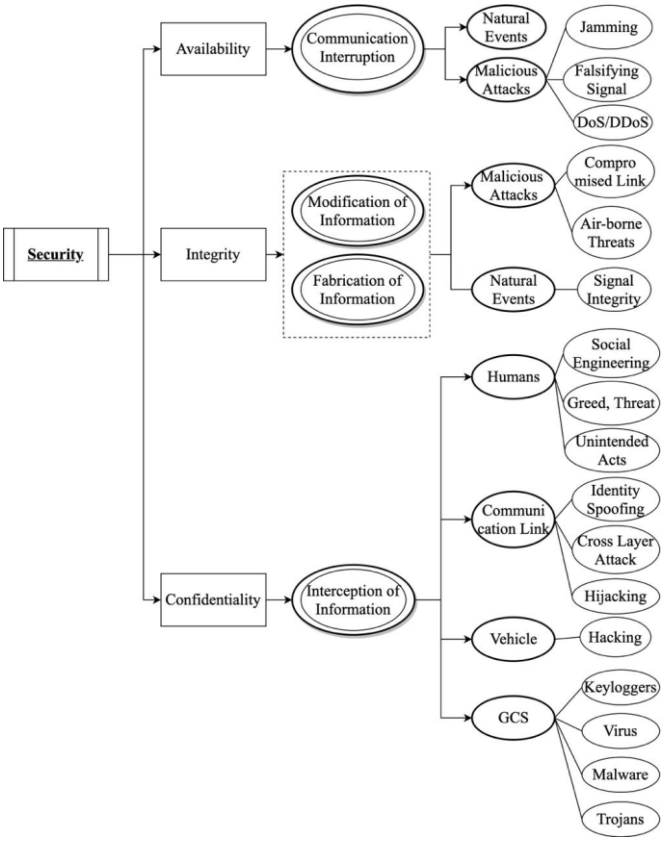

Fig. 3. Typical threat model

The problem is that these models are guided by the reflection of general recommendations that should be considered, but in no way indicate the real possible violators and at what stage they may begin to exploit system vulnerabilities.

Given the above, it is necessary to conduct research and build a threat model that more accurately transmits information about possible vulnerabilities of information systems on the example of a notification system via wireless communication.

Experiment

Threat modeling is a structured process through which IT pros can identify potential security threats and vulnerabilities, quantify the seriousness of each, and prioritize techniques to mitigate the attack and protect IT resources.

This broad definition may just sound like the job description of a cybersecurity professional, but the important thing about a threat model is that it is systematic and structured. Threat modelers walk through a series of concrete steps to fully understand the environment they're trying to secure and identify vulnerabilities and potential attackers.

Within cybersecurity, we see many terms used within military operations, including demilitarized zones (DMZs), defense-in-depth, and APT (Advanced Persistent Threat). Another widely used term is the kill chain where military operations would attack a specific target, and then look to destroy it. A defender will then look to break the kill chain and understand how it might be attacked. An example of the kill chain approach is "F2T2EA", where we Find (a target), Fix (on the location of the target), Track (the movement of the target), Engage (to fix the weapon onto the target), Assess (the damage to the target). A core of this approach is the provision of intelligence around the finding, tracking, and assessment of the target.

One of the most used cybersecurity models to understand threats is the kill chain model and was proposed by Lockheed Martin. Yadav and co-authors determine that the technical nature of the key stages of an attack, include Reconnaissance, Weaponize, Delivery, Exploitation, Installation, Command & Control, and Act on Objective (Fig. 4).

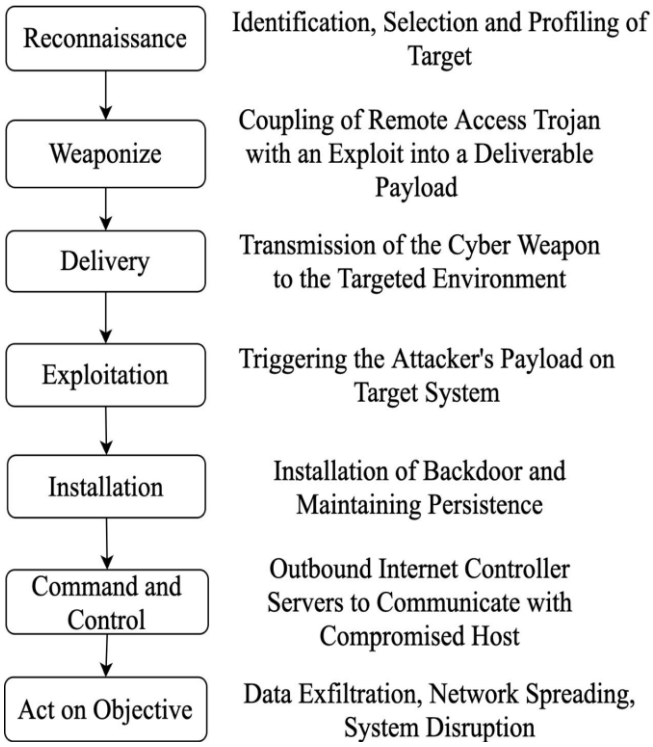

Fig. 4. Simple Cyber Kill Chain model

Each stage is related to a certain type of activity in a cyberattack, regardless of whether it's an internal or external attack.

1) Reconnaissance

The observation stage: attackers typically assess the situation from the outside-in, to identify both targets and tactics for the attack

2) Intrusion

Based on what the attackers discovered in the reconnaissance phase, they're able to get into your systems: often leveraging malware or security vulnerabilities

3) Exploitation

The act of exploiting vulnerabilities, and delivering malicious code onto the system, to get a better foothold

4) Privilege Escalation

Attackers often need more privileges on a system to get access to more data and permissions: for this, they need to escalate their privileges often to an administrator:

1) Lateral Movement.

Once a hacker enters the system, he can move laterally to other systems and accounts to gain more leverage: whether that's higher permissions, more data, or greater access to systems;

2) Obfuscation/Anti-forensics.

To successfully pull off a cyberattack, attackers need to cover their tracks, and in this stage, they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team;

3) Denial of Service.

Disruption of normal access for users and systems, to stop the attack from being monitored, tracked, or blocked;

4) Exfiltration.

The extraction stage: getting data out of the compromised system.

The term "Kill Chain" was originally used as a military concept related to the structure of the attack. The idea is to effectively prevent or counteract the opponent in the various phases of the attack lifecycle.

To attribute cyber threats effectively, it is necessary to identify them based on their attack patterns in different phases of the kill chain. These are tactics, techniques, procedures, and the tools used (software). Tactics are the goals or states that an attacker tries to achieve to complete their mission. A technique is how a specific behavior or activity achieves that goal or state. A tactic can have many techniques and a technique can have many tactics. Procedures and software identify the tools or steps used to complete a series of actions conducted in a certain order or manner. To achieve one of these steps an APT can use many tactics. In turn, these tactics are accomplished by using one or many techniques and/or software tools.

Taking into account the above, we will define the criteria according to which the model of cybersecurity threats of the alarm system via wireless communication will be built based on the following interrelated points.

- stage of the model "Cyber Kill Chain";
- description of threat at this stage;
- typical tools of the attacker at this stage;
- entry points of the attacker at this stage (possible security gaps);
- danger actor (person or department with whose hands you can enter the information system) at this stage;
- the mechanism for implementing malicious actions at this stage;
- the level of danger of the attacker at this stage (scale 1–5, where 1 – the threat of breakage does not entail any consequences; 5 – possible complete failure of the system);
- the current level of implementation of preventive actions at the stage of the model "Cyber Kill Chain".

Given the defined criteria for building an extended model of cyber threats to the notification system via wireless communication, the results are presented in Table 1.

Table 1

Enhanced cybersecurity threat model

Stage	Description of threat	Typical tools	Entry points	Threat actors	Implementing mechanism or device	Level of danger (1–5)	Current level of preventive actions
Reconnaissance	Target investigation	nmap, vuln search, aircrack-ng phishing; sqlmap	SSID is visible, known employee's e-mail; Captive Portal website	Cracker (hacker)	–	2	1**
Weaponize	Making a payload or phishing link, basics on the investigation of a target	Msfvenom, custom payload; compromised e-mail account	Weak Wi-Fi encryption mechanism; handshake capture; admin's mail service; Captive Portal website	Cracker	Wi-Fi access point; e-mail service without antispam; weak SQL database	3	3**
Delivery	Launch exploit	Meta-sploit framework, msfvenom, bash shell	Outside IP address for Internet access; Captive Portal website	Cracker	Server, smartphone or laptop	4	3**
Exploitation	System infection	Malware, malicious connect	Mobile devices with Bluetooth vulnerabilities open ports on AP*	Cracker, administrator	Server (Radius, main)	4	2**

Stage	Description of threat	Typical tools	Entry points	Threat actors	Implementing mechanism or device	Level of danger (1–5)	Current level of preventive actions
Installation	Starting payload's session	Meterpreter, bash shell, malware attack	Vulnerable service, AP, or server	Cracker, administrator	Server or laptop, mobile device	4	3**
Command and control	Using payload's session to take control of the overall system	Meterpreter, bash shell	Payload on a server or vulnerable service exploit	Cracker	Compromised devices in a system	5	4**
Act and objective	Data compromising system disruption	Meterpreter, bash shell, ransom-ware attack	Payload on a server or vulnerable service exploit	Cracker	Compromised devices in a system	5	5**

*Open ports, which are using for Radius server services or main server access
**Average assessment of experts (research will be conducted in the next scientific article)

In cases of the extreme complexity of the problem, its novelty, insufficient information available, the impossibility of mathematical formalization of the solution process, one has to turn to the recommendations of competent specialists who know the problem perfectly – to experts. Their solution to the problem, argumentation, formation of quantitative assessments, processing of the latter by formal methods are called the method of expert assessments.

Expert assessment involves the creation of a collective opinion that has greater capabilities compared to the capabilities of an individual. The source of collective opinion is the search for weak associations and assumptions based on the experience of an individual specialist. The expert approach has great potential for solving problems that cannot be solved in the usual analytical way.

Let's provide expert estimates for each point of the model presented above about the current level of preventive actions (Table 2).

Table 2

The current level of implementation of preventive actions at the stage of the model "Enhanced cybersecurity threat model"

Stage	Expert 1	Expert 2	Expert 3	Average score
Reconnaissance	1	2	1	1
Weaponize	2	3	3	3
Delivery	3	3	3	3
Exploitation	3	2	2	2
Installation	4	3	3	3
Command and control	4	4	4	4
Act and objective	5	5	5	5

Conclusion

At this stage of the study, data were obtained that allow us to conclude about the use of the Cyber Kill Chain model. When applied to a typical threat model, the result gives a broader view of the threats to the information system (including actors, typical hacker software, devices that may eventually become hacker tools when the system is hacked).

It was also proposed to introduce expert assessments to determine the degree of security of the information system at a certain stage of the developed model, which will be studied in more detail and the results will be provided in future research papers.

Further research should be aimed at improving the extended threat model of information systems. In the first stage, the integration of this model should be carried out on a small segment of the network to collect data on the security of the information system and identify possible gaps in its security.

Further analysis and improvement of such a model will show how effective the information system will be in terms of cybersecurity and will help to immediately understand and correct deficiencies. Network security issues deserve special attention, especially in the case of the integration of next-generation networks in such important areas of infrastructure as, for example, wireless alert systems, electricity, or energy delivery system.

Also, new standards for the organization of computer networks can be applied in other areas of telecommunications. As a result, the developed model can be used in cybersecurity audits or cybersecurity departments to the in-depth study of the information system and improve its resilience to hacker attacks.

The use of modeling to study each of the structural components of the warning system is determined to be appropriate. This is justified by the fact that it is impractical to conduct a real experiment, especially with the reproduction of cyber incidents, due to significant financial and labor costs. This approach is also effective when it is necessary to conduct an analysis of the designed system, which does not yet physically exist in this organization.

References

1. Kang B., Choo H. A deep-learning-based emergency alert system. *ICT Express*. 2016. Vol.2, Is. 2. Pp. 67–70. doi: 10.1016/j.icte.2016.05.001.
2. Hidayanti, Supangkat S. H. Designing a distribution emergency information service in earthquake post-disaster based on service computing system engineering. *In: Proceedings of the International Conference on ICT for Smart Society (ICISS).* Semarang, Indonesia. 2018. Pp. 1–6. doi: 10.1109/ICTSS.2018.8549969.
3. Berkunskyi Y., Knyrik K., Farionova T., Smykodub T. Using microservices in educational applications of IT-company. *In: Proceedings of the IEEE 1st Ukraine Conference on Electrical and Computer Engineering (UKRCON 2017).* Kyiv, Ukraine. 2017. Pp. 1208–1211. Article number 8100443. doi: 10.1109/UKRCON.2017.8100443.
4. Mishra S., Golias M. M., Thapa D. Work zone alert systems. *Technical Report RES2019-01*. Memphis, Tennessee : The University of Memphis,2021.
5. Kurtz J. A. Hacking wireless access points: Governmental context. *In book: Cracking, Tracking, and Signal Jacking*. Chapter 7. Elsevier, Burlington, MA : Syngress Publ. 2017. Pp. 93–107. doi: 10.1016/B978-0-12-805315-7.00007-3.
6. Garba F. A. The anatomy of a cyber attack: Dissecting the Cyber Kill Chain. *Scientific and Practical Cyber Security Journal (SPCSJ)*. 2019. Vol. 3, Is. 1. Pp. 29–44.
7. Tatam M., Shanmugam B., Azam S., Kannoorpatti K. A review of threat modelling approaches for APT-style attacks. *Heliyon.* 2021. Vol. 7, Is. 1. Article number e05969. doi: 10.1016/j.heliyon.2021.e05969.
8. Knight A. Threat modeling. *In book: Hacking Connected Cars: Tactics, Techniques, and Procedures*. Chapter 3. Hoboken, NJ : Wiley, 2020. doi: 10.1002/9781119491774.ch3.
9. Fruhlinger J. Threat modeling explained: A process for anticipating cyber attacks. Publ. 2020, April 15. URL: https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.
10. Shostack A. 20 years of STRIDE: Looking back, looking forward. Publ. 2019, March 29. URL: https://www.darkreading.com/risk/20-years-of-stride-looking-back-looking-forward.
11. Zhang W. A distributed security situation evaluation model for global network. *CEUR Proceeding*. 2018. Vol. 2300. Pp. 245–248.
12. Burlachenko I., Zhuravska I., Davydenko Ye., Savinov V. Vulnerabilities analysis and defense based on MAS method in fast dynamic wireless networks. *In: Proceeding of the 4th IEEE International Symposium Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IEEE IDAACS-SWS* 2018). Lviv, Ukraine. 2018. Pp. 98–102. doi: 10.1109/IDAACS-SWS.2018.8525692.
13. Merc L., Sobeslav V., Mikulecky P., Macinka M. Infrastructure Authentication, Authorization and Accounting solutions for an OpenStack platform. *In book: Mobile Web and Intelligent Information Systems. Lecture Notes in Computer Science.* Vol. 11673. London : Springer-Verlag, 2019. Pp. 123–135. doi: 10.1007/978-3-030-27192-3_10.
14. Types of wireless attacks. Publ. 2017, Jun 13. URL: https://blog.ct-networks.io/types-of-wireless-attacks-9b6ecc3317b9.
15. Prinetto P., Roascio G. Hardware security, vulnerabilities, and attacks: A comprehensive taxonomy. *CEUR Proceeding.* 2020. Vol. 2597. Pp. 12–23.

Sergii Bozhatkin **Сергій Божаткін**	Senior Lecturer of the Department of Computer Technologies and Information Security, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine, e-mail: sergii.bozhatkin@nuos.edu.ua https://orcid.org/0000-0002-4653-8880	старший викладач кафедри комп'ютерних технологій та інформаційної безпеки, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна
Viktoriia Guseva-Bozhatkina **Вікторія Гусєва-Божаткіна**	Senior Lecturer of Department of Automated Systems Software, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine, e-mail: GusevaBozh@meta.ua https://orcid.org/0000-0002-1117-3391	старший викладач кафедри програмного забезпечення автоматизованих систем, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна
Tetyana Farionova **Тетяна Фаріонова**	PhD on Engineering, Associate Professor, Director of the Educational and Scientific Institute of Computer Sciences and Project Management, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine, e-mail: tetyana.farionova@nuos.edu.ua https://orcid.org/0000-0003-3384-4712	канд. техн. наук, доцент, директор Навчально-наукового інституту комп'ютерних наук та управління проектами, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна.
Volodymyr Burenko **Володимир Буренко**	PhD Student of Department of Project Management, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine e-mail: volodymyr.burenko22@gmail.com https://orcid.org/0000-0002-0862-5879	аспірант кафедри управління проектами, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна
Bohdan Pasiuk **Богдан Пасюк**	PhD Student of Department of Automated Systems Software, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine e-mail: bwolverine44@gmail.com https://orcid.org/0000-0002-4634-4090	аспірант кафедри програмного забезпечення автоматизованих систем, Національний університет кораблебудування імені адмірала Макарова, Миколаїв, Україна