Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2022, № 2 (106) https://doi.org/10.33108/visnyk_tntu2022.02
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 65.011.56:004

PROJECT MANAGEMENT FEATURES IN THE CYBERSECURITY AREA

Mariia Stadnyk; Andriy Palamar

Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

Summary. *This paper has presented detailed comparative analysis of the project manager work on IT and cybersecurity projects by each PMI project management process group: initiating, planning, executing, monitoring and controlling, and closing. Based on the results, a list of project management peculiarities in cyber security was obtained, and a list of industry knowledge and requirements for a cyber security manager was presented. Proposals for the application of tools and techniques for each process of the cyber security project were formed in accordance with the features.*

Key words: *cybersecurity, project manager, project management process group, knowledge areas, infosec domain.*

https://doi.org/10.33108/visnyk_tntu2022.02.054 *Received 02.03.2022*

Statement of the problem. Nowadays, independent countries face not only their physical enemy, but also an informational enemy. This is evidenced by cyber-attacks on important state resources, management systems of key enterprises, departments, radio and television broadcasting centers. Accordingly, there is a need for cyber protection of core business assets and comprehensive employees training in the field of cyber security for preventive protection. At the state level a vivid example of the need for protection is the Ukrainian-Russian war in the information space, as a result of which several web resources were temporarily blocked and unavailable. It led to the formation of the IT Army of Ukraine, the main purpose of which is to repel the enemy in cyberspace by launching DDoS attacks on banks, propaganda sites and channels, and communication services. Of course, such a self-organization is formed on the enthusiasm of Ukrainians, but with proper management, it can develop into an official structure for combating cybercrimes.

It is necessary to take care of cyber security not only at the state level. Each enterprise has certain information assets that are necessary for the successful management of business processes. Usually, companies use the services of the third-party contractors in the field of cyber security, who are able to analyze the vulnerabilities of the existing organization and, implement a project related to cyber protection based on the audit results. The success and effectiveness of the project depends on the selected project management methodology, analysis tools and implementation techniques. Accordingly, the study of the project management features in the field of cyber protection and the application of appropriate techniques will avoid typical mistakes, increase efficiency and reduce the time spent on their implementation.

Analysis of the available investigations. The boundaries between IT management and Cybersecurity Management are blurred, so there is usually no clear separation of cybersecurity projects into a separate branch of project management. For the most part, project managers are guided by the PMBOK standard from the Project Management Institute (PMI) [1]. This standard covers all typical projects and contains a detailed explanation of the implementation of the project phases of initiating, planning, executing, monitoring and controlling, and closing.

In the article [2], the authors also investigate the peculiarities of project management specifically in the field of cyber security, namely: the increased level of influence from the state, the complexity of the initiation stage, the critical importance of implementation deadlines, significant differentiation according to the budget, an unlimited number of possible participants, a high level of personalization, complexity in the calculations of efficiency metrics.

The main standard that the manager is guided by is ISO-27001:2013 [3] on the implementation of the information security management system (ISMS). As all sizes organizations collect, process, store and transmit information in some form, ISO-27001:2013 was developed as a guide to cybersecurity. The standard contains 14 thematic categories and 114 controls. Each control may be unrelated to the enterprise for which the audit is conducted. The essence of ISO-27001:2013 involves the analysis of each control and determination of its level of compliance with the standard.

The main concept of ISO-27001 [4] is the identification of information security risk and the application of appropriate controls to reduce the risk. The ISO-27005 standard is an extremely important standard that describes risk management methods in cyber security. The ISO-27037 standard [5] defines guidelines related to security practices that can identify, collect, retrieve, and preserve digital evidence.

The authors of the article [6] apply the project management methodology for information security and cyber security, which is based on the ISO-27001:2013 standard. This methodology was developed and implemented in fifty small and medium-sized enterprises located in the central region of Portugal. The participants of the project were the Polytechnic University of Leiria and a group of IT auditors/consultants. The authors provide a comparative analysis of the use of different audit types usages and the benefits received from their implementation.

Mubarak et al [7] claim that one of the proven ways of managing information security is the usage of available international standards, frameworks, and best practices in an enterprise.

The authors of the article [8] investigate gaps in the ISO-27001 standard regarding its application to small and medium-sized businesses. The main trends and recommendations for a successful methodology of information security management are defined and presented in a form of the Small Business Standard.

The Objective of the work is a study of the project management peculiarities in the cyber security, which the cyber security manager faces. It is also necessary to outline the basic knowledge domain areas that a cybersecurity project manager should additionally possess.

Statement of the task. To study the peculiarities of project management in the field of cyber security, it is necessary to solve the following tasks:

1. Provide a clear definition of the project in the cyber security area.
2. To present the necessary domain knowledge for a project manager in the field of cyber security.
3. Compare each project process from the PMI process group.
4. Provide conclusions and recommendations on the use of tools and techniques for effective project management.

Cybersecurity project. It is extremely important to be clear about what is considered a project in the cybersecurity field. However, it is first necessary to separate and distinguish the terms information security and cyber security.

The concepts of information security and cyber security are very intertwined, and therefore for most stakeholders, the understanding of processes and tasks is not always clearly understood. It is very important to understand the differences between these similar areas during project implementation. According to the ISO-27032 standard, information security is concerned with «the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user» (ISO, 2012). On the other hand, cybersecurity is defined as «the preservation of confidentiality, integrity and availability of information in the cyberspace». The relationship between information security and cyber security is presented in fig. 1.

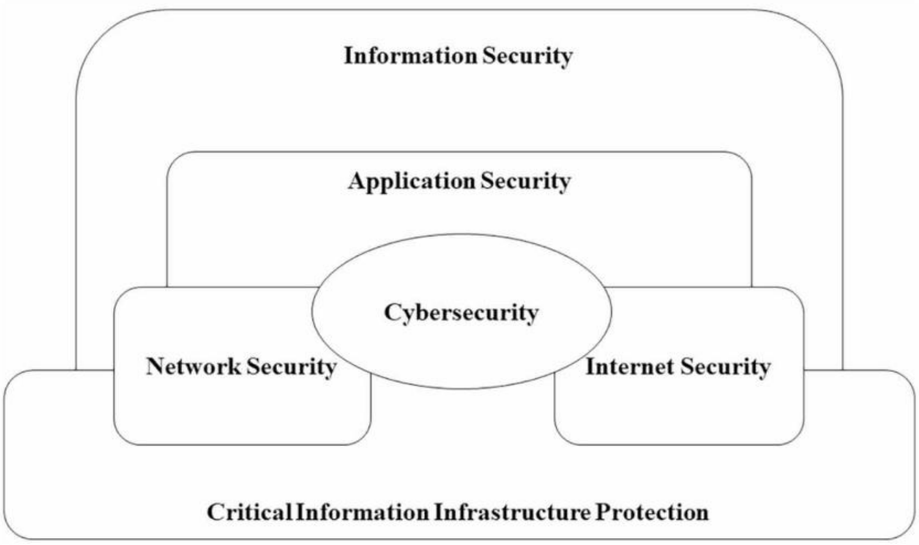

Figure 1. Relationship between cybersecurity and other security domains (redrawn from ISO/IEC 27032 (ISO/IEC, 2012))

Accordingly, cyber security is based on information security, application security, network security, and Internet security.

The definition of the term «project» is the next stage for researching the project management peculiarities in the field of cyber security. According to the PMI standard, a project [9] is a temporary endeavor undertaken to create a unique project service or result. That is, the main characteristics of the project are its beginning and end, as well as obtaining a unique result. Usually, the uniqueness of the result means modern developments, innovations, and innovative technologies. However, the uniqueness of the project results involves the uniqueness of the project implementation conditions, the technical statement of work, the formed team, technology, and resources. The result of the project will not always be new and innovative. Let's present a specific example of the project: a website implementation for a certain organization. The development of a web resource can be performed on existing technologies, and ready-made content management systems, which do not reflect any innovation regarding the technical component of the project. However, the design (color scheme, author's elements, concept) of this web resource will be unique to this organization, although the design elements will be determined by the main trends of UX/UI design. For IT developers, such a project is considered a typical implementation.

The main characteristic of the project is its execution time: start and finish. It is extremely important to distinguish between «project» execution and «process» continuity. To make the distinction, let's give an example: there is an organization that provides services for the implementation of cyber security projects to an external organization and conducts actions to ensure a sufficient level of cyber protection within the organization. Maintaining a certain level of protection is a continuous process that has a beginning and does not end during the existence of the organization, requiring repetitive work to check cybersecurity every day by an expert.

It is also necessary to understand the difference between the project and the support of this project for a certain period after its implementation, as a separate type of work that is not included in the scope of the project. Let's present an example for a better understanding of the difference between the terms «project» and «support»: a leak of valuable information is recorded in the organization. It indicates damage to the cyber security system. Investigating the cause of information leakage, reading all existing registry logs, and implementing improvements and fixes to further prevent such a scenario is a support task. Such type of work is characterized by significant use of resources at the issue time, a significantly short execution time, and a significant level of uncertainty.

Therefore, the term «Cybersecurity project» will be understood as a temporary endeavor undertaken to create a unique project service or result to preserve confidentiality, integrity, and availability of information in the cyberspace.

Cybersecurity project manager. According to PMI standards, a project manager should possess the following knowledge of the domain areas:

1. Technical area.
2. Soft skills area.
3. Business area.

The technical area of knowledge involves the project manager’s understanding of the main project management methodologies; waterfall, agile, scrum; software; product or service development models: incremental or iterative; ability to work under various types of contracts: fixed price and their derivatives, time and material.

Soft skills area involves the project manager's ability to work with the team, stakeholders, and engage experts in the project. One of the main skills of a manager is resolving conflicts in favor of the project and taking into account all interested parties, motivating developers or experts in the field of cyber security, developing human resources for their further effectiveness in the organization and in general.

Business area involves understanding the basic principles of conducting business in general: feasibility of project implementation, benefits obtained from the creation of a product or result. In previous years, the business area was not mandatory according to the standard, but starting from 2020, it is included in the mandatory part of project manager training.

It should be noted that the project manager may not have technical skills in programming or creating an IT product according to the PMI standard. There is a certain category of managers who are defined as Technical Project Manager, a person who has the necessary stack of knowledge about writing code, setting up servers or understands the technical architecture of the product.

Regarding the Cybersecurity manager, there are also requirements for knowledge in eight basic domains defined by the International Information System Security Certification Consortium [10], namely:

1. Security and Risk Management.
2. Asset Security
3. Security Engineering and Architecture.
4. Communications and Network Security.
5. Identity and Access Management.
6. Security Assessment and Testing.
7. Security Operations.
8. Software Development Security.

To be effective, a cybersecurity manager needs to traverse the technology and understand its inner workings: develop or understand the information security charter, information security policy, and security incident response plan, various IT policies and procedures.

Fig. 2 represents the necessary knowledge and skills that a cybersecurity manager must possess, namely: specific knowledge in the field of cyber security to conduct a security audit of an existing organization, create requirement list for ensuring the required level of cyber protection, execute a project in accordance with the requirements; knowledge in the field of project management for effective project management and teamwork.

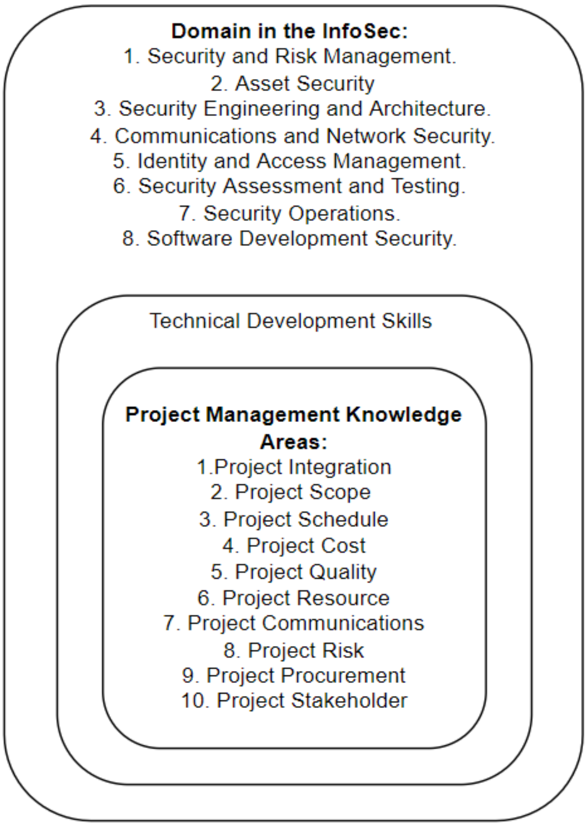
Domain in the InfoSec:
1. Security and Risk Management.
2. Asset Security
3. Security Engineering and Architecture.
4. Communications and Network Security.
5. Identity and Access Management.
6. Security Assessment and Testing.
7. Security Operations.
8. Software Development Security.
Technical Development Skills
Project Management Knowledge Areas:
1.Project Integration
2. Project Scope
3. Project Schedule
4. Project Cost
5. Project Quality
6. Project Resource
7. Project Communications
8. Project Risk
9. Project Procurement
10. Project Stakeholder

Figure 2. A necessary knowledge stack for a cybersecurity manager

Features of the cybersecurity project. Together with external infosec experts from organizations implementing cybersecurity projects, 22 successfully completed projects were analyzed. Based on the received data, a list of features of the cybersecurity project was formed within the framework of the non-disclosure agreement and structured in accordance with the project management process group (I – initiating, P – planning, E – executing, MC – monitoring and controlling, C – closing) of the PMI standard. The results are presented in table 1.

Table 1

The main features of the cybersecurity project by the project management processes

Phase	Process	Feature
1	2	3
I	4.1 Develop project charter	One of the purposes of signing the project charter is to define preapproved financial resources. According to the PMI standard, the real cost of the project can range from -25% to +75% of the previously preapproved cost. Performing a preliminary cyber security audit in order not to exceed the costs limits and to determine the key goals of the project is necessary to implement this project stage. It is the peculiarity of this process. Only after having a large part of the information, the contractor will be able to assess the customer’s current level of security, necessary cyber security actions and sign this document with some reliability. This process is characterized by a significant duration for substantiating a given level of compliance.

To be contінied

1	2	3
I	13.1 Identify Stakeholders	External projects require the involvement of all employees of the customer's organization as project stakeholders. The scale of the project increases the number of stakeholders, whose management in the future is also complicated. In the case of distributed teams, identification of stakeholders requires considerable time. This process is characterized by the complexity of identifying all stakeholders, and in the subsequent implementation of cyber protection, taking into account their job position and requirements.
P	5.2 Collect requirements	Cybersecurity projects are personalized for a certain organization, which requires detailed research and identification of cyber security requirements, taking into account the customer’s organizational structure, location, compliance with the requirements of state regulators.
P	6.5 Develop schedule	They take place only on the basis of detailed and validated requirements, taking into account the risks.
P	7.3 Determine Budget	
P	8.1 Plan Quality Management	Establishing appropriate metrics for the quality of project execution is fuzzy. The customer usually determines the quality – passing a certain audit from the regulators of his business. Establishing real quality metrics of the completed project significantly increases the cost of its implementation.
P	11.2 Identify Risks	The most significant risks are related to the requirements of the state regulator in the field of cyber security, or the requirements of third parties involved in the implementation of the customer's business processes. The least significant, but most widespread risk is the risk of information loss due to a poorly configured communication strategy.
E	10.2 Manage Communications	When implementing a project for an organization with spatially distributed departments, it is necessary to apply significant regulatory techniques for communication: determining the person responsible for one or another department in terms of informativeness, manage a communication schedule between departments, checking the reliability of the information received.
MC	6.6 Control Schedule	Significant delays related to the work of state regulators, causing the use of back-up buffers of time and funds. All investigated projects used reserves several times.
MC	7.4 Control Costs	
MC	11.7 Monitor Risks	Occurs with higher frequency than with typical software development projects.

For the cyber security project implementation, a mixture of methodologies was usually used. For example scrum with the critical chain with clearly defined milestones. The flexible scrum methodology allows you to make changes within the budget and is quite suitable for the implementation of team management. By using the critical chain, a critical sequence of tasks that must be performed to achieve the appropriate level of cyber protection is determined, and time buffers are set, or delays for the implementation of Risk Responses. One of the positive characteristics of using the critical chain method is the possibility of parallelizing activities into feeds based on priority. Also, indicating a milestone on the critical path facilitates control over project resources, based on it all stakeholders can assess the current state of the project and make certain adjustments.

The usage of methodologies in their permanent design causes various limitations. The waterfall method involves performing the next task only after completing the previous one. However, it is necessary to carry out rescheduling in case of delay caused by the regulator's work or the risk occurrence in order to avoid the delay of the entire project.

Applying only flexible methodology causes limitations on project evaluation and control. The Scrum methodology involves evaluating tasks in story points. Such gradation is not clear to the customer.

An important feature of the project’s cyber defense implementation is the interest of the customer’s state or country. In essence, the state can act as a customer of cybersecurity projects at its state enterprises, and on the other hand, it is one of the regulators of state policy regarding the main principles of ensuring cyber security of Ukraine [11].

Conclusions.

1. Cybersecurity project is as a temporary endeavor undertaken to create a unique project service or result to preserve confidentiality, integrity, and availability of information in the cyberspace.

2. Cybersecurity manager must possess not only knowledge in the project management area, but also the main domains in the cybersecurity.

3. Cybersecurity projects are characterized by the following features: a long-term initialization phase caused by additional audits before project implementation; a significant level of personalization of projects in accordance with the customer organization; difficulties in collecting requirements and forming the project scope; the involvement of a significant number of regulators who have a neutral interest in the implementation of the project, but significant influence; involvement of the state regulator in the field of cyber security.

4. Taking into account the peculiarities of cybersecurity project management, a mix of project management methodologies is best suited.

References

1. PMI (2022). PMBOK Guide [Online]. URL: https://www.pmi.org/pmbok-guide-standards/foundational/PMBOK.
2. Andreichenko A. V., Horbachenko S. A., Dykyi O. V. Osoblyvosti upravlinnia proiektamy u sferi kiberzakhystu. Cybersecurity. Vol. 2 (10). 2020. P. 45–51. DOI: https://doi.org/10.28925/2663-4023.2020.10.4553
3. ISO-ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements. 2022. URL: https://www.iso.org/standard/54534.html.
4. Information Security Management System ISMS. 2022. URL: https://www.isms.online/information-security-management-system-isms/.
5. ISO-ISO/IEC 27037:2012. Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. 2022. URL: https://www.iso.org/standard/44381.html.
6. Antunes M., Maximiano M., Gomes R. J., Pinto D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal, Journal of cybersecurity and privacy. Vol. 1. 2021. P. 219–238. DOI: https://doi.org/10.3390/jcp1020012

7. Mubarak S., Heyasat H., Wibowo S. Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review. In Proceedings of the Australasian Conference on Information Systems. 2019. P. 148–154.
8. Ozkan B. Y, Spruit M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a research agenda. Int. J. Stand. Res. Vol. 17. P. 41–72. DOI: https://doi.org/10.4018/IJSR.20190701.oa1
9. Weaver P. (2010). Understanding Programs and Projects Oh, There's a Difference! Paper presented at PMI® Global Congress. URL: https://www.pmi.org/learning/library/understanding-difference-programs-versus-projects-6896.
10. Luke Irwin (2019) The 8 CISSP domains explained. URL: https://www.itgovernance.co.uk/blog/the-8-cissp-domains-explained.
11. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII, redaktsiia vid 03.07.2020. 2020. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Список використаних джерел

1. PMI (2022). PMBOK Guide. URL: https://www.pmi.org/pmbok-guide-standards/foundational/PMBOK.
2. Андрейченко А. В., Горбаченко С. А., Дикий О. В. Особливості управління проєктами у сфері кіберзахисту. Кібербезпека. № 2 (10). 2020. С. 45–51. DOI: https://doi.org/10.28925/2663-4023.2020.10.4553
3. ISO-ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements. 2022. URL: https://www.iso.org/standard/54534.html.
4. Information Security Management System ISMS. 2022. URL: https://www.isms.online/information-security-management-system-isms/.
5. ISO-ISO/IEC 27037:2012. Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. 2022. URL: https://www.iso.org/standard/44381.html.
6. Antunes M., Maximiano M., Gomes R. J., Pinto D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal, Journal of cybersecurity and privacy. Vol. 1. 2021. P. 219–238. DOI: https://doi.org/10.3390/jcp1020012
7. Mubarak S., Heyasat H., Wibowo S. Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review. In Proceedings of the Australasian Conference on Information Systems. 2019. P. 148–154.
8. Ozkan B. Y, Spruit M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a research agenda. Int. J. Stand. Res. Vol. 17. P. 41–72. DOI: https://doi.org/10.4018/IJSR.20190701.oa1
9. Weaver P. (2010). Understanding Programs and Projects Oh, There's a Difference! Paper presented at PMI® Global Congress. URL: https://www.pmi.org/learning/library/understanding-difference-programs-versus-projects-6896.
10. Luke Irwin (2019) The 8 CISSP domains explained. URL: https://www.itgovernance.co.uk/blog/the-8-cissp-domains-explained.
11. Про основні засади забезпечення кібербезпеки України: Закон України № 2163- VIII, редакція від 03.07.2020. 2020. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

УДК 65.011.56:004

ОСОБЛИВОСТІ УПРАВЛІННЯ ПРОЄКТАМИ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Марія Стадник; Андрій Паламар

Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

Резюме. *Управління проєктами є універсальними інструментом для ефективної реалізації певних дій щодо досягнення результатів. Застосування відповідного методології управління проєктом передбачає відповідності умов та особливостей проєкту. В статті досліджено сутність проєкту у галузі кібербезпеки на основі проведеного аналізу сутностей "процесу" та "супортової задачі чи дії". Визначено, що проєкт у галузі кібербезпеки є це тимчасовою дією для створення унікальної послуги чи результату з метою збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. Тимчасовість проєкту забезпечується визначеними термінами початку* *та завершення, а унікальність результату проєкту формується вимогами замовника, умовами виконання та використаними технологіями та технікам щодо його реалізації. В роботі також досліджено вимоги щодо проєктного менеджера в галузі кібербезпеки. Незважаючи на те, що згідно стандарту* Project Management Institute *проєктний менеджер повинен розуміти і ефективно застосовувати відповідну методологію управління проєктом в заданих умовах визначених замовником, володіти навичками ведення ефективної комунікації, мати достатній рівень емоційного інтелекту для формування ефективного мікроклімату роботи в команді, розуміти принципи роботи бізнесу, його ефективності та наявних потреб, але і повинен володіти знаннями у галузі кібербезпеки. Стаття також відображає основні особливості ведення проєктів у сфері кіберзахисту. Проаналізувавши доступну інформацію згідно договорів про нерозголоження даних щодо 22 успішно завершених проєктів було визначено наступні особливості: тривала фаза ініціалізації спричинена попереднім аудитом організації замовника з метою точної оцінки необхідних дій щодо досягнення обговореного рівня кібербезпеки та точнішої оцінки вартості проєкту; значна кількість стейкхолдерів вимагає від проєктного менеджера чіткої стратегії комунікації та документування вимог, визначення основних представників зацікавлених сторін; залежність від значної кількості регуляторів у сфері кібербезпеки є причиною щодо формування використання додаткових резервів часу та грошей на певні затримки; залученням держави у ролі замовника або ж національного регулятора. Для реалізації проєктів у сфері кібербезпеки з врахуванням основних особливостей застосовують кілька методологій в комплексі, з метою забезпечення ефективного управління командою експертів та контролю над обсягом виконаної роботи, графіком та витраченими коштами.*

Ключові слова: *кібербезпека, проєктний менеджер, група процесів управління проєктами, області знань, домен інформаційної безпеки.*

https://doi.org/10.33108/visnyk_tntu2022.02.054 *Отримано 02.03.2022*