МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

КУРІЙ ЄВГЕНІЙ ОЛЕГОВИЧ

УДК 004.057.2

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РАХУНОК ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ

125 Кібербезпека

12 «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ /Курій Євгеній Олегович/

Науковий керівник: Опірський Іван Романович, д.т.н., професор

Львів – 2024

АНОТАЦІЯ

Курій Є. О. **Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека». – ІКТА Національний університет «Львівська політехніка» Україна, Львів, 2024 р.

У сучасному світі, де технології відіграють ключову роль у функціонуванні критичної інфраструктури, кібербезпека стає дедалі важливішою. Кібератаки на енергетичні, транспортні та фінансові системи можуть призвести до серйозних наслідків для економіки та безпеки громадян. Впровадження передових технологій та стандартів аудиту з кібербезпеки є ключовими для ефективного захисту. Однак, існують проблеми, такі як недостатня узгодженість стандартів, складність впровадження та недосвідченість персоналу, які ускладнюють процес забезпечення безпеки та вимагають значних зусиль для подолання.

Дисертаційна робота вирішує зазначені проблеми шляхом перехресного впровадження стандартів аудиту з кібербезпеки. За рахунок використання цього підходу можна досягти більшої узгодженості між різними стандартами, спростити процес впровадження та оцінки відповідності, а також забезпечити більш ефективний захист об'єктів критичної інфраструктури. Такий комплексний підхід дозволить знизити складність процесу забезпечення безпеки та оптимізувати використання ресурсів, надаючи при цьому високий рівень захисту від кіберзагроз.

Об’єктом дослідження є стандарти та процеси аудиту з кібербезпеки.

Предметом дослідження є методи та засоби впровадження стандартів аудиту з кібербезпеки, які включають в себе такі етапи як проведення оцінки на відповідність, проведення оцінки ризиків інформаційної безпеки, розроблення політик і додаткових артефактів інформаційної безпеки організації, і вибір фізичних, технічних та адміністративних контролів, необхідних для ефективного впровадження стандартів аудиту з кібербезпеки.

У процесі досліджень використано методи аналізу, порівняння, індукції, моделювання, вимірювання, експертної оцінки, тестування, консультацій із зацікавленими сторонами та документування.

У першому розділі «**Аналіз стану проблеми впровадження вимог стандартів аудиту з кібербезпеки в об'єктах критичної інфраструктури»** досліджується важливість захисту критичної інфраструктури України, особливо в контексті загроз кібербезпеці, зумовлених гібридною війною росії. Впровадження різноманітних стандартів аудиту з кібербезпеки, таких як ISO 27001, NIST SP 800-53, SOC 2, PCI DSS та інших, визначається як ефективний метод захисту. Ці стандарти надають організаціям структурований підхід до забезпечення безпеки інформації, включаючи захист конфіденційності, цілісності та доступності, оцінку та зменшення ризиків, відповідність законодавству, а також постійне вдосконалення систем безпеки. Проте впровадження цих стандартів часто ускладнюється відсутністю розуміння та ресурсів, а також складністю вибору та впровадження відповідного стандарту. Для подолання цих проблем необхідне правильне планування, розуміння контексту організації, ризик-орієнтований підхід та вивчення спільних рис та відмінностей різних стандартів аудиту з кібербезпеки.

У другому розділі **«Обґрунтування методології перехресного впровадження декількох стандартів кібербезпеки для підвищення**

захищеності об’єкта критичної інфраструктури» був проведений детальний аналіз стандарту ISO 27001, визначеного як один з ключових у галузі інформаційної безпеки. Аналіз дозволив краще зрозуміти вимоги, структуру та принципи цього стандарту, включаючи нову редакцію 2022 року. Особлива увага була приділена порівняльному аналізу з попередньою версією 2013 року, а також розробці перехресної відповідності між контролями для полегшення переходу між версіями та узгодження з іншими відомими стандартами кібербезпеки, такими як NIST SP 800-53, SOC 2 та PCI DSS. Це дослідження виявило переваги такої методології, зокрема підвищення рівня безпеки активів, повноту охоплення ризиків та підвищення довіри клієнтів, але також відзначило його недоліки, такі як складність впровадження та підтримки декількох стандартів. Загалом, це дослідження надає важливі висновки для розуміння та оптимізації систем управління інформаційною безпекою в організації.

Третій розділ «**Розроблення універсального алгоритму і методу оцінки захищеності об'єкта критичної інфраструктури на основі стандартів кібербезпеки»** присвячено розробці універсального алгоритму та методології оцінки захищеності об'єкта критичної інфраструктури, заснованого на використанні стандартів кібербезпеки. Шляхом аналізу існуючих методів впровадження стандартів було визначено їхні недоліки, після чого розроблено інноваційний метод оцінки відповідності системи управління інформаційною безпекою об’єкта критичної інфраструктури вимогам стандарта ISO 27001 на основі контрольного списка. Крім того, розроблено методологію оцінки ризиків інформаційної безпеки, яка включає визначення активів, ідентифікацію та оцінку ризиків, та визначення стратегії обробки ризиків. Також розроблено методологію перехресного впровадження стандартів аудиту з кібербезпеки на основі зіставлення їхніх контролів безпеки та визначено перелік документації для досягнення

відповідності стандарту. Результатом дослідження є комплексний підхід до забезпечення захищеності об'єкта критичної інфраструктури, що враховує сучасні підходи та вимоги у галузі кібербезпеки, сприяючи ефективному управлінню загрозами та ризиками і забезпечуючи високий рівень безпеки.

У четвертому розділі **«Розроблення системи для оцінки захищеності об’єкта критичної інфраструктури та забезпечення його відповідності стандартам кібербезпеки»** представлено метод і форму оцінювання для аналізу організації на відповідність стандарту ISO 27001 та впровадження стандартів аудиту кібербезпеки. Також у розділі проведено оцінку ступеня перехресного покриття стандартів кібербезпеки та оцінено ефективність застосування розробленої методології для впровадження стандартів.

Ефективність та переваги запропонованої у дослідженні методології порівняно з аналогами демонструють її значний потенціал у підвищенні рівня кібербезпеки в організаціях та об’єктах критичної інфраструктури, що стає важливим кроком у їхньому захисті від сучасних кіберзагроз.

Подальше дослідження даної проблематики буде направлене на вдосконалення прототипу системи для впровадження стандартів аудиту з кібербезпеки та розширення зони її охоплення за рахунок опрацювання додаткових стандартів.

У **висновках** дисертаційної роботи викладено основні результати дослідження і рекомендації, які випливають з проведених досліджень.

У **додатках** до дисертації долучено акти впровадження дисертаційного дослідження, шаблони для проведення оцінки на відповідність та оцінки ризиків, шаблон Політики Інформаційної Безпеки, а також список наукових праць і апробацій автора за темою дисертації.

Ключові слова: інформаційна безпека, кібербезпека, кіберзагроза, об'єкти критичної інфраструктури, інформаційна система, система управління інформаційною безпекою, безпека даних, ISO 27001, SOC 2,

NIST, PCI DSS, стандарт кібербезпеки, оцінка на відповідність, управління інформаційними ризиками, аудит кібербезпеки.

Список публікацій здобувача:

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Kurii, Y. Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32;

2. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 6–20.doi: https://doi.org/10.15587/1729-4061.2023.273363;

3. Kurii, Y. ., & Opirskyy, I. (2023). ISO 27001: АНАЛІЗ ЗМІН ТА ОСОБЛИВОСТІ ВІДПОВІДНОСТІ НОВІЙ ВЕРСІЇ СТАНДАРТУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655;

4. Євгеній Курій, Віталій Сусукайло, Іван Опірський (2023). РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001. Ukrainian Information Security Research Journal. 25(3):132-139. DOI: https://doi.org/10.18372/2410-7840.25.17938;

5. Vakhula O., Kurii Y., Opirskyy I., Susukailo V. (2024) Security-as-code concept for fulfilling ISO/IEC 27001:2022 requirements // Paper presented at the CEUR Workshop Proceedings, vol. 3654, . 59–72.

6. Курій Є. О., Опірський І. Р. (2024) Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS // Кібербезпека: освіта, наука, техніка. – Т. 3, № 23. – С. 145–155. DOI: https://doi.org/10.28925/2663-4023.2024.23.145155

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Yevhenii KURII, Ivan OPIRSKYY, Leonid BORTNIK ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD // Materials of IXth International Scientific and Technical Conference INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY, May 25–26, 2023. - Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6;

8. Курій Є. О., Опірський І. Р. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ ФРЕЙМВОРКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 85): матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 15-16 лютого 2024 р.). – 2024. – С. 34–36.

9. Курій Є. О., Опірський І. Р. АНАЛІЗ ПЕРЕВАГ І НЕДОЛІКІВ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ // Materials of the V International Research and Practical Internet Conference «Development Strategies for Modern Education and Science», – 2024. – 2024. – С. 16–17.

SUMMARY

Kurii Y.O. **Methodology for increasing the security of critical infrastructure through the cross-implementation of the cybersecurity standards** – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the specialty 125 «Cyber Security». – Lviv Polytechnic National University, Lviv, 2024.

In today's world, where technology plays a key role in the operation of critical infrastructure, cyber security is becoming increasingly important. Cyberattacks on energy, transportation, and financial systems can lead to serious consequences for the economy and the security of citizens. Implementing advanced cybersecurity technologies and security standards is key to effective protection. However, there are challenges such as lack of consistency of standards, complexity of implementation, and lack of experience of personnel, which complicate the security process and require significant efforts to overcome.

The dissertation addresses these issues by employing cross-implementation of cybersecurity audit standards. This approach enhances consistency among different standards, simplifies implementation and gap assessment processes, and ensures more effective protection of critical infrastructure assets. This comprehensive strategy aims to reduce the complexity of security procedures and optimize resource utilization while maintaining a high level of protection against cyber threats.

The object of the research is cyber security audit standards and processes.

The subject of research is the methods and means of implementing cyber security audit standards, which includes such stages as conducting a gap assessment, conducting an information security risk assessment, developing policies and additional artifacts of the organization's information security, and

selecting physical, technical and administrative controls necessary for effective implementation of cyber security audit standards.

In the process of research, methods of analysis, comparison, induction, modeling, measurement, expert evaluation, testing, consultation with interested parties and documentation were used.

The first chapter, **«Analysis of the state of the problem of implementation of the requirements of cyber security audit standards in critical infrastructure objects»,** delves into the critical importance of protecting Ukraine's critical infrastructure, particularly amidst the cyber security threats posed by russia's hybrid warfare tactics. It identifies the implementation of various cybersecurity audit standards such as ISO 27001, NIST SP 800-53, SOC 2, PCI DSS, and others as an effective means of protection. These standards offer organizations a structured approach to ensuring information security, covering aspects like safeguarding confidentiality, integrity, and availability, as well as assessing and mitigating risks, ensuring compliance with regulations, and continually enhancing security measures. However, challenges in implementing these standards often arise from a lack of understanding and resources, as well as the complexity of selecting and implementing an appropriate framework. Overcoming these obstacles requires proper planning, a deep understanding of the organization's context, a risk-oriented approach, and a thorough examination of the commonalities and differences among various information security frameworks.

In the second chapter, **«Justification of the method of increasing the security of critical infrastructure objects by the simultaneous implementation of several cyber security standards»,** a comprehensive examination of the ISO 27001 standard, recognized as pivotal in the realm of information security, was conducted. This analysis aimed to deepen insights into the requirements, framework, and underlying principles of this standard, with a

focus on the latest 2022 edition. Emphasis was placed on comparing it with the previous 2013 version and devising a cross-mapping approach for controls to ease the transition and harmonize with other popular cybersecurity standards like NIST SP 800-53, SOC 2, and PCI DSS. The study identified the method's advantages, such as enhanced asset security, extensive risk coverage, and heightened customer trust, alongside its challenges, such as the complexity associated with implementing and sustaining multiple standards. Overall, these findings offer valuable insights for optimizing information security management systems within organizations.

The third chapter, **«Development of a universal algorithm and method of assessing the security of a critical infrastructure object based on cyber security standards»,** focuses on developing a universal algorithm and method for evaluating the security of critical infrastructure objects based on the cyber security standards. Through an analysis of existing implementation methods, shortcomings were identified, leading to the development of an innovative gap assessment method for ISO 27001 requirements using a detailed checklist. Furthermore, the methodology for conducting information security risk assessment was created, encompassing asset identification, risk analysis, risk assessment, and development of mitigation strategy. Additionally, a control implementation methodology was developed, accompanied by a documentation list to aid in achieving compliance with the standard. The outcome of the study is a comprehensive approach to critical infrastructure security, integrating contemporary cyber security approaches and requirements, thereby enhancing threat and risk management effectiveness and ensuring a high level of security.

The fourth chapter, **«Development of a system for assessing the security of a critical infrastructure object and its compliance with cybersecurity standards»,** outlines the method designed for analyzing an organization's adherence to the ISO 27001 standard and the implementation of cybersecurity

audit standards. This chapter also evaluates the extent of overlaping among cybersecurity standards and assesses the effectiveness of the methodology in implementing these standards.

The demonstrated effectiveness and advantages of the proposed methodology compared to alternatives underscore its significant potential in elevating cyber security controls within organizations. This marks a crucial step toward safeguarding critical infrastructure against modern cyber threats.

Further research on this topic will focus on refining the system prototype for implementing cybersecurity audit standards and broadening its application by covering additional standards.

In the dissertation **conclusions**, the main research findings and recommendations resulting from the conducted research are summarized.

The **appendices** to the dissertation include documentation of the dissertation research implementation, templates for gap assessment and risk assessment, an Information Security Policy template, as well as a list of the proceedings where basic scientific results of thesis were published and scientific works certifying the approval of the dissertation materials.

Keywords: information security, cybersecurity, cyber threat, critical infrastructure objects, information systems, information security management system, data security, ISO 27001, SOC 2, NIST, PCI DSS, cybersecurity standard, gap assessment, information risk management, cybersecurity audit.

The list of author's publications:

Proceedings where basic scientific results of thesis were published:

1. Kurii, Y. Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32;

2. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 6–20.doi: https://doi.org/10.15587/1729-4061.2023.273363;

3. Kurii, Y. ., & Opirskyy, I. (2023). ISO 27001: ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD. Electronic professional scientific publication «Cybersecurity: education, science, technology», 3(19), 46–55. DOI: https://doi.org/10.28925/2663-4023.2023.19.4655;

4. Kurii Y., Susukailo V., Opirskyy I. (2023). DEVELOPMENT OF A METHODOLOGY FOR ASSESSING COMPLIANCE WITH ISO 27001 STANDARD. Ukrainian Information Security Research Journal. 25(3):132-139. DOI: https://doi.org/10.18372/2410-7840.25.17938;

5. Vakhula O., Kurii Y., Opirskyy I., Susukailo V. (2024) Security-as-code concept for fulfilling ISO/IEC 27001:2022 requirements // Paper presented at the CEUR Workshop Proceedings, vol. 3654, . 59–72.

6. Kurii, Y., Opirskyy, I. (2024) Security of payment transactions: Overview and characteristics of key changes in the new edition of the PCI DSS standard // Electronic professional scientific publication «Cybersecurity: education, science, technology», – T. 3, № 23. – P. 145–155. DOI: https://doi.org/10.28925/2663-4023.2024.23.145155

Scientific works certifying the approval of the dissertation materials:

7. Yevhenii KURII, Ivan OPIRSKYY, Leonid BORTNIK ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD // Materials of IXth International Scientific and Technical Conference INFORMATION

PROTECTION AND INFORMATION SYSTEMS SECURITY, May 25–26, 2023. - Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6;

8. Kurii Y., Opirskyy I. COMPARATIVE CHARACTERISTICS OF THE MAIN INFORMATION SECURITY FRAMEWORKS // Information society: technological, economic and technical aspects of development (issue 85): materials of the International Scientific Internet Conference, (Ternopil, Ukraine; Opole, Poland, February 15-16, 2024). – 2024. – P. 34–36.

9. Kurii Y., Opirskyy I. ANALYSIS OF THE ADVANTAGES AND DISADVANTAGES OF CROSS-IMPLEMENTATION OF CYBERSECURITY STANDARDS IN CRITICAL INFRASTRUCTURE OBJECTS // Materials of the V International Research and Practical Internet Conference «Development Strategies for Modern Education and Science», – 2024. – 2024. – P. 16–17.

ЗМІСТ

АНОТАЦІЯ 2
SUMMARY 8
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 16
ВСТУП 17
РОЗДІЛ 1. АНАЛІЗ СТАНУ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ВИМОГ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ В ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 29
1.1 Аналіз сучасного стану досліджень та публікацій 29
1.2 Визначення і опис поняття об'єкт критичної інфраструктури 33
1.3 Огляд резонансних атак на критичну інфраструктуру України 38
1.3.1 Атаки на енергетичні компанії України 38
1.3.2 Атака вірусом NotPetya 40
1.3.3 Кібератаки на українські державні сайти 42
1.4 Аналіз сучасних стандартів аудиту з кібербезпеки 44
1.4.1 Аналіз стандарту ISO 27001:2022 46
1.4.2 Аналіз стандарту NIST SP 800-53 51
1.4.3 Аналіз TSC від AICPA (SOC 2) 54
1.4.4 Аналіз стандарту PCI DSS v.4.0 56
1.5 Аналіз проблем впровадження стандартів аудиту з кібербезпеки 58
1.6 Порівняльна характеристика основних стандартів аудиту з кібербезпеки з погляду ширини покриття 60
1.7 Висновки до першого розділу 62
РОЗДІЛ 2. ОБҐРУНТУВАННЯ МЕТОДОЛОГІЇ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ ДЕКІЛЬКОХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ 64
2.1 Дослідження і зіставлення контролів редакцій стандарту ISO 27001 2013 і 2022 року 64
2.1.1 Виявлення основних критеріїв і особливостей стандарту ISO 27001:2022 64
2.1.2 Визначення відмінностей між редакціями стандарту ISO/IEC 27001 2013 та 2022 років 67
2.2 Розроблення методу зіставлення контролів провідних стандартів аудиту з кібербезпеки 78
2.3 Аналіз переваг і недоліків перехресного впровадження стандартів аудиту з кібербезпеки 85
2.4 Висновки до другого розділу 87
РОЗДІЛ 3. РОЗРОБЛЕННЯ УНІВЕРСАЛЬНОГО АЛГОРИТМУ І МЕТОДУ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ КІБЕРБЕЗПЕКИ 89
3.1 Дослідження та оцінка недоліків існуючих методів впровадження стандартів аудиту з кібербезпеки 89

3.2 Розроблення методу проведення оцінки СУІБ на відповідність стандартам аудиту з кібербезпеки 95
3.2.1 Постановка проблеми проведення оцінки на відповідність 95
3.2.2 Опис процесу проведення оцінки на відповідність з використанням контрольного списка 98
3.3 Розроблення методології оцінки ризиків інформаційної безпеки 104
3.3.1 Ідентифікація активів організації 106
3.3.2 Ідентифікація ризиків інформаційної безпеки для активів 108
3.3.3 Оцінка ризиків на основі розрахунку імовірності настання ризику і впливу 109
3.3.4 Визначення стратегії обробки ризику 114
3.3.5 Обробка і постійний моніторинг ризиків 115
3.4 Розроблення методології перехресного впровадження стандартів аудиту з кібербезпеки на основі зіставлення контролів 118
3.5 Розроблення політик і допоміжних документів для впровадження стандартів аудиту з кібербезпеки 122
3.5.1 Визначення і огляд основних політик в рамках впровадження стандартів 122
3.5.2 Розроблення методології створення політик інформаційної безпеки 140
3.6 Висновки до третього розділу 142
РОЗДІЛ 4. РОЗРОБЛЕННЯ СИСТЕМИ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ ЙОГО ВІДПОВІДНОСТІ СТАНДАРТАМ КІБЕРБЕЗПЕКИ 144
4.1 Розроблення форми оцінювання СУІБ ОКІ на відповідність стандартам аудиту з кібербезпеки 144
4.2 Наповнення системи і тестування взаємодії компонентів системи між собою 147
4.3 Визначення ефективності роботи методології впровадження стандартів аудиту з кібербезпеки та її переваг над сучасними аналогами 147
4.4 Висновки до четвертого розділу 155
ВИСНОВКИ 158
СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ 161
ДОДАТОК А. АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ 178
ДОДАТОК Б. ОГЛЯД ВІДМІННОСТЕЙ МІЖ ВЕРСІЯМИ 4.0 І 3.2.1 СТАНДАРТУ PCI DSS 182
ДОДАТОК В. КОНТРОЛЬНИЙ СПИСОК ДЛЯ ПРОВЕДЕННЯ ОЦІНКИ НА ВІДПОВІДНІСТЬ 191
ДОДАТОК Г. ШАБЛОН ДЛЯ ОЦІНКИ РИЗИКІВ 269
ДОДАТОК Д. ШАБЛОН ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 270

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОКІ	Об’єкт критичної інфраструктури.
СУІБ	Система управління інформаційною безпекою.
AICPA	American Institute of Certified Public Accountants, Американський інститут дипломованих бухгалтерів.
CSF	Cybersecurity Framework, Фреймворк Кібербезпеки.
IDS	Intrusion Detection System, система виявлення вторгнень.
IEC	International Electrotechnical Commission. Міжнародна електротехнічна комісія.
IPS	Intrusion Prevention System, система запобігання вторгненням.
ISMS	Information Security Management System, Система управління інформаційною безпекою.
ISO	International Organization for Standardization, Міжнародна організація по сертифікації.
NIST	National Institute of Standards and Technology, Національний інститут стандартів і технологій.
PCI DSS	Payment Card Industry Data Security Standard, Стандарт безпеки індустрії платіжних карт.
SOC	System and Organization Controls, Контролі систем та організацій.
SP	Special Publication, спеціальна публікація.
TSC	Trust Services Criteria, критерії довірчих послуг.

ВСТУП

У сучасному світі, де високотехнологічні системи стають невід'ємною частиною інфраструктури, загрози кібербезпеці стають все більш важливими та актуальними. Величезні масштаби та серйозні наслідки кібератак на об'єкти критичної інфраструктури відображають потребу у надійних заходах захисту. Порушення безпеки у таких сферах, як енергетика, транспорт, фінанси, можуть мати катастрофічні наслідки для економіки, соціальної стабільності та безпеки громадян. Забезпечення надійного захисту цих об'єктів є надзвичайно важливим завданням, що потребує комплексного підходу та використання передових технологій [1].

Для забезпечення ефективного захисту об'єктів критичної інфраструктури необхідно впроваджувати передові технології та методики кібербезпеки. Стандарти аудиту з кібербезпеки надають систематичний підхід до ідентифікації потенційних ризиків та впровадження заходів з їх запобігання. Вони допомагають упорядкувати процес забезпечення безпеки, створюючи загальноприйняті рамки та вимоги [2].

Однак, впровадження вимог стандартів аудиту з кібербезпеки в об'єктах критичної інфраструктури стикається з рядом проблем та недоліків. Недостатня узгодженість між різними стандартами, велика кількість контролів та вимог, недостатність практичного досвіду у людей відповідальних за впровадження, а також складність їхнього впровадження та оцінки можуть ускладнювати процес забезпечення відповідності та вимагати значних зусиль та ресурсів [3].

Для подолання цих проблем важливо сприяти співпраці між організаціями та стандартизації підходів до кібербезпеки. Також, необхідно надавати належну підтримку та освіту тим, хто відповідає за впровадження

стандартів, щоб забезпечити їхню ефективність та відповідність потребам конкретної організації.

Додатковою проблемою може бути нестача практичного досвіду у впровадженні стандартів кібербезпеки, особливо для тих організацій, які мають обмежені ресурси або обмежений доступ до висококваліфікованих кадрів.

Більше того, впровадження стандартів аудиту з кібербезпеки може вимагати значних витрат часу та ресурсів. Організація повинна бути готовою до вкладення зусиль у вдосконалення своїх процесів та систем безпеки, а також у регулярне оновлення та адаптацію до змін у загрозах кібербезпеки [4].

З урахуванням цих складнощів, ефективне впровадження стандартів аудиту з кібербезпеки на об'єктах критичної інфраструктури вимагає системного підходу, ретельного планування та великої уваги до деталей. Важливо поєднувати технологічні та організаційні заходи з метою створення комплексної системи захисту, яка забезпечує надійність та стійкість інфраструктури в умовах постійної загрози кібератак.

Перехресне впровадження стандартів аудиту з кібербезпеки є важливою стратегією для підвищення ефективності програм забезпечення інформаційної безпеки в організаціях. Цей підхід полягає в тому, щоб використовувати інформацію та ресурси, зібрані під час впровадження одного стандарту, для покриття вимог інших стандартів [5].

До ключових переваг такого підходу можна віднести ефективніше використання ресурсів. Оскільки, впровадження стандартів кібербезпеки може бути витратним за часом та ресурсами процесом, використання інформації, досвіду та напрацювань, набутих під час впровадження одного стандарту, для впровадження інших стандартів дозволяє оптимізувати використання ресурсів [6].

Іншою перевагою є мінімізація дублювання. Часто стандарти аудиту кібербезпеки містять вимоги, які можуть взаємно перекриватися. Перехресне впровадження дозволяє уникнути дублювання зусиль, концентруючись на покритті тих аспектів, які ще не враховані.

Також, таке перехресне впровадження дозволяє досягнути загального підвищення рівня безпеки в організації через забезпечення відповідності більш широкому спектру стандартів кібербезпеки. Це може зменшити ризик виникнення пробілів у захисті інформації, оскільки більше аспектів буде охоплено контролями безпеки.

Окрім того, впровадження різних стандартів кібербезпеки може бути вимогами з боку клієнтів, партнерів або регуляторів. Здійснення перехресного впровадження стандартів дозволяє забезпечити відповідність цим вимогам без додаткових витрат. Це також спрощує процес аудиту та відповідності. Замість того, щоб мати окремі процедури та контрольні точки для кожного стандарту, організація може розробити спільні процеси, які охоплюють вимоги кількох стандартів одночасно [7].

Наостанок, перехресне впровадження дозволяє підвищити прозорість та конкурентоспроможність. Коли організація підтримує відповідність декільком стандартам, це може сприяти підвищенню прозорості та довіри серед зацікавлених сторін, оскільки демонструється широкий спектр заходів забезпечення безпеки. Разом з тим організації, які можуть швидко та ефективно впроваджувати та відповідати вимогам кількох стандартів кібербезпеки, можуть мати перевагу на ринку. Клієнти та партнери можуть більше довіряти таким організаціям, вважаючи їх більш компетентними та надійними в плані захисту інформації [8].

Отже, перехресне впровадження стандартів аудиту з кібербезпеки є стратегічно важливим для ефективного управління ризиками та

забезпечення високого рівня захисту інформації в сучасному цифровому середовищі.

Актуальність. Зростаюча кількість кібератак та загроз інформаційній безпеці ставлять під загрозу функціонування об'єктів критичної інфраструктури, таких як енергетичні системи, транспортні мережі, фінансові установи та інші важливі компоненти сучасного суспільства. Забезпечення надійного захисту об'єктів критичної інфраструктури є надзвичайно важливим для забезпечення економічної стабільності, соціальної безпеки та захисту громадян, і вимагає комплексного підходу та використання передових методів та засобів [9].

У контексті забезпечення інформаційної безпеки об'єктів критичної інфраструктури, одним із ключових інструментів є впровадження стандартів аудиту з кібербезпеки. Ці стандарти надають систематичний підхід до ідентифікації, оцінки та управління ризиками кібербезпеки, допомагають забезпечити прозорість та надійність у сфері захисту інформації.

Однак, впровадження вимог стандартів аудиту з кібербезпеки в об'єктах критичної інфраструктури стикається з рядом проблем та недоліків. Недостатня узгодженість між різними стандартами, велика кількість контролів та вимог, недостатність практичного досвіду у людей відповідальних за впровадження, а також складність їхнього впровадження та оцінки можуть ускладнювати процес забезпечення відповідності та вимагати значних зусиль та ресурсів [10].

Іншою актуальною проблемою, що стосується впровадження стандартів аудиту з кібербезпеки в Україні, є часта орієнтація організацій на відповідність, ніж на реальну безпеку. Це полягає в тому, що компанії не мають на меті забезпечити реальний і достатній набір практик безпеки відповідно до свого профілю ризику, а стараються забезпечити мінімально

необхідний набір контролів, щоб формально відповідати вимогам стандарту, і забезпечити виконання вимог своїх клієнтів. Проблемою такого підходу є те, що хоч організації і можуть підтвердити, що їхні практики відповідають вимогам стандартів аудиту, на практиці, такі організації все ще залишаються дуже вразливими до сучасних загроз і кібератак [11].

Ще однією проблемою яку варто вказати, є постійне оновлення практик безпеки відповідно до зростаючих загроз. Не всі організації мають необхідні ресурси і експертизу для своєчасного контролю і оновлення практик кібербезпеки відповідно до змінного ландшафту загроз. Зокрема, після недавнього оновлення найпопулярнішого стандарту інформаційної безпеки ISO 27001 багато організацій опинилися в ситуації коли вони не мають дієвого плану переходу на оновлену версію стандарту [12].

Дана дисертаційна робота описує переваги та недоліки перехресного провадження стандартів аудиту кібербезпеки на об’єктах критичної інфраструктури і пропонує унікальний метод оцінки відповідності системи управління інформаційною безпекою (СУІБ) об’єкта критичної інфраструктури (ОКІ) сучасним практикам інформаційної безпеки і впровадження стандартів аудиту з кібербезпеки на основі цієї оцінки.

Також ця робота розв'язує науково-практичну задачу підвищення рівня інформаційної безпеки об’єктів критичної інфраструктури за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки.

Одним із ключових результатів дослідження є розроблення універсального методу оцінки захищеності об'єкта критичної інфраструктури на основі стандартів кібербезпеки. Цей підхід дозволить ефективно визначати рівень безпеки об'єктів і розробляти стратегії для підвищення їхньої захищеності.

Крім того, в рамках дисертаційної роботи розроблено систему для оцінки захищеності об'єкта критичної інфраструктури та відповідності стандартам кібербезпеки. Ця система допоможе фахівцям з інформаційної безпеки швидко і точно оцінити стан захищеності об'єктів порівняно з найпоширенішими стандартами, а також згенерувати план і артефакти для досягнення відповідності із застосовними стандартами. Це дозволить організаціям ефективно впроваджувати необхідні заходи з кібербезпеки і забезпечити високий рівень захищеності об'єктів критичної інфраструктури.

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційні дослідження виконувались у відповідності до наукового напряму кафедри захисту інформації Національного університету «Львівська політехніка»

Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни «Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки» для студентів напрямку підготовки 125 «Кібербезпека та захист інформації».

Також, практичні результати дисертаційної роботи впроваджені в діяльності підприємств ТОВ «Бінарікс Україна», ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ», і ТОВ «ПІК РІСОРСИС».

Мета роботи. Метою дисертаційної роботи є підвищення захищеності об’єктів критичної інфраструктури від кіберзагроз за рахунок розроблення методології перехресного впровадження стандартів аудиту з кібербезпеки в об’єктах критичної інфраструктури. Дана методологія сприяє підвищенню рівня інформаційної безпеки та захищеності ОКІ, а також зменшенню часу і ресурсів для досягнення відповідності декільком стандартам аудиту з кібербезпеки одночасно.

Завдання. Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання підвищення рівня інформаційної безпеки та захищеності об'єктів критичної інфраструктури.

Для успішного досягнення мети даної роботи необхідно виконати наступні завдання:

1. Провести аналіз проблеми впровадження вимог стандартів аудиту з кібербезпеки в об’єктах критичної інфраструктури.
2. Провести порівняльний аналіз найпопулярніших і найбільш поширених стандартів аудиту з кібербезпеки.
3. Провести оцінку та зіставлення двох останніх версій стандарту ISO 27001 та оцінити тотожність, на основі розробленої таблиці відповідності, між контролями Додатку А двох версій стандарту.
4. Розробити методологію перехресного впровадження провідних стандартів аудиту з кібербезпеки.
5. Розробити універсальний метод для оцінки СУІБ об’єкта критичної інфраструктури на відповідність стандарту ISO 27001.
6. Розробити методологію для оцінки ризиків інформаційної безпеки об’єкта критичної інфраструктури.
7. Розробити універсальну методологію для створення політик інформаційної безпеки об’єкта критичної інфраструктури.
8. Експериментально визначити ефективність роботи розробленої методології перехресного впровадження стандартів аудиту з кібербезпеки.

Об'єкт дослідження. Об’єктом дослідження є стандарти та процеси аудиту з кібербезпеки.

Предметом дослідження є методи та засоби впровадження стандартів аудиту з кібербезпеки, яка включає в себе такі етапи як проведення оцінки на відповідність, проведення оцінки ризиків інформаційної безпеки, розроблення політик інформаційної безпеки організації, і вибір фізичних,

технічних та адміністративних контролів, необхідних для ефективного впровадження стандартів аудиту з кібербезпеки.

Методи дослідження. У ході наукової роботи були застосовані такі методи: аналіз, порівняння, індукція, моделювання, вимірювання, експертна оцінки, тестування, консультації із зацікавленими сторонами та документування.

Наукова новизна роботи полягає в тому, що:

1. Вперше розроблено методологію проведення перехресного впровадження стандартів аудиту з кібербезпеки за рахунок впровадження розробленої таблиці зіставлення контролів безпеки провідних стандартів. Розроблена методологія дозволяє організаціям і ОКІ уніфікувати взаємозв'язок між різними стандартами аудиту з кібербезпеки, визначити ступінь кореляції їхніх систем управління інформаційною безпекою вимогам визначених стандартів, а також оцінити відповідність контролів безпеки, необхідних для досягнення вимог додатковому стандарту безпеки, що у свою чергу підвищує комплексність та ефективність захисту ОКІ від кіберзагроз.

2. Вперше розроблено метод оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні контрольного списка, який містить детальний перелік перевірок для визначення статусу відповідності контролям безпеки, а також перелік доказів і документів, необхідних для досягнення відповідності. Розроблений метод забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки, скорочує час на впровадження стандарту, і забезпечує комплексний і всебічний захист ОКІ від кіберзагроз.

3. Вперше розроблено метод зіставлення контролів безпеки провідних стандартів на основі встановлення відповідності як між самими контролями

безпеки, так і додатковими рекомендаціями для впровадження конкретних контролів і вимог. Розроблений метод підвищує ефективність захисту ОКІ за рахунок комплексного охоплення контролів безпеки.

4. Вперше розроблено методологію створення політик інформаційної безпеки ОКІ на основі інтеграції зведеної таблиці із зіставленням контролів безпеки провідних стандартів кібербезпеки. Ця методологія підвищує ефективність захищеності ОКІ від загроз за рахунок автоматизації і пришвидшення процесу створення політик інформаційної безпеки з забезпеченням покриття усіх найважливіших доменів і контролів безпеки.

Практичне значення одержаних результатів полягає у можливості використання розробленої методології для уніфікації процесів досягнення відповідності стандартам аудиту з кібербезпеки на ОКІ, при одночасному збільшенні ефективності впровадження цих стандартів, і зменшенні ресурсів і часу на їх впровадження.

1. Розроблено таблицю перехресної відповідності між контролями Додатку А двох останніх редакцій стандарту ISO 27001 – 2013 і 2022 років. Використання розробленої таблиці відповідності скорочує час і ресурси необхідні для впровадження оновленої версії стандарту та приведення СУІБ до відповідності новим вимогам безпеки.

2. Розроблено універсальний шаблон для ідентифікації і управління ризиками інформаційної безпеки ОКІ. Даний шаблон забезпечує досягнення відповідності провідним стандартам аудиту з кібербезпеки, таким як ISO 27001, SOC 2, NIST чи PCI DSS без залучення спеціалістів з інформаційної безпеки.

3. Розроблено алгоритм зіставлення контролів безпеки провідних стандартів аудиту, який дозволяє організаціям і ОКІ забезпечити взаємозв'язок між різними стандартами кібербезпеки та оцінити відповідність їхніх СУІБ вимогам стандартів. Впровадження розробленої, у

результаті використання даного алгоритму, таблиці зіставлення контролів дозволяє автоматизувати процес визначення унікальних контролів безпеки стандартів, зменшити час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки, і забезпечити ефективний захист ОКІ від кіберзагроз шляхом перехресного впровадження вимог декількох стандартів аудиту одночасно.

4. Розроблена таблиця відповідності контролів безпеки провідних стандартів аудиту, таких як ISO 27001, SOC 2, NIST та PCI DSS, демонструє, що у результаті зіставлення контролів безпеки, при впровадженні стандарту ISO 27001:2022 організація покриває в середньому від 66% до 94% контролів інших досліджених стандартів, що зменшує час і ресурси на впровадження унікальних контролів безпеки кожного стандарту.

5. Розроблено форму оцінювання для проведення оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, яка містить детальний перелік перевірок для визначення статусу відповідності контролям безпеки, а також перелік доказів і документів, необхідних для досягнення відповідності. Розроблена форма оцінювання у вигляді контрольного списка забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки і, завдяки розробленим практичним рекомендаціям по впровадження стандарту ISO 27001, скорочує час на впровадження стандарту. Зокрема, використання даної форми, в комбінації з використанням методології перехресного впровадження стандартів аудиту з кібербезпеки, дає змогу впроваджувати стандарти аудиту ефективніше та до 50% швидше в порівнянні з традиційними методами.

Наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри захисту інформації Національного університету «Львівська політехніка», зокрема для студентів спеціальності

125 «Кібербезпека та захист інформації» в курсі лекцій з дисципліни «Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки».

Основні результати дисертаційної роботи використано і впроваджено з метою покращення внутрішніх процесів, пов'язаних з інформаційною безпекою, і сприяння забезпеченню статусу відповідності міжнародним стандартам інформаційної безпеки компаніями ТОВ «Бінарікс Україна», ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ», і ТОВ «ПІК РІСОРСИС», що підтверджено актами впровадження (Додаток А).

Особистий внесок. Важливі наукові результати цієї дисертації були досягнуті автором незалежно. У роботах, опублікованих разом із співавторами, ключовий внесок належить автору. Зокрема, автор вніс наступний вклад (за нумерацією, вказаною у Додатку Д): [3, 5, 7] – аналіз змін у новій версії міжнародного стандарту ISO 27001 і розроблення рекомендацій по його впровадженню; [2] – вдосконалення математичного апарату, який лежить в основі процесу дослідження кібератак і кіберзлочинів; [4] – розроблення універсального методу для оцінки СУІБ організацій і ОКІ на відповідність стандарту ISO 27001; [1, 6, 8, 9] – дослідження стандартів аудиту з кібербезпеки і розроблення методології перехресного впровадження їхніх вимог в об'єктах критичної інфраструктури.

Апробація результатів. Ключові наукові досягнення цієї дисертації були представлені та обговорювались на трьох міжнародних і вітчизняних науково-технічних конференціях та семінарах. Це включає участь у IX Міжнародній науково-технічній конференції «Захист інформації та безпека інформаційних систем» у м. Львів в 2023 році, участь у Міжнародній науковій інтернет-конференції «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» у м. Тернопіль, Україна і м. Ополе, Польща, у 2024 році, та участь у Міжнародній науково-практичній

інтернет-конференції «Development Strategies for Modern Education and Science» у місті Ждяр-над-Сазавою, Чехія, у 2024 році. Окрім цього, дисертаційна робота була повністю представлена на наукових семінарах кафедри Захисту інформації Національного університету «Львівська політехніка».

Публікації. Основні результати дослідження викладено у дев'яти наукових публікаціях, а саме: у шести статтях у фахових наукових виданнях України і трьох тезах виступів на науково-практичних заходах.

Структура та обсяг дисертації. Дисертація складається з вступу, чотирьох розділів, що охоплюють 21 підрозділ, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 287 сторінок, з яких 160 – основний текст, 17 – список використаних джерел (125 найменувань), 110 – додатки.

РОЗДІЛ 1. АНАЛІЗ СТАНУ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ВИМОГ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ В ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Аналіз сучасного стану досліджень та публікацій

Захист об'єктів критичної інфраструктури України завжди мав велике значення в контексті забезпечення стійкості та обороноздатності держави. Одним із ключових напрямів захисту інфраструктури є захист від кібератак, що також закріплюється в Законі України «Про основні засади забезпечення кібербезпеки України» [13], де одним з об'єктів кібербезпеки визначаються об'єкти критичної інфраструктури.

Особливої важливості цей захист набув в останні роки, що пов'язано із розвитком інформаційних технологій, масовим переходом до режиму віддаленої роботи та, найбільшою мірою, зі збройною військовою агресією росії проти України. Зокрема, в розв'язаній війні, північні сусіди неодноразово вдавалися до практики гібридної війни, використовуючи на ряду із застосуванням конвенційної зброї, кібератаки на критичну інфраструктуру і державні урядові сайти. До найбільш масових кібератак росії можна віднести хакерську атаку на підприємства різної форми власності та розміру, державні та недержавні установи із використанням комп'ютерного хробака сімейства Petya у червні 2017; атаку вірусом-хробаком BadRabbit в жовтні 2017 року, масові атаки на українські державні сайти напередодні повномасштабного вторгнення 2022 року та ін. [14]

Зокрема у статті «Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак» [15] С.М. Цяпа розглядає правові та організаційні аспекти забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Звертається увага на позитивний досвід США у забезпеченні стійкості об'єктів критичної інфраструктури та аналізуються положення нової Стратегії

кібербезпеки України, одним з пріоритетів якої визначено удосконалення нормативного забезпечення з питань кіберзахисту об’єктів критичної інфраструктури.

У іншій статті «Framework for critical information infrastructure protection in smart government: a case study in Indonesia» [16] авторами розроблено стандарт для захисту критичної урядової інфраструктури як альтернатива популярним стандартам таким як NIST Cybersecurity Framework і ISO 27001. Запропонована концепція стандарту для захисту даних включає декілька вимірів: цілі, взаємозалежність, функціональність, управління ризиками, ресурси та управління. Всім цим вимірам відповідає 20 елементів і 41 змінна.

У іншій роботі, «Cybersecurity and Protection of Critical Infrastructure» [17] Małgorzata Czuryk досліджує залежність функціонування критичної інфраструктури від інформаційно-телекомунікаційних технологій, які забезпечують безперебійну роботу її обладнання чи засобів. Загрози її функціонуванню можуть становити серйозну проблему для держави та суспільства, оскільки вони також охоплюють стратегічні сектори, що надають важливі послуги і сервіси. Через взаємозв’язок, який об’єднує стратегічні системи в межах критичної інфраструктури та одночасно підтримує її роботу з основними службами, забезпечення кібербезпеки також впливатиме на захист цієї інфраструктури. Слід підкреслити, що критична інфраструктура може бути належним чином захищена шляхом забезпечення кіберстійкості інформаційно-телекомунікаційних систем, які вона використовує, і шляхом співпраці між державним і приватним секторами.

У іншій недавній статті «Methodology of ISMS Establishment Against Modern Cybersecurity Threats» [9], автори В. Сусукайло, І. Опірський та О. Яремко на основі результатів аналізу найпоширеніших методів та

векторів атак за останні роки, розглядають підхід до створення системи управління інформаційною безпекою (СУІБ), що забезпечує необхідні засоби контролю для уникнення поширених сьогодні загроз кібербезпеці. Авторами визначено набір практик інформаційної безпеки, які можуть мінімізувати ризики, пов'язані з сучасними загрозами кібербезпеці та проведено аналіз провідних стандартів аудиту з кібербезпеки, таких як ISO 27001/2, CIS Top 18, NIST 800-53. Також у статті пропонується алгоритм впровадження СУІБ із детальним поясненням кожного етапу та засобів контролю, необхідних для впровадження системи.

Щоб успішно досягати цілей впровадження кібербезпеки на різних рівнях, організаціям слід дотримуватися ряду процедур і стандартів. Стандарти кібербезпеки визначають вимоги, яких має дотримуватися організація, щоб досягти цілей кібербезпеки та сприяти боротьбі з кіберзлочинцями [5], а також забезпечити постійне управління засобами контролю інформаційної безпеки.

Одним з найпоширеніших стандартів інформаційної безпеки в світі вважається стандарт ISO/IEC 27001. Відповідно до даних опитування «The ISO Survey of Management System Standard Certifications 2022», у 2022 році компаніям по всьому світу загалом було видано 67326 сертифікатів ISO 27001, що на 11549 або 21% більше, ніж в попередньому 2021 році [18]. Ці цифри свідчать про стрімке зростання галузі кібербезпеки та важливість впровадження кращих практик безпеки на підприємствах, особливо на об'єктах критичної інфраструктури.

Цей підхід добре простежується у фундаментальному документі «Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури», затвердженому наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (із змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку від 10.07.2022 № 343) [19]. Ці

рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology). Рекомендації можуть використовуватися під час впровадження заходів кіберзахисту, які спрямовані на управління ризиками кібербезпеки для об'єкта критичної інфраструктури, а також для використання іншими суб'єктами забезпечення кібербезпеки і описують загальний підхід до забезпечення кібербезпеки, що дозволяє [19]:

- здійснити аналіз та надати характеристику поточного стану кібербезпеки ОКІ;
- описати цільовий стан кібербезпеки ОКІ;
- ідентифікувати та визначити пріоритети, рівень впровадження заходів кіберзахисту в контексті безперервного та повторюваного процесу управління ризиками у сфері кібербезпеки ОКІ;
- оцінити прогрес у досягненні цільового стану кібербезпеки ОКІ;
- забезпечити комунікацію між суб'єктами, які безпосередньо знаходяться на ОКІ, та із суб'єктами, які є партнерами організації щодо управління ризиками у сфері кібербезпеки.

Загалом, ці рекомендації перегукуються також з іншим відомим документом від Національного інституту стандартів та технологій Сполучених Штатів Америки – NIST Cybersecurity Framework, основним недоліком якого є його ширина і загальність контролів безпеки. Також, дані рекомендації не відповідають потребам організацій і ОКІ у підтвердженні відповідності своїх безпекових процесів визнаним стандартам кібербезпеки шляхом сертифікації.

Наостанок, «Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518» [20] визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури. Відповідно до постанови, кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Постанова також визначає необхідність призначення відповідальних осіб за функціонування та інформаційну безпеку критичних бізнес/операційних процесів; визначення переліку інформаційних, програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; проведення оцінки ризиків на об’єктах критичної інфраструктури; розробку політики інформаційної безпеки тощо.

1.2 Визначення і опис поняття об’єкт критичної інфраструктури

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [21] важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури, ОКІ) визначаються як підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення

функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

Більш детально, до об'єктів критичної інфраструктури відносяться підприємства, установи, організації незалежно від форми власності, які [22]:

- провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, оборонно-промислового комплексу, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;
- надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва харчових продуктів, охорони здоров'я;
- включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;
- підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;
- є об'єктами підвищеної небезпеки;
- є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;
- є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

За секторальним (галузевим) принципом виділяються об’єкти критичної інфраструктури, які забезпечують:

- послуги, що надаються підсекторами електроенергетики, ядерної енергетики, нафти та нафтопродуктів, постачання газу;

- послуги постачання теплової енергії та гарячої води, централізованого водопостачання та централізованого водовідведення, поводження побутовими відходами;
- послуги, що надаються підсекторами авіаційного, автомобільного, залізничного морського та річного транспорту;
- послуги, що надаються фінансовим сектором, поштовим підсектором;
- послуги, що надаються сектором харчової промисловості та агропромислового комплексу, сектором охорони здоров'я, сектором промисловості, сектором цивільного захисту населення та територій.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [21], система кіберзахисту визначається як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Однією зі стратегічних цілей в Стратегії кібербезпеки України [23], яка затверджена Указом Президента України від 26 серпня 2021 р. No 447/2021, визначено, потребу розбудови кіберготовності та системи кіберзахисту – Україна повинна запровадити і реалізувати чіткі та зрозумілі для всіх зацікавлених сторін заходи щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Україна посилить кіберготовність, що полягатиме у здатності всіх зацікавлених сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови їх виникнення, забезпечивши тим самим

кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури та створить національну систему управління інцидентами.

Відповідно до Стратегії кібербезпеки [23], посилення національної кіберготовності та кіберзахисту забезпечуватиметься шляхом:

- розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі;
- розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик;
- впровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичної оцінки ризиків на підставі розроблених методик;
- впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;
- забезпечення розвитку організаційно-технічної моделі кіберзахисту;
- завершення процесів визначення ОКІ та ОКІІ, створення і забезпечення функціонування державного реєстру ОКІІ, постійного перегляду та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;
- запровадження на постійній основі оцінки стану захищеності ОКІІ та державних інформаційних ресурсів на вразливість, встановлення

обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

- впровадження системи аудиту інформаційної безпеки, насамперед на ОКІ, визначення механізмів та базових методик проведення аудитів, встановлення вимог до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;
- забезпечення розвитку систем технічного і криптографічного захисту інформації, пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та ОКІІ;
- створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих ОКІ, їх блокування та визначення пріоритетності.

Нагальну потребу запровадження зазначених заходів підтверджують численні випадки кібератак на об’єкти критичної інфраструктури країн світу. Як свідчать результати аналізу стратегічних цілей національних стратегій кібербезпеки у багатьох країнах (США, Німеччина, Франція, Люксембург) захист ключових об’єктів інфраструктури визнається пріоритетною ціллю на рівні керівництва державою [24].

1.3 Огляд резонансних атак на критичну інфраструктуру України

1.3.1 Атаки на енергетичні компанії України

Електромережа України є об’єктом численних кібератак. Найвідоміша кібератака була здійснена 23 грудня 2015 року. Вона значним чином вплинула на енергорозподільчі компанії, що призвело до масового відключення електроенергії та залишило значну кількість населення без електроенергії на тривалий період часу [25].

У ході цієї атаки, зловмисники використовували фішингову кампанію, надсилаючи заражені документи на електронну пошту співробітникам енергокомпаній. При відкритті та виконанні макросу запускався шкідливий код BlackEnergy3. На початковій фазі атаки, зловмисники здобули доступ до Windows Domain Controllers та зібрали дані, включаючи реквізити та паролі співробітників для мереж VPN. Це дало їм можливість підготувати наступні етапи атаки [25].

Зловмисники спочатку переналаштували пристрої безперебійного живлення (UPS) у диспетчерських центрах, вимикаючи електропостачання та освітлення. Далі вони перепрограмували конвертери на підстанціях, обмеживши дистанційне керування запобіжниками. Вони також здійснювали телефонні атаки на кол-центри енергокомпаній, перекриваючи доступ користувачів та заважаючи сповіщенням про аварії. Хакери замінили програмне забезпечення конвертерів шкідливим кодом, що вимкнуло їх. В кінці атаки, зловмисники використовували програму KillDisk для знищення файлів на комп'ютерах операторів підстанцій, що спричинило їх відключення.

Схожа атака відбулась 19 та 20 лютого 2016 року. Невідомими зловмисниками було здійснено точкове «вірусне розсилання» на електронні адреси (близько 100 одержувачів) великої кількості енергетичних

підприємств України. Завдяки розслідуванню компанії ESET, ми можемо побачити приклади як виглядав лист та заражений документ (Рисунок 1.1) [26]. Завдяки розслідуванню відомо, що планування атаки ГРУ на енергосистему України у 2015-му забрало 19 місяців, а атака 2016-го на електромережі – два з половиною роки.

Електронний лист містить HTML-вміст із посиланням на файл .PNG, розташований на віддаленому сервері, щоб зловмисники отримували сповіщення про те, що електронний лист було доставлено та відкрито ціллю (Рисунок 1.1).

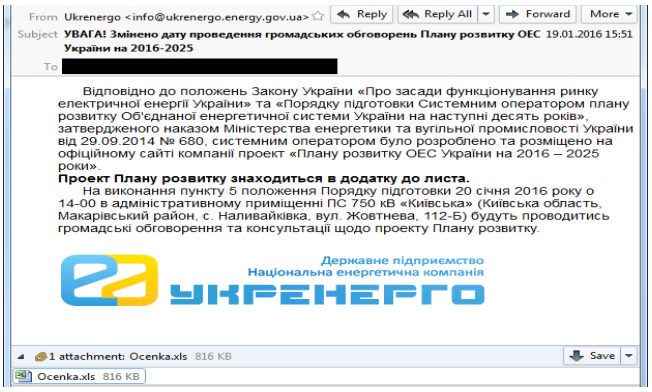


Рис. 1.1. Електронний лист, який отримали користувачі під час атаки на урядові сайти

Шкідливий файл за допомогою соціальної інженерії намагався змусити одержувача проігнорувати вбудоване попередження безпеки Microsoft Office, тим самим необачно запустивши макрос (Рисунок 1.2).

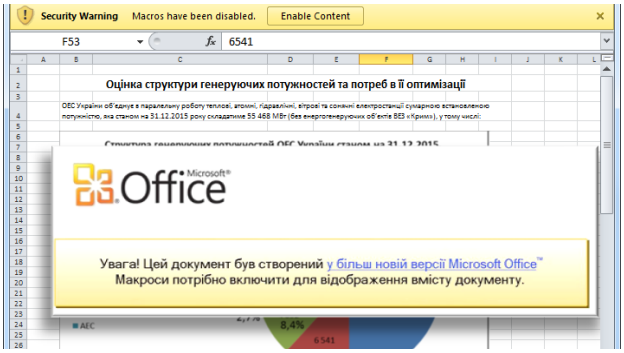


Рис. 1.2. Попередження безпеки Microsoft Office

Виконання макросу призводило до запуску шкідливого трояна-завантажувача, який намагався виконати остаточне завантаження шкідливого вмісту з віддаленого сервера.

1.3.2 Атака вірусом NotPetya

У червні 2017 року відбулася масштабна кібератака, в результаті якої хакерська група Sandworm зламала сервери компанії Linkos Group, виробника програмного забезпечення M.E.Doc. – цей продукт широко використовувався українськими підприємствами для електронного документообігу. Згідно з даними Кіберполіції, близько 2000 компаній, банків і державних установ постраждали в результаті цієї атаки.

Розробники вірусу використовували дві вразливості операційної системи Windows – Mimikatz і EternalBlue. Перша з них дозволяла отримувати логіни та паролі користувачів шляхом зчитування з оперативної пам'яті комп'ютера, а друга – проникати в локальну мережу та використовувати спільні мережеві ресурси для розповсюдження. Вірус отримував доступ до комп'ютерів через оновлення M.E.Doc і поширювався далі у мережі, використовуючи логін та пароль адміністратора.

27 червня відбувся фінальний і найагресивніший етап кібератаки. Вірус почав перезаписувати диск на певних комп'ютерах, що призводило до шифрування системних та файлів користувачів, що мало безповоротні наслідки для цих систем.

Вірус NotPetya швидко поширювався серед українських компаній. Для того, щоб проникнути у внутрішню мережу одного з українських банків, йому знадобилося всього 45 секунд. Інший великий український транспортний хаб, який був використаний як демонстраційний об'єкт для обладнання ISSP, був заражений за 16 секунд. Такий спосіб атаки називається «атака на ланцюги поставок» (supply chain attack). Він дозволяє

провести масове зараження корпоративних мереж, не зламуючи кожну організацію окремо.

Одним з факторів, що призвів до широкого поширення вірусу, була відсутність програми M.E.Doc у списку перевірок брандмауерів та антивірусних програм. Тому трафік, пов'язаний з цією програмою, не перевірявся на наявність шкідливого коду. Це дало вірусу змогу обійти всі мережеві бар'єри.

Вірус NotPetya став однією з найбільш руйнівних кібератак в історії. Він завдав значних збитків українським приватним компаніям та державним установам, а також призвів до серйозних наслідків у сфері бухгалтерського обліку, фінансів, транспорту та енергетики.

Ось короткий перелік українських компаній, які постраждали від вірусу NotPetya: [27]

- 6 госпіталів у Києві;
- 6 енергетичних компаній;
- 2 аеропорти;
- 22 українські банки;
- понад 300 приватних компаній;
- 10% всіх комп'ютерів у країні.

Україна зазнала 75,24% від загальної кількості заражень по всьому світу [28]. На другому місці була Німеччина з 9,06%, далі Польща - з 5,81%, Сербії дісталось 2,87% атак, Греції - 1,39%, а Румунії - 1,02%. У росії та Чехії було лише 0,8% заражень (Рисунок 1.3.).

Рис. 1.3. Карта європейських країн, які постраждали від атаки NotPetya

1.3.3 Кібератаки на українські державні сайти

З 2021 по 2022 рр. росія атакувала понад 150 військових і державних сайтів (Рисунок 1.4.). Цілями були українські військові та дипломатичні організації, а також урядові установи, які керують критичною інфраструктурою, державними службами та управлінням у надзвичайних ситуаціях [29].

У 2022 році росія збільшила кількість атак на кінцевих користувачів в Україні на 250% порівняно з 2020 роком.

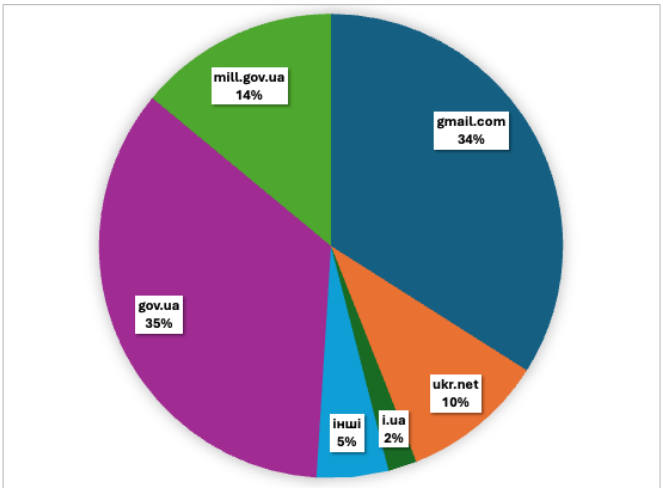


Рис. 1.4. Домени які стали цілями атак у 2021-2022 роках

У 2022 році українські сайти стали жертвами серії кібератак, які відбулися 14 січня, 15 та 16 лютого і 23 лютого. Перша атака сталася 14 січня 2022 року і була спрямована на близько 70 державних вебсайтів, що були побудовані на платформі CMS October від компанії Kitsoft [29].

Під час атак на сайти, здійснювалися заміни сайтів, так звані дефейси, та розміщувалися повідомлення українською, польською та російською мовами, що закликали до помсти українцям. У цих повідомленнях згадувалися події з української історії, такі як Волинська трагедія, ОУН-УПА та інші. Крім того, повідомлення містили дані про локацію, що вказували на Варшаву. Польща звинуватила росію у здійсненні цих кібератак. Атаки стали можливими через вразливість CMS October, яка була виявлена у травні 2021 року [29].

Друга атака сталася 15-16 лютого і цього разу були атаковані близько 15 банків, включаючи «ПриватБанк» та «Ощадбанк», а також сайти з доменом gov.ua. Деякі з цих сайтів тимчасово були недоступні, але завдяки допомозі США вдалося відбити атаку. Представники Великої Британії та США заявили, що росія несе відповідальність за ці атаки.

Третя атака сталася 23 лютого, за день до російського повномасштабного вторгнення. Під час цієї атаки були пошкоджені вебсайти Верховної Ради, Кабінету Міністрів України та Міністерства закордонних справ. Деякі інші вебсайти, такі як СБУ та Міністерства стратегічних галузей, також постраждали. На той момент не було точних відомостей про відповідальних за атаки, але попередні докази вказували на дії росії. Уряд росії відкидав будь-яку відповідальність.

Після DDoS атаки 23 лютого на сайтах почали діяти шкідливі програмні засоби під назвою HermeticWiper, які призначені для знищення інформації в базах даних. Цей вірус був виявлений близько 17:00 23 лютого, але його код був скомпільований ще 28 грудня 2021 року.

1.4 Аналіз сучасних стандартів аудиту з кібербезпеки

Щоб успішно досягати цілей впровадження кібербезпеки на різних рівнях, організаціям і ОКІ слід дотримуватися ряду процедур і стандартів. Стандарти аудиту з кібербезпеки визначають вимоги, яких має дотримуватися організація чи ОКІ, щоб досягти цілей кібербезпеки та сприяти боротьбі з кіберзлочинцями [5], а також забезпечити постійне управління засобами контролю інформаційної безпеки.

Крім того, ці стандарти встановлюють спільне розуміння для визначення програми кібербезпеки, що дозволяє організаціям та ОКІ встановлювати цілі кібербезпеки на основі оцінки ризиків на управлінському рівні організації і транслювати їх на виконавчі команди операційного рівня [30].

Таким чином, дані стандарти виступають так званим планом для управління та зниження рівня організаційних ризиків.

Фахівці з інформаційної безпеки використовують стандарти аудиту з кібербезпеки для визначення та пріоритезації завдань, необхідних для управління програмою безпеки організації. Стандарти також використовуються для підготовки до перевірок на відповідність та інших аудитів безпеки та IT інфраструктури.

Водночас, вибір необхідного та застосовного стандарту – зовсім нетривіальне завдання. Для вибору необхідного застосовного стандарту з числа провідних стандартів інформаційної безпеки, в першу чергу оцінюється кількість унікальних засобів контролю (вимог) інформаційної безпеки в кожному з них.

Обсяг цих вимог безпосередньо впливає на кількість доменів, охоплених цим стандартом. Менша кількість елементів керування або контролів в структурі стандарту може спростити впровадження, але також може не забезпечити необхідного охоплення, якого потребує організація чи

ОКІ з погляду адміністративних, технічних і фізичних методів захисту інформації [31].

Саме тут визначення застосовного та відповідного стандарту є перш за все бізнес-рішенням [32], заснованим на контексті організації та профілі ризику, яке потребує врахування чинних законів і нормативних актів, необхідних для підтримки існуючих або запланованих бізнес-процесів.

Як правило, цей процес відбору зазвичай призводить до вибору одного з наступних стандартів:

- ISO 27001/002 [33, 34]
- Спеціальна публікація NIST 800-53 [35]
- NIST Cybersecurity Framework [36]
- PCI DSS [37, 38]
- CIS Controls [39, 40]
- HITRUST [41]
- HIPAA [42]
- CSA CCM [43]
- GDPR [44]
- ISO 27701 [45]
- Trust Services Criteria from AICPA (SOC 2) [46]
- COBIT [47]

Кожен стандарт безпеки має свою унікальну спеціалізацію та ширину охоплення. Розуміння цього може допомогти прийняти обґрунтоване рішення щодо найкращого стандарту для задоволення організаційних потреб [48, 49]. Може навіть виявитись, що потребується використання метастандарту (наприклад, сукупності стандартів) для вирішення складніших вимог відповідності (наприклад, коли організація зберігає

персональні дані громадян ЄС і обробляє дані власників карток, вона повинна відповідати вимогам GDPR і PCI DSS).

Ключовим фактором для вибору стандарту кібербезпеки є розуміння рівня вмісту та покриття, які пропонує кожен стандарт. Це безпосередньо вплине на доступні засоби контролю інформаційної безпеки в кожному стандарті [50].

Нижче ми розглянемо декілька найпопулярніших і найпоширеніших у світі стандартів аудиту з кібербезпеки та дослідимо особливості їхнього впровадження.

1.4.1 Аналіз стандарту ISO 27001:2022

Стандарт ISO/IEC 27001 або просто ISO 27001 є міжнародним стандартом, що встановлює вимоги для систем управління інформаційною безпекою (СУІБ). Його метою є забезпечення конфіденційності, цілісності та доступності інформації, а також забезпечення захисту від загроз, таких як несанкціонований доступ чи руйнування або втрата даних. На сьогодні цей стандарт є одним з найпопулярніших стандартів інформаційної безпеки в світі.

Основна мета застосування стандарту ISO 27001 полягає у розробці, впровадженні та підтриманні ефективної системи управління інформаційною безпекою в організації. Цей стандарт надає рекомендації, що допомагають організаціям виявити, оцінити та керувати ризиками, пов'язаними з інформаційною безпекою. Він розглядає широкий спектр засобів і контролів, включаючи політику безпеки, управління ризиками інформаційної безпеки, безпеку фізичного середовища, управління персоналом, управління вразливостями, безпеку доступу до інформації, управління інцидентами, забезпечення безперервності інформаційної безпеки та ін.

Основні етапи впровадження ISO 27001 включають визначення області застосування, ідентифікацію активів та ризиків, визначення політики інформаційної безпеки, розробку процедур та контрольних механізмів, навчання персоналу та аудит системи. Стандарт також передбачає необхідність постійного моніторингу та вдосконалення системи управління інформаційною безпекою з метою забезпечення високого рівня інформаційної безпеки в організації [51-53].

ISO 27001 є гнучким стандартом, який може бути застосований до будь-якої організації чи ОКІ, незалежно від її розміру або сфери діяльності. Впровадження цього стандарту допомагає забезпечувати конфіденційність, цілісність та доступність інформації, а також зменшувати ризики, пов'язані з безпекою даних [54].

Нижче описана структура стандарту ISO/IEC 27001 від 2022 року. Перші три розділи або пункти стандарту визначають його сферу застосування, нормативні посилання та терміни і визначення, що зустрічаються в ньому. Ці три пункти не містять вимог. Фактичні вимоги до СУІБ містяться в пунктах 4–10, їх і розглянемо детальніше.

- **Пункт 4 – Контекст організації (Context of the organisation) –** розуміння організаційного контексту, потреб і очікувань зацікавлених сторін і визначення сфери застосування СУІБ. У розділі 4.4 зазначено, що «Організація повинна створити, запровадити, підтримувати та постійно вдосконалювати» СУІБ, тобто вона має бути працездатною, постійно переглядатися і вдосконалюватися, а не тільки бути розробленою та задокументованою [55].

Організація повинна визначити внутрішні та зовнішні проблеми, які мають відношення до мети та впливають на її здатність досягти запланованих бізнес цілей чи результатів її системи управління інформаційною безпекою. Це виконується для того, щоб досягти наступних

цілей: адаптувати СУІБ до контексту організації, визначити сферу застосування СУІБ і дати змогу організації визначити ризики та можливості, які можуть бути пов’язані між собою в залежності від її контексту.

Стандарт також акцентує увагу на визначенні зацікавлених сторін та їхніх вимог до СУІБ. Термін «зацікавлена сторона» стосується осіб або організацій, які можуть впливати на рішення чи дії щодо впровадження і підтримки СУІБ. Зацікавленими сторонами є не тільки клієнти організації або користувачі її продуктів і послуг. Ними можуть бути також власники компанії та інвестори, працівники компанії, підрядники, державні установи і регулятори тощо. Деякі вимоги зацікавлених сторін є обов’язковими, оскільки вони випливають із законів чи нормативних актів і стосуються діяльності організації (наприклад, регулярне звітування перед регуляторними органами). Інші вимоги можуть бути прийняті добровільно, наприклад, договірні зобов’язання з клієнтами чи постачальниками [56].

- **Пункт 5 – Лідерство (Leadership) –** вище керівництво має продемонструвати лідерство та відданість СУІБ, визначити політику та призначити ролі, обов’язки та повноваження щодо інформаційної безпеки. Створення та впровадження системи управління інформаційною безпекою в організації є проектом, який може охоплювати всю компанію. Тому без підтримки вищого керівництва ймовірність успіху такого проекту дуже низька. Для успішного впровадження та ефективного функціонування СУІБ необхідні ресурси, такі як компетентні кадри для управління, фінансові засоби, технічна підтримка тощо. Вище керівництво повинно пояснити необхідність заходів з інформаційної безпеки та важливість дотримання стандартів СУІБ всім працівникам організації. Загальна відповідальність за СУІБ лежить на вищому керівництві [57].

Обов’язки і повноваження також мають бути відповідним чином донесені до відома персоналу, а не просто призначені. Повинен бути

офіційний розподіл обов'язків і повноважень. У разі проведення аудиту СУІБ, швидше за все, організації доведеться документально підтверджувати, що вона призначила керівних осіб СУІБ [58].

- **Пункт 6 – Планування (Planning) –** описує процес виявлення, аналізу та планування усунення ризиків інформаційної безпеки, уточнення цілей інформаційної безпеки та управління змінами СУІБ.

Отже, ISO 27001 говорить, що організація повинна розглядати внутрішні та зовнішні питання як частину свого контексту та вимоги зацікавлених сторін при визначенні тих ризиків, які пов'язані із СУІБ.

Ризики інформаційної безпеки зазвичай пов'язані із можливістю того, що загрози будуть використовувати вразливі місця інформаційного активу або групи активів і завдати шкоди організації.

Ризик зазвичай виражається в термінах ймовірності виникнення і наслідків або впливу події.

Стандарт вимагає, щоб була доступна документована інформація про цілі інформаційної безпеки та про плани їх досягнення [59-60].

- **Пункт 7 – Підтримка (Support) –** Організація повинна визначити та забезпечити ресурси, необхідні для створення, впровадження, підтримки та постійного вдосконалення СУІБ. Ресурси є засадничими для здійснення будь-якої діяльності та будь-якого проекту організації [61].

Також організація повинна визначити вимоги до компетентності осіб, відповідальних за роботу СУІБ. Ці вимоги, в ідеалі, повинні бути також задокументовані у посадових інструкціях або подібних документах. Після визначення вимог до компетенції наступним кроком буде гарантування того, що особи є компетентними на основі їхньої освіти, підготовки та досвіду. Щоразу, коли існує розрив між існуючою та необхідною компетенціями, організації потрібно впровадити заходи, такі як навчання чи наставництво

або найм зовнішніх кваліфікованих кадрі, для отримання необхідних компетенцій [62].

Відповідно до стандарту ISO 27001, організація зобов'язана забезпечити, щоб особи, які працюють під її контролем були обізнані про політику інформаційної безпеки та про свій внесок в ефективність СУІБ. Люди повинні знати, чого від них очікують щодо інформаційної безпеки і що робити, чого не робити і як поводитися в різних обставинах [63].

Також, ISO 27001 визначає, що організація повинна визначити потребу у внутрішніх і зовнішніх комунікаціях, які стосуються інформаційної безпеки. Стандарт вимагає, щоб організація визначала, про що вона буде повідомляти [64].

- **Пункт 8** – **Функціонування (Operation) –** описує вимоги щодо оцінки та усунення ризиків інформаційної безпеки, керування змінами та документування інформації (частково для того, щоб їх могли перевірити аудитори під час сертифікаційного аудиту) [65].

Оцінка та усунення ризиків є ключовими елементами будь-якої системи управління інформаційною безпекою, і оскільки речі змінюються та розвиваються в кожній організації, важливо застосовувати оцінку ризиків і усунення на регулярній основі та коли в цьому є потреба [66].

- **Пункт 9 – Оцінка ефективності (Performance evaluation) –** визначає вимоги щодо моніторингу, вимірювання, аналізу та оцінки/аудиту контролів, процесів і СУІБ загалом, з метою систематичного вдосконалення.

Щоб мати уявлення про ситуацію, організація повинна контролювати та вимірювати свої процеси інформаційної безпеки та наявні контролі, аналізувати отримані дані та оцінювати їх ефективність [67].

Одним з методів такої оцінки є проведення внутрішнього аудиту. Внутрішній аудит – це інструмент, який організація використовує для оцінки стану своєї СУІБ. Аудитори можуть бути зсередини організації або

зовнішніми аудиторами. Але дуже важливо, щоб вони були компетентними, об’єктивними та неупередженими у своїй оцінці. Це означає, що аудитори не повинні перевіряти свою власну роботу чи діяльність, у якій вони зацікавлені [68].

- **Пункт 10 – Удосконалення (Improvement) –** цей пункт вказує на важливість постійного удосконалення системи управління інформаційною безпекою. Це необхідно для того, щоб система була не лише придатною і адекватною, але й ефективною в забезпеченні безпеки інформації. Удосконалення може включати в себе постійний моніторинг стану безпеки, аналіз потенційних загроз і вразливостей, впровадження нових технологій та методів захисту, а також постійне навчання персоналу з питань інформаційної безпеки. Цей підхід допомагає забезпечити, що система управління інформаційною безпекою залишається актуальною і ефективною в умовах змінного середовища загроз і технологій [69-70].
- **Додаток А – Посилання на контролі інформаційної безпеки –** назви засобів контролю, задокументованих у ISO/IEC 27002:2022. Додаток є «нормативним», що означає, що сертифіковані організації повинні використовувати його для перевірки своєї СУІБ на повноту (відповідно до пункту 6.2), але це не означає, що вони зобов’язані впроваджувати усі засоби контролю; з огляду на їхні особливі ризики, вони можуть віддати перевагу іншим контролям безпеки.

1.4.2 Аналіз стандарту NIST SP 800-53

Спеціальна публікація (Special Publication – SP) 800-53 «Контролі безпеки та конфіденційності для інформаційних систем і організацій» (Security and Privacy Controls for Information Systems and Organizations) від Національного інституту стандартів і технологій (National Institute of Standards and Technology – NIST) наразі перебуває у 5-ій редакції, датованій

вереснем 2020 року. Спочатку вона була розроблена для захисту федеральних установ США, але швидко набула популярності серед приватного сектору і зараз вважається одним з найпопулярніших стандартів інформаційної безпеки у світі. Частково це було спричинено значним аутсорсингом приватним компаніям, які ведуть справи з федеральним урядом США [71].

NIST SP 800-53 містить каталог контролів для забезпечення безпеки та конфіденційності (privacy) для інформаційних систем і організацій з метою захисту організаційних операцій і активів, окремих осіб, інших організацій і країни від різноманітних загроз і ризиків, зокрема ворожих атак, людських помилок, стихійних лих, структурних збоїв, іноземних розвідувальних організацій та ризиків конфіденційності [72].

У стандарті використовується багаторівневий підхід до управління ризиками через відповідність контролю. Контроль поділяється на три класи: низький (low), середній (moderate) і високий (high) і базується на впливі. Всі контролі розділені на 18 сімейств, що дозволяє організаціям вибирати лише ті, які найбільше відповідають їхнім вимогам. NIST SP 800-53 вводить концепцію базового рівня (baseline) як відправної точки для процесу вибору контролів. Це дає змогу організаціям створити основу для розробки безпечної організаційної інфраструктури [35].

Опис кожного контролю підпорядкований визначеному шаблону. Перш за все зазначено код сімейства контролів та його номер, наприклад, AU-2. Далі вказано його назву.

Основна частина стандарту складається з наступних розділів [35]:

- **Контроль (Control):** Опис специфічних дій або активностей, які виконуються організацією або інформаційною системою та мають відношення до забезпечення безпеки. Для певних контролів передбачено

можливість гнучкого налаштування, яке надає можливість для організацій визначати окремі з параметрів, пов'язаних з контролем [35]. Для прикладу, в ролі такого параметра може бути частота проведення аудитів або тривалість зберігання журналу подій. Це дозволяє підлаштовувати контролі під потреби конкретної організації, спираючись на вимоги, запропоновані для забезпечення безпеки зі сторони цілей поставлених організацією та результатів оцінок рівня ризику та його прийнятності.

- **Супроводжуючі відомості (Supplemental Guidance):** Додаткові відомості для певного контролю. Включає в себе роз'яснювальну інформацію стосовно впровадження та використання контролю.
- **Покращення контролю (Control Enhancements):** Дана секція визначає можливості для «покращення» контролів, додаючи до них додаткову функціональність.
- **Довідкові матеріали (References):** Включає в себе посилання на закони, нормативні акти тощо.
- **Пріоритетність і базовий набір (Priority and Baseline Allocation):** Має вигляд таблиці, в якій зведено інформацію щодо рекомендованого пріоритету в ході прийняття рішень про реалізацію контролів і стартовий розподіл контролів серед базових наборів для систем з різними рівнями критичності. Пріоритезація впровадження дає змогу організаціям проводити реалізацію контролів ефективніше та в правильній послідовності, спочатку впроваджуючи найкритичніші заходи.

Для впорядкування та забезпечення структурності підходу проведено розподіл контролів за різними типами. Він залежить від призначення контролю:

- **Загальний (Common):** Загальні контролі, що можуть бути реалізовані в різноманітних системах і можуть бути використані поза

межами окремої інформаційної системи.

- **Специфічний для системи (System-specific):** Контроль створено для реалізації а конкретній специфічній інформаційній системі.
- **Гібридний (Hybrid):** Контроль функціонує частково як загальний і частково як специфічний для системи.

Загалом цей стандарт є дуже детальним і при умові дотримання хоча б мінімальних елементів керування, які він окреслює, охоплюється більшість факторів ризику, з якими стикаються організації.

Це також забезпечує базову лінію для вдосконалення. При кращому розумінні конкретних потреб організації можна переглянути налаштування інфраструктури та визначити, які конкретні контролі можна покращити та в які варто інвестувати.

1.4.3 Аналіз TSC від AICPA (SOC 2)

SOC 2 (Service Organization Control 2) – це стандарт безпеки, розроблений Американським Інститутом Дипломованих Бухгалтерів (American Institute of Certified Public Accountants, AICPA), який визначає вимоги до систем управління інформаційною безпекою для організацій, які надають послуги в сфері технологій та обробки даних, таких як хмарні сервіси, хмарне зберігання, системи управління відносинами з клієнтами (CRM) та інші подібні послуги. SOC 2 гарантує, що постачальник послуг безпечно управляє даними для захисту інтересів організації та конфіденційності її клієнтів. Для підприємств, які піклуються про безпеку, відповідність SOC 2 є мінімальною вимогою при розгляді постачальника SaaS [73].

SOC 2 базується на п'яти «Trust Service Criteria» (критерії надійності служб) (Рисунок 1.5), а саме [74]:

- **Безпека (Security):** Організація має захищати системи та дані від несанкціонованого доступу, несанкціонованих подій та інших загроз.
- **Доступність (Availability):** Системи повинні бути доступні для операцій та функцій відповідно до угоди про рівень обслуговування (SLA).
- **Цілісність обробки (Processing Integrity):** Системи мають забезпечувати точність та цілісність обробки даних.
- **Конфіденційність (Confidentiality):** Інформація повинна залишатися конфіденційною, як передбачено договором або угодою.
- **Приватність (Privacy):** Збір, використання, розкриття та управління персональною інформацією повинні відбуватися відповідно до визначених політик та процедур.

Рис. 1.5. П’ять критеріїв (принципів) надійності SOC 2

Здобуття сертифіката SOC 2 вказує на те, що організація відповідає високим стандартам інформаційної безпеки та може довести свою здатність ефективно управляти та захищати дані своїх клієнтів [75].

1.4.4 Аналіз стандарту PCI DSS v.4.0

Будь-яка організація, яка приймає платіжні картки, повинна дотримуватися стандарту PCI DSS відповідно до вимог компаній, що видають кредитні картки. Це міжнародний стандарт, а не національне регулювання. Цей стандарт є досить вичерпним, технічним та детальним і вважається достатньо самостійним для забезпечення кібербезпеки [76].

PCI DSS (Payment Card Industry Data Security Standard, у перекладі з англ. «стандарт безпеки індустрії платіжних карток») – стандарт зі сфери кібербезпеки, спрямований на захист даних власників карток при їх зберіганні, обробці або передачі. Він був розроблений у грудні 2004 року при участі п’яти транснаціональних корпорацій у сфері платіжних карт: Visa, MasterCard, American Express, Discover Financial Services та JCB International.

Кожна із корпорацій мала на меті створити мінімальний рівень захисту для даних власників карток при їх зберіганні, обробці або передачі шляхом поєднання напрацювань кожної зі сторін [77].

Стандарт PCI DSS передбачає декілька умовних рівнів, на які поділяються компанії, що підпадають під дію стандарту. Відповідно від рівня відповідності визначається які саме звітні документи необхідно заповнити QSA (аудитору) для PCI DSS сертифікації компанії.

Рівні поділяються за кількістю транзакцій щорічно наступним чином:

- Рівень 1 – більше 6-ти мільйонів транзакцій щорічно;
- Рівень 2 – від 1-го до 6-ти мільйонів транзакцій щорічно;
- Рівень 3 – від 20 000 до 1-го мільйона транзакцій щорічно;
- Рівень 4 – менше 20 000 транзакцій щорічно.

Стандарт PCI DSS застосовується для всіх організацій, залучених в обробку платіжних карток: провайдерів сервісів, процесингових центрів,

еквaєрів, емітентів та постачальників послуг, а також будь-яких інших організацій, які зберігають, обробляють або передають [78]:

- дані власників карток: номер картки (PAN), ім’я власника картки, дата завершення терміну роботи картки, сервісний код та/або
- критичні автентифікаційні дані: повні дані треку (дані магнітної смуги картки або чіпа), CAV2/CVC2/CVV2/CID, PIN-коди та/або PIN-блоки.

Подібно до стандарту ISO 27001, PCI DSS також розвивається, щоб не відставати від стану електронної комерції та більш складних кіберзагроз і у 2022 році отримав значне оновлення. Нова версія стандарту – PCI DSS v.4.0 – була випущена 31 березня 2022 року.

PCI DSS v.4.0 є останньою значною ітерацією галузевого стандарту платіжних карток, який впроваджує значні зміни у вимогах, зосереджуючись більше на підтримці безперервної безпеки, а також додаючи нові методи для задоволення вимог стандарту [79].

Основною метою PCI DSS v.4.0 є продовження розвитку стандарту для задоволення мінливих потреб індустрії платіжних карток і нових технологій, які впроваджуються щодня.

PCI DSS v.4.0 містить ряд змін, спрямованих на досягнення чотирьох ключових цілей [80]:

- продовження задоволення потреб платіжної індустрії;
- сприяння забезпеченню безпеки як безперервного процесу;
- додавання гнучкості та додаткових методів для підтримки безпеки платежів;
- вдосконалення методів і процедур підтвердження платежів.

У Додатку Б наведено таблицю із описом огляд цих змін у порівнянні з попередньою версію PCI DSS 3.2.1.

Загалом, PCI DSS став помітно об’ємнішим. На відміну від попередньої версії стандарту PCI DSS v.3.2.1, кількість сторінок в документі збільшилася з 180 до 360. Потрібно також відзначити вищий рівень деталізації в новій версії, більше уваги приділено ризик-орієнтованому підходу, категоризації вимог та даних. Також додано цілу низку нових вимог та контролів безпеки [81].

1.5 Аналіз проблем впровадження стандартів аудиту з кібербезпеки

Управління інформаційною безпекою в організації може бути складним завданням, особливо враховуючи, що воно може охоплювати багато сфер, від фізичної та мережевої безпеки до безпеки людських ресурсів і управління постачальниками [2]. Це може бути особливо важко для молодих або недостатньо досвідчених спеціалістів, які можуть упустити деякі важливі напрямки через брак практичного досвіду. Саме тут стають у нагоді стандарти інформаційної безпеки, які додають формальності процесу розробки та реалізації стратегії безпеки.

За умови використання стандарта інформаційної безпеки стає набагато простіше визначити процеси та процедури, які організація повинна застосовувати для оцінки, моніторингу та пом’якшення ризиків кібербезпеки і застосування належних засобів контролю для захисту цінної інформації.

Але інша проблема виникає, коли потрібно вибрати оптимальний стандарт для організації, враховуючи більш специфічні характеристики бізнесу, як-от контекст організації, область діяльності, чинні закони, нормативні акти та договірні зобов’язання, а також інші чинники, такі як зрілість стандарту, всебічність або популярність.

Ще одним важливим фактором є обмеженість конкретного стандарту і відсутність деяких специфічних і важливих для організації контролів. Така проблема може виникнути через певний рівень узагальненості стандарту. Розглянемо для прикладу стандарт ISO 27001. Контролі безпеки в ньому містять досить узагальнюючий і універсальний характер, і більше задають певні рамки ніж фактичні строгі вимоги до безпеки. Це, з одного боку, дозволяє застосовувати його для дуже широкого кола організацій, але з іншого, створює ризик ситуації, коли вимоги безпеки задовольняються поверхнево. Тобто, фактично організація відповідає вимогам стандарту, але застосовні контролі безпеки недостатні для ефективної протидії кіберзагрозам.

У цьому випадку дуже важливими є кваліфікація персоналу, який займається впровадженням стандарту, їхня обізнаність із найкращими практиками безпеки, а також усвідомленість керівництва організації про ризики, які можуть виникнути при недостатньому або поверхневому захисті від загроз.

Але що робити, якщо такої експертизи і розуміння в компанії немає? Часто для вирішення цього питання, організації звертаються за допомогою до спеціалізованих компаній по забезпеченню інформаційної безпеки і впровадженню стандартів інформаційної безпеки. Залучення зовнішніх експертів може значно полегшити процес впровадження системи управління інформаційною безпекою та дозволити організації ефективно впоратися з викликами в цій області, забезпечивши найвищий рівень захисту інформації.

Проте навіть із залученням зовнішніх експертів, залишається проблема застосовності контролів і покриття релевантних доменів беручи до уваги контекст організації. Також надважливим завданням є вибір необхідного стандарту інформаційної безпеки для впровадження в організації, беручи до

уваги контекст, сферу діяльності, типи даних які обробляються в організації та застосовні нормативно-правові документи.

1.6 Порівняльна характеристика основних стандартів аудиту з кібербезпеки з погляду ширини покриття

Який зі стандартів інформаційної безпеки найкраще відповідає поставленим вимогам? Перш за все, концепція «найкращого» стандарту інформаційної безпеки є помилковою, оскільки вибір найбільш відповідного стандарту значною мірою залежить від організаційної бізнес-моделі [5]. Застосовні до організації закони, нормативні акти та договірні зобов'язання найчастіше вкажуть на доволі сталий перелік провідних стандартів аудиту з кібербезпеки [82].

Коли графічно зобразити різноманітні провідні стандарти інформаційної безпеки від «простішого до складнішого» (Рисунок 1.6), в першу чергу потрібно зосередити увагу на кількості унікальних контролів безпеки. Обсяг цих контролів (вимог) безпосередньо впливає на кількість доменів, охоплених цим стандартом. Стандарт із меншою кількістю контролів може здатися легшим для впровадження, але він також може не забезпечити необхідного покриття, якого потребує організація з погляду адміністративних, технічних та фізичних засобів забезпечення захисту інформації [4]. Визначення «правильного» стандарту для організації – це перш за все бізнес-рішення, засноване на розумінні контексту організації та профілю ризику, яке повинно враховувати чинні закони, нормативні акти та договірні зобов'язання, необхідні для підтримки існуючих або запланованих бізнес-процесів [5].

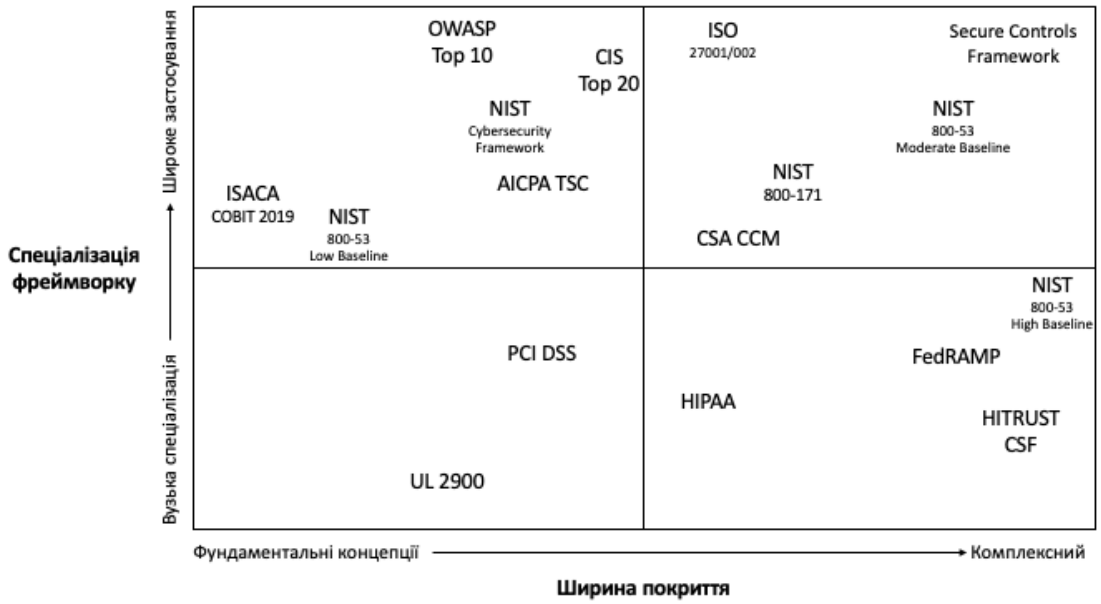


Рис. 1.6. Класифікація стандартів кібербезпеки на основі їхнього покриття і спеціалізації

Дуже важливим аспектом при виборі стандарта є необхідність його налаштування чи адаптації. Малоймовірно, що окремий стандарт ідеально відповідатиме визначеним потребам, тому доведеться розраховувати на адаптацію стандарту до конкретних потреб організації (наприклад, додавання до нього відсутніх контролів чи об’єднання декількох стандартів одночасно).

Не всі стандарти інформаційної безпеки однакові, і це цілком нормально. Причому нерідко досвідчені фахівці з кібербезпеки мають фундаментальне нерозуміння відмінностей між законами та стандартами.

Також, кожен стандарт кібербезпеки має власну унікальну сферу застосування (спеціалізацію) і глибину охоплення. Однак розуміння класифікації складності може допомогти організаціям прийняти обґрунтоване рішення про те, з чого почати роботу і який зі стандартів може стати найбільш відповідним до її потреб (проте часто організації використовують більше ніж один стандарт) [3]. У процесі роботи,

організації можуть виявити що їм потрібен метастандарт (сукупність стандартів), щоб відповідати складнішим вимогам відповідності і безпеки.

1.7 Висновки до першого розділу

У першому розділі дисертації проведено аналіз наукової літератури за темою дисертації, зокрема, проаналізовано останні атаки на ОКІ України та підходи до забезпечення їхнього захисту, обґрунтовано необхідність використання стандартів аудиту з кібербезпеки для успішної протидії кібератакам і створення ефективної та всебічної системи захисту, визначено проблематику дослідження та подальші кроки виконання дисертаційної роботи.

Проведене дослідження дозволяє виділити наступне:

1. Проведений аналіз кібератак на ОКІ, демонструє важливість належного захисту ОКІ у зв'язку зі стрімким розвитком інформаційних технологій, масовим переходом до режиму віддаленої роботи та збройною військовою агресією росії проти України. Виявлено, що багато атак було успішно реалізовано через відсутність базових процесів інформаційної безпеки, таких як управління інформаційною безпекою у відносинах з постачальниками, систематичне оновлення програмного забезпечення та недостатній рівень обізнаності щодо інформаційної безпеки серед персоналу. Зазначені процеси регулюються провідними стандартами аудиту з кібербезпеки, такими як ISO 27001, SOC 2, NIST 800-53 та PCI DSS. Відповідно, впровадження цих стандартів аудиту здатне значно зменшити ризики та втрати внаслідок кібератак, оскільки надають спільне розуміння для розробки програми кібербезпеки та пропонують організаціям структурований підхід до впровадження політик, процедур та технологій, спрямованих на забезпечення безпеки.

2. Аналіз сучасних підходів до захисту ОКІ визначив важливість і ефективність використання встановлених вимог і практик у формі стандартів аудиту з кібербезпеки. Стандарти, що встановлюють спільне розуміння для визначення програми кібербезпеки, сприяють уніфікації підходів до її забезпечення, забезпечують охоплення усіх важливих аспектів безпеки, і надають організаціям і ОКІ рекомендації та структурований підхід до розробки та впровадження необхідних політик, процедур та технологій.

3. На основі проведених досліджень особливостей застосування і впровадження провідних стандартів аудиту з кібербезпеки, таких як ISO 27001, SOC 2, NIST 800-53 і PCI DSS, доведено доцільність і ефективність застосування перехресного впровадження стандартів аудиту з кібербезпеки, що дозволить забезпечити повне охоплення контролів безпеки та підвищити рівень захисту організації порівняно з будь-яким окремим стандартом.

4. Дослідження проблем впровадження стандартів аудиту з кібербезпеки дозволило визначити, що управління інформаційною безпекою в сучасних організаціях і ОКІ є складним завданням, яке охоплює різні сфери від фізичної та мережевої безпеки до управління постачальниками. Проте, використання стандартів аудиту з кібербезпеки суттєво спрощує цей процес, дозволяючи систематизувати процеси та процедури оцінки, моніторингу та зниження ризиків кібербезпеки.

РОЗДІЛ 2. ОБҐРУНТУВАННЯ МЕТОДОЛОГІЇ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ ДЕКІЛЬКОХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Дослідження і зіставлення контролів редакцій стандарту ISO 27001 2013 і 2022 року

2.1.1 Виявлення основних критеріїв і особливостей стандарту ISO 27001:2022

ISO/IEC 27001:2022 – це стандарт розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародним електротехнічним комітетом (IEC), який встановлює вимоги до створення, впровадження, управління та постійного вдосконалення системи управління інформаційною безпекою в організаціях.

ISO 27001 встановлює широкий набір вимог, які дозволяють організаціям будувати ефективні системи управління інформаційною безпекою та забезпечувати захист конфіденційності, цілісності та доступності інформації.

Важливо відзначити, що нова версія 2022 року використовується переважно у комерційних організаціях і об'єктах приватної власності, тоді як державні установи і ОКІ здебільшого користуються ДСТУ ISO/IEC 27001:2015, який відповідає версії ISO 27001:2013. Проте, оскільки практики інформаційної безпеки постійно оновлюються, це лише питання часу, коли нова версія стандарту буде ратифікована і почне використовуватися для захисту державних підприємств і ОКІ. Відповідно, перед цими організаціями постане проблема ефективного приведення своїх процесів і практик, пов'язаних з інформаційною безпекою, до відповідності новій редакції стандарту.

З метою подальшої розробки методології перехресного впровадження стандартів аудиту з кібербезпеки, важливо дослідити і виявити основні критерії і особливості даного стандарту, оскільки він виступає як базис для побудови процесу оцінки на відповідність і зіставлення контролів стандартів.

Стандарт ISO/IEC 27001:2022 включає наступні елементи [83]:

1. **Визначення контексту організації:** Організація визначає свої цілі, перелік зацікавлених сторін та внутрішні та зовнішні фактори, що впливають на її інформаційну безпеку.

2. **Проведення оцінки на відповідність:** Організація проводить аудит і аналіз того, наскільки поточний стан політик, контролів та процесів відповідає вимогам, які встановлює стандарт.

3. **Управління ризиками:** Визначення і оцінка ризиків інформаційної безпеки, розроблення та впровадження відповідних контролів для зменшення ризиків до прийнятного рівня.

4. **Створення та управління документацією:** Розроблення та зберігання політик, процедур, інструкцій, планів та іншої документації, необхідної для ефективного управління інформаційною безпекою.

5. **Залученість керівництва:** Залучення керівництва організації до підтримки та сприяння у впровадженні системи управління інформаційною безпекою.

6. **Впровадження контролів:** Впровадження контролів інформаційної безпеки є ключовою складовою частиною системи управління інформаційною безпекою. Ці контролі призначені для захисту інформації від різних загроз, забезпечення конфіденційності, цілісності та доступності даних, а також забезпечення відповідності вимогам щодо безпеки інформації.

7. **Постійне вдосконалення:** Впровадження механізмів для постійного оновлення та вдосконалення системи управління інформаційною безпекою на основі результатів аналізу, аудитів та оцінки ризиків.

8. **Навчання у сфері інформаційної безпеки:** Забезпечення навчання та підвищення свідомості персоналу щодо інформаційної безпеки, включаючи визначення ролей і відповідальностей, навчання щодо безпечних практик та свідомого використання інформаційних ресурсів.

9. **Внутрішній аудит:** Здійснення внутрішніх та зовнішніх аудитів для перевірки відповідності системи управління інформаційною безпекою вимогам стандарту та ідентифікації можливих відхилень, невідповідностей та рекомендацій по покращенню.

10. **Аналіз з боку керівництва та впровадження коригувальних дій:** Впровадження процедур для виявлення та обробки відхилень, включаючи запровадження коригуючих та запобіжних заходів для запобігання подібним проблемам у майбутньому.

11. **Сертифікаційний аудит:** Сертифікаційний аудит є фінальним етапом процесу впровадження системи управління інформаційною безпекою згідно зі стандартом ISO 27001. Цей аудит проводиться зовнішнім незалежним сертифікаційним органом, що має відповідну акредитацію, і має на меті оцінку та підтвердження відповідності організації вимогам стандарту і встановленим політикам та процедурам захисту інформації.

Головна мета стандарту ISO 27001 полягає в тому, щоб організації розробляли, впроваджували та підтримували систему управління інформаційною безпекою, що відповідає вимогам стандарту. Це дозволяє організаціям ефективно виявляти, оцінювати та зменшувати ризики безпеки інформації, забезпечувати відповідність законодавству та регуляторним вимогам, а також підвищувати довіру клієнтів, постачальників та інших зацікавлених сторін [84].

Отже, стандарт ISO 27001 визначає ключові пункти та зміст, що необхідні для впровадження ефективної системи управління інформаційною безпекою в об'єктах критичної інфраструктури.

2.1.2 Визначення відмінностей між редакціями стандарту ISO/IEC 27001 2013 та 2022 років

Через дев’ять років після публікації ISO 27001:2013, провідний світовий стандарт інформаційної безпеки було оновлено – 25 жовтня 2022 року було опубліковано новий стандарт ISO/IEC 27001:2022.

Для успішного впровадження оновленої версії стандарту в організації і ОКІ, і що важливіше, для ефективного і якісного процесу переходу зі старої редакції стандарту на оновлену версію необхідно визначити ключові відмінності між даними редакціями і встановити відповідність між контролями безпеки в Додатку А.

Більшість змін в стандарті є редакційними, наприклад, зміна формулювання «міжнародний стандарт» на «документ» та зміна чи ре-організація порядку фраз, щоб забезпечити кращий міжнародний переклад [85].

Також були зроблені зміни для узгодження з принципом гармонізації (англ. harmonized) який пропагує ISO.

Ось ключові зміни оновленого стандарту ISO/IEC 27001:2022 [85]:

- Назву стандарту було змінено відповідно до ISO/IEC 27002:2022. Нова назва ISO/IEC 27001:2022 – Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги;
- Назва Додатку А також змінилася з Довідкові цілі контролів та контролі (Reference control objectives and controls) на Довідка про контролі інформаційної безпеки (Information security controls reference);

- Додаток А зіставляється з контролями зі стандарту ISO 27002:2022. Новий Додаток А тепер містить 93 контролі та включає таку інформацію як назва контролю і безпосередньо опис самого контролю;
- Присутні незначні зміни у використовуваній термінології, формулюваннях і структурі в пунктах 4-10, зокрема в пунктах 4.2, 6.2, 6.3 і 8.1;
- У пункті 6.1.3 c) було переглянуто і змінено примітки. Слово «контроль» було замінено на «контроль інформаційної безпеки», а цілі контролю вилучено;
- У пункті 6.1.3 d) було змінено формулювання для уникнення двозначності;
- Додано вимогу щодо визначення процесів, необхідних для впровадження системи управління інформаційною безпекою, та їх взаємодії;
- Додано вимогу повідомляти зацікавленим сторонам про організаційні ролі, що стосуються інформаційної безпеки в організації;
- Додано новий пункт 6.3 – Планування змін;
- Додано нову вимогу щодо того, щоб організація вирішила, як повідомляти важливу інформацію (частина пункту 7.4);
- Додано нові вимоги щодо встановлення критеріїв операційних процесів та здійснення їх контролю.

Основні зміни, однак, стосуються оновлень поточних контролів в Додатку А, щоб краще узгодити стандарт із нещодавніми змінами до ISO/IEC 27002 – Інформаційна безпека, кібербезпека та захист конфіденційності [86].

Додаток А стандарту ISO/IEC 27001:2022 містить зміни як у кількості контролів, так і в їх переліку в групах. Кількість контролів в Додатку А

зменшилася зі 114 до 93. Зменшення кількості контролів здебільшого відбулося внаслідок об’єднання багатьох із них [87]:

- 35 контролів залишилися незмінними зі зміною контрольного номера та реорганізацією на 4 секції;
- Додано 11 нових контролів;
- 23 контролі перейменовано для кращого розуміння;
- Незважаючи на те, що кількість контролів було зменшено (зі 114 до 93), ні одного контролю не було виключено;
- 57 контролів було об’єднано в 24 контролі;
- 1 контроль було розділено. Контроль 18.2.3 Огляд технічної відповідності було розділено на:
  - 5.3.6 – Відповідність політикам, правилам і стандартам інформаційної безпеки;
  - 8.8 – Управління технічними вразливостями.

Загалом, 93 контролі були реорганізовані в чотири групи або секції.

- A.5 Організаційні контролі (Organizational controls) – містить 37 контролів;
- A.6 Контролі направлені на людей (People controls) – містить 8 контролів;
- A.7 Фізичні контролі (Physical controls) – містить 14 контролів;
- A.8 Технологічні контролі (Technological controls) – містить 34 контролі.

ISO/IEC 27001:2022 також додав 11 нових контролів до Додатку А:

1. Дані про кіберзагрози (Threat intelligence);
2. Інформаційна безпека при використанні хмарних сервісів (Information security for the use of cloud services);

3. Готовність (підготовка) інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу (ICT readiness for business continuity);

4. Моніторинг фізичної безпеки (Physical security monitoring);

5. Управління налаштуваннями (Configuration management);

6. Видалення інформації (Information deletion);

7. Маскування даних (Data masking);

8. Запобігання витокам даних (Data leakage prevention);

9. Моніторингова діяльність / Діяльність по моніторингу (Monitoring activities);

10. Веб-фільтрація (Web filtering);

11. Безпечне кодування (Secure coding).

У таблиці 2.1 наведено зіставлення контролів з додатку А двох версій стандарту.

Таблиця 2.1

Зіставлення контролів додатку А стандартів ISO 27001 2013 і ISO 27001:2022

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.5 – Організаційні контролі		
A.5.1	A.5.1.1, A.5.1.2	Політики інформаційної безпеки
A.5.2	A.6.1.1	Ролі та обов'язки з інформаційної безпеки
A.5.3	A.6.1.2	Розподіл обов'язків
A.5.4	A.7.2.1	Обов'язки керівництва

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.5.5	A.6.1.3	Контакти з органами влади
A.5.6	A.6.1.4	Контакти з групами за інтересами
A.5.7	Новий	Інформація про загрози
A.5.8	A.6.1.5, A.14.1.1	Інформаційна безпека в управлінні проєктами
A.5.9	A.8.1.1, A.8.1.2	Інвентаризація інформації та інших пов’язаних активів
A.5.10	A.8.1.3, A.8.2.3	Прийнятне використання інформації та інших пов’язаних активів
A.5.11	A.8.1.4	Повернення активів
A.5.12	A.8.2.1	Класифікація інформації
A.5.13	A.8.2.2	Маркування інформації
A.5.14	A.13.2.1, A.13.2.2, A.13.2.3	Передача інформації
A.5.15	A.9.1.1, A.9.1.2	Управління доступом
A.5.16	A.9.2.1	Управління ідентифікацією
A.5.17	A.9.2.4, A.9.3.1, A.9.4.3	Інформація для автентифікації

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.5.18	A.9.2.2, A.9.2.5, A.9.2.6	Права доступу
A.5.19	A.15.1.1	Інформаційна безпека у відносинах з постачальниками
A.5.20	A.15.1.2	Врахування вимог інформаційної безпеки в рамках угод з постачальниками
A.5.21	A.15.1.3	Управління інформаційною безпекою в ланцюгу постачання інформаційно-комунікаційних технологій (ІКТ)
A.5.22	A.15.2.1, A.15.2.2	Моніторинг, аналіз та управління змінами послуг постачальника
A.5.23	Новий	Інформаційна безпека використання хмарних сервісів
A.5.24	A.16.1.1	Планування та підготовка управління інцидентами інформаційної безпеки
A.5.25	A.16.1.4	Оцінка та прийняття рішень щодо подій інформаційної безпеки
A.5.26	A.16.1.5	Реагування на інциденти інформаційної безпеки

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.5.27	A.16.1.6	Навчання на інцидентах інформаційної безпеки
A.5.28	A.16.1.7	Збір доказів
A.5.29	A.17.1.1, A.17.1.2, A.17.1.3	Безпека інформації під час збою
A.5.30	Новий	Готовність постачальників ІКТ послуг до безперервності бізнесу
A.5.31	A.18.1.1, A.18.1.5	Правові, законодавчі, нормативні та договірні вимоги
A.5.32	A.18.1.2	Права інтелектуальної власності
A.5.33	A.18.1.3	Захист записів
A.5.34	A.18.1.4	Конфіденційність та захист персональних даних
A.5.35	A.18.2.1	Незалежна перевірка інформаційної безпеки
A.5.36	A.18.2.2, A.18.2.3	Дотримання політик, правил і стандартів інформаційної безпеки
A.5.37	A.12.1.1	Задокументовані операційні процедури
A.6 – Контролі людських ресурсів		
A.6.1	A.7.1.1	Скринінг/перевірка персоналу

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.6.2	A.7.1.2	Умови працевлаштування
A.6.3	A.7.2.2	Поінформованість, освіта та навчання з питань інформаційної безпеки
A.6.4	A.7.2.3	Дисциплінарний процес
A.6.5	A.7.3.1	Обов'язки після звільнення або зміни місця роботи
A.6.6	A.13.2.4	Угоди про конфіденційність або нерозголошення
A.6.7	A.6.2.2	Дистанційна робота
A.6.8	A.16.1.2, A.16.1.3	Звітування про події інформаційної безпеки
A.7 – Фізичні контролі		
A.7.1	A.11.1.1	Периметр фізичної безпеки
A.7.2	A.11.1.2, A.11.1.6	Фізичний контроль входу
A.7.3	A.11.1.3	Охорона офісів, приміщень та об'єктів
A.7.4	Новий	Моніторинг фізичної безпеки
A.7.5	A.11.1.4	Захист від фізичних і екологічних загроз
A.7.6	A.11.1.5	Робота в безпечних зонах

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.7.7	A.11.2.9	«Чистий стіл» і «чистий екран»
A.7.8	A.11.2.1	Розташування обладнання та його захист
A.7.9	A.11.2.6	Безпека активів за межами приміщення
A.7.10	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5	Носії інформації
A.7.11	A.11.2.2	Допоміжні утиліти
A.7.12	A.11.2.3	Безпека кабельної розводки
A.7.13	A.11.2.4	Обслуговування обладнання
A.7.14	A.11.2.7	Безпечна утилізація або повторне використання обладнання
A.8 – Технологічні контролі		
A.8.1	A.6.2.1, A.11.2.8	Кінцеві пристрої користувача
A.8.2	A.9.2.3	Привілейовані права доступу
A.8.3	A.9.4.1	Обмеження доступу до інформації
A.8.4	A.9.4.5	Доступ до вихідного коду
A.8.5	A.9.4.2	Безпечна автентифікація

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.8.6	A.12.1.3	Управління потужностями
A.8.7	A.12.2.1	Захист від шкідливого програмного забезпечення
A.8.8	A.12.6.1	Управління технічними вразливостями
A.8.9	Новий	Управління налаштуваннями
A.8.10	Новий	Видалення інформації
A.8.11	Новий	Маскування даних
A.8.12	Новий	Запобігання витоку даних
A.8.13	A.12.3.1	Резервне копіювання інформації
A.8.14	A.17.2.1	Резервування засобів обробки інформації
A.8.15	A.12.4.1, A.12.4.2, A.12.4.3	Логування подій
A.8.16	Новий	Моніторингова діяльність
A.8.17	A.12.4.4	Синхронізація годинників
A.8.18	A.9.4.4	Використання привілейованих службових програм
A.8.19	A.12.5.1, A.12.6.2	Встановлення програмного забезпечення на операційні системи

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.8.20	A.13.1.1	Безпека мереж
A.8.21	A.13.1.2	Безпека мережевих сервісів
A.8.22	A.13.1.3	Сегрегація мереж
A.8.23	Новий	Веб-фільтрація
A.8.24	A.10.1.1, A.10.1.2	Використання криптографії
A.8.25	A.14.2.1	Безпечний життєвий цикл розробки
A.8.26	A.14.1.2, A.14.1.3	Вимоги до безпеки додатків
A.8.27	A.14.2.5	Безпечна архітектура системи та принципи безпечної розробки
A.8.28	Новий	Безпечне кодування
A.8.29	A.14.2.8, A.14.2.9	Тестування безпеки на етапі розробки та прийняття (продукту)
A.8.30	A.14.2.7	Аутсорсингова розробка
A.8.31	A.12.1.4, A.14.2.6	Розділення середовища розробки, тестування та експлуатації
A.8.32	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	Управління змінами

Продовження таблиці 2.1

ISO 27001:2022	**ISO 27001:2013**	**Назва контролю**
A.8.33	A.14.3.1	Тестові дані
A.8.34	A.12.7.1	Захист інформаційних систем під час аудиту

2.2 Розроблення методу зіставлення контролів провідних стандартів аудиту з кібербезпеки

Розроблений метод зіставлення контролів провідних стандартів аудиту з кібербезпеки базується на інноваційному підході до зіставлення контролів безпеки між стандартами. На відміну від традиційного порівняння на рівні вимог чи контролів, у даному методі використовується зіставлення з додатковими рекомендаціями по впровадженню контролів для створення детального та всеохоплюючого аналізу.

На рисунку 2.1 зображені основні етапи проведення зіставлення контролів стандартів аудиту з кібербезпеки.

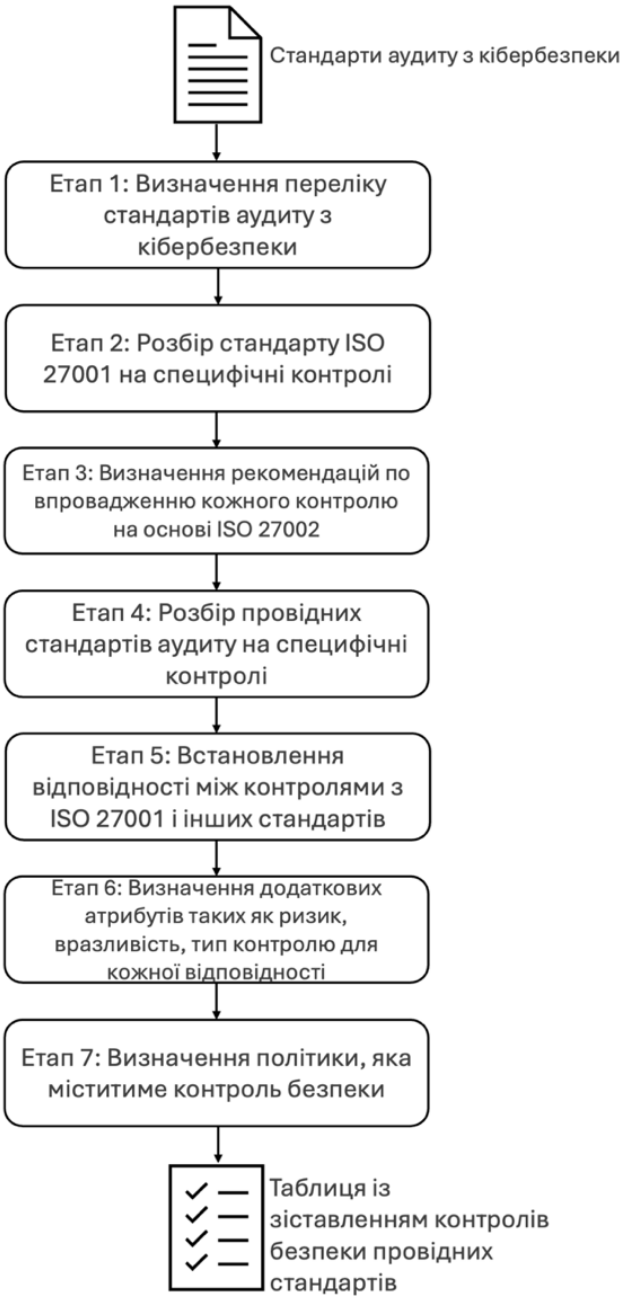


Рис. 2.1. Етапи проведення зіставлення контролів провідних стандартів аудиту з кібербезпеки

На **першому етапі** визначається перелік стандартів, які ляжуть в основу проведеного зіставлення контролів. Стандарт ISO 27001:2022 є одним із найбільш визнаних і широко використовуваних стандартів у сфері управління інформаційною безпекою. Саме тому його взято за основу для

розробки перехресного зіставлення контролів безпеки. Також, на основі дослідження і аналізу провідних практик та літературних джерел у галузі забезпечення інформаційної безпеки, вибрано наступний перелік стандартів аудиту з кібербезпеки для проведення перехресного зіставлення контролів:

- ISO/IEC 27001:2013
- NIST SP 800-53
- Trust Services Criteria (SOC 2)
- PCI DSS v.3.2.1
- PCI DSS v.4.0
- ISO/IEC 27701:2019

На **другому етапі** проводиться розбір стандарту ISO 27001:2022 на окремі специфічні контролі безпеки. А на **третьому етапі** проводиться зіставлення контролів зі стандарту ISO 27001:2022 з рекомендаціями по впровадженню стандарту ISO 27002:2022. Таким чином, кожному контролю стандарту ISO 27001:2022 буде відповідати декілька детальніших рекомендацій по впровадженню зі стандарту ISO 27002:2022.

На наступному, **четвертому етапі**, проводиться аналіз кожного з додаткових провідних стандартів аудиту і їхній розбір на окремі контролі.

На **п’ятому етапі** відбувається перехресне зіставлення між контролями усіх вибраних стандартів. Отримується матриця зіставлення, яка відображає відповідність між контролями та рекомендаціями кожного стандарту. У результаті цього, можна точно визначити, які вимоги та контролі з одного стандарту відповідають рекомендаціям з інших стандартів. Це дозволяє оцінити, яка частина контролів з одного стандарту вже покрита впровадженням іншого, а також ідентифікувати прогалини в безпеці, які можуть бути зміцнені додатковими контролями.

На **шостому етапі** розробляються додаткові атрибути, такі як загрози, вразливості та ризики для кожної встановленої відповідності. Ці атрибути полегшують використання таблиці зіставлення і служать додатковим референсним матеріалом для визначення застосовності того чи іншого контролю.

На **сьомому етапі** додатково зіставляється кожна встановлена відповідність контролів із назвою документа, який може містити ці вимоги, і слугувати документованою інформацією для підтримки СУІБ.

У результаті цієї послідовності дій, отримується таблиця відповідності контролів провідних стандартів аудиту з кібербезпеки (Рисунок 2.2 – Рисунок 2.3).

Підсумовуючи описаний метод, під час зіставлення аналізується кожен контроль з основного стандарту безпеки і встановлюється відповідність між ним та рекомендаціями з іншого стандарту. Якщо виявляється, що деякі контролі з одного стандарту вже покриті впровадженням іншого, то можна точно визначити, яка кількість контролів забезпечується додаванням нового стандарту.

Проте, також може статися, що після зіставлення виявляються прогалини в безпеці, де деякі контролі з основного стандарту не відповідають жодній рекомендації з іншого стандарту. У такому випадку можна розглянути додаткові контролі з того самого домену безпеки, які можуть бути впроваджені для зміцнення захисту. Це дозволяє створити більш повну та ефективну систему кібербезпеки, яка охоплює найважливіші аспекти безпеки даних та інформації.

Використання цього методу дозволяє ефективно впроваджувати набір стандартів кібербезпеки, забезпечуючи комплексний захист інформації та ресурсів організації. Існує можливість вибирати та адаптувати стандарти залежно від конкретних потреб організації, забезпечуючи оптимальний

рівень безпеки. Також, розроблена методологія перехресного впровадження стандартів не лише дозволяє ефективно управляти ризиками кібербезпеки, а й сприяє розвитку системи безпеки на основі широкого аналізу та використання кращих практик з різних стандартів.

Створення перехресного зіставлення дозволяє організаціям зрозуміти взаємозв'язок між різними стандартами кібербезпеки та показати відповідність їхніх систем управління інформаційною безпекою вимогам стандартів.

Практично, це означає, що впровадивши один стандарт аудиту з кібербезпеки, організація чи ОКІ отримує можливість оцінити, наскільки вона вже відповідає контрольним вимогам інших стандартів. Це означає, що при подальшому впровадженні нового стандарту їй необхідно буде лише перевірити та доповнити ті контрольні механізми, які ще не включені до вже існуючих стандартів. Такий підхід робить процес відповідності декільком стандартам набагато ефективнішим, економлячи час та ресурси організації.

Номер контролю ISO 27001:2022	Назва контролю ISO 27001:2022	Номер контролю ISO 27001:2013	Код	Назва контролю ISO 27001:2013	Контроль ISO 27001:2013	Домен/область/категорія активу	Загроза	Вразливість	Ризик	Посібник з впровадження
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.10	Політика щодо мобільних пристроїв	Для управління ризиками, пов'язаними з використанням мобільних пристроїв, слід прийняти політику та відповідні заходи безпеки.	Мобільні пристрої	Крадіжка або несанкціоноване розголошення інформації	Відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Крадіжка або несанкціоноване розголошення інформації через відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Забезпечити визначення та впровадження відповідних криптографічних методів для захисту інформації, що зберігається на мобільних пристроях або передається ними
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.11	Політика щодо мобільних пристроїв		Мобільні пристрої	Зараження шкідливим програмним забезпеченням	Відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних	Зараження шкідливим програмним забезпеченням через відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Забезпечити захист від шкідливих програм на мобільних пристроях (наприклад, шляхом встановлення рішення для захисту від шкідливих програм)
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.12	Політика щодо мобільних пристроїв		Мобільні пристрої	Крадіжка обладнання	Відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних	Крадіжка обладнання через відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Переконайтеся, що засоби керування для віддаленого вимкнення, стирання або блокування визначені та налаштовані для мобільних пристроїв (наприклад, через застосування рішення MDM).
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.13	Політика щодо мобільних пристроїв		Мобільні пристрої	Втрата або пошкодження системи чи даних	Відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних	Втрата або пошкодження системи або даних через відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Переконайтеся, що резервне копіювання важливої інформації налаштоване для мобільних пристроїв
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.14	Політика щодо мобільних пристроїв		Мобільні пристрої	Компрометація системи	Відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних	Компрометація системи через відсутність або недостатнє впровадження політики та допоміжних заходів безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв	Забезпечити визначення та впровадження вимог та обмежень щодо використання веб-сервісів та веб-додатків на мобільних пристроях (наприклад, за допомогою агентів ЕЦП)

Рис. 2.2. Таблиця зіставлення контролів безпеки провідних стандартів аудиту з кібербезпеки

Посібник з впровадження	Тип контролю	SOC2	NIST	PCI DSS	ISO 27701	PCI DSS 4.0	Відповідна політика інформаційної безпеки	Ідентифікатор політики
Забезпечити визначення та впровадження відповідних криптографічних методів для захисту інформації, що зберігається на мобільних пристроях або передається ними	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи	8
Забезпечити захист від шкідливих програм на мобільних пристроях (наприклад, шляхом встановлення рішення для захисту від шкідливих програм)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи	8
Переконайтеся, що засоби керування для віддаленого вимкнення, стирання або блокування визначені та налаштовані для мобільних пристроїв (наприклад, через застосування рішення MDM).	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи	8
Переконайтеся, що резервне копіювання важливої інформації налаштоване для мобільних пристроїв	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи	8
Забезпечити визначення та впровадження вимог та обмежень щодо використання веб-сервісів та веб-додатків на мобільних пристроях (наприклад, за допомогою агентів ЕЦП)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи	8

Рис. 2.3. Таблиця зіставлення контролів безпеки провідних стандартів аудиту з кібербезпеки (продовження)

Номер контролю ISO 27001:2022	Назва контролю ISO 27001:2022	Номер контролю ISO 27001:2013	Код	Назва контролю ISO 27001:2013	Контроль ISO 27001:2013	Домен/область/категорія активу	Посібник з впровадження	Тип контролю	SOC2	NIST	PCI DSS	ISO 27701	PCI DSS 4.0	Відповідна політика інформаційної безпеки
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.2	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити захист бізнес-інформації при використанні мобільних пристроїв шляхом застосування відповідних адміністративних (політика використання мобільних пристроїв), фізичних (блокування кабелів) та технічних (автентифікація, шифрування, захист від шкідливого програмного забезпечення) засобів контролю безпеки.	Адміністративний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.3	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що впроваджені відповідні засоби контролю для усунення ризиків роботи з мобільними пристроями в незахищених середовищах (наприклад, шифрування, віддалене стирання, рішення для захисту від шкідливого програмного забезпечення, реєстрація та моніторинг подій безпеки тощо). Користувачі пристроїв BYOD повинні підписувати контрактну угоду, яка зобов'язує працівника дотримуватися вимог інформаційної безпеки організації (в тому числі дотримуватися практик безпеки для мобільних пристроїв).	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.4	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що всі мобільні пристрої ідентифіковані та зареєстровані (наприклад, у реєстрі активів)	Адміністративний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.5	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що для фізичного захисту мобільних пристроїв впроваджено відповідні засоби контролю (наприклад, пломби, шифрування тощо).	Фізичний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.6	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити визначення та впровадження обмежень щодо встановлення програмного забезпечення на мобільних пристроях (наприклад, за допомогою офіційної політики щодо мобільних пристроїв, групових політик, агента EDR або системи MDM)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.7	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити визначення та впровадження вимог до версій програмного забезпечення для мобільних пристроїв та застосування патчів (наприклад, за допомогою автоматизованого процесу оновлення)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.8	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити визначення та впровадження обмежень на підключення мобільних пристроїв до інформаційних сервісів (наприклад, за допомогою групових політик, агента EUJT або системи MDM)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.9	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що засоби контролю доступу визначені та впроваджені для всіх мобільних пристроїв (наприклад, RADIUS, Windows Active Directory, LDAP, SecurID, Google Workspace тощо).	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.10	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити визначення та впровадження відповідних криптографічних методів для захисту інформації, що зберігається на мобільних пристроях або передається ними	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.11	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити захист від шкідливих програм на мобільних пристроях (наприклад, шляхом встановлення рішення для захисту від шкідливих програм)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.12	Політика щодо мобільних пристроїв	Для управління ризиками, пов'язаними з використанням мобільних пристроїв, слід прийняти політику та відповідні заходи безпеки.	Мобільні пристрої	Переконайтеся, що засоби керування для віддаленого вимкнення, стирання або блокування визначені та налаштовані для мобільних пристроїв (наприклад, через застосування рішення MDM).	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.13	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що резервне копіювання важливої інформації налаштоване для мобільних пристроїв	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.14	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити визначення та впровадження вимог та обмежень щодо використання веб-сервісів та веб-додатків на мобільних пристроях (наприклад, за допомогою агентів EUJT)	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.15	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що всі співробітники проінформовані та навчені (наприклад, за допомогою особистих тренінгів, розсилки електронною поштою, розвішування плакатів тощо) щодо захисту мобільних пристроїв у громадських місцях, конференц-залах та інших незахищених приміщеннях.	Адміністративний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.16	Політика щодо мобільних пристроїв		Мобільні пристрої	Забезпечити захист для уникнення несанкціонованого доступу до інформації, що зберігається та обробляється мобільними пристроями, або її розголошення, наприклад, за допомогою криптографічних методів та примусового використання секретної інформації для автентифікації.	Технічний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи
A.8.1	Кінцеві пристрої користувача	A6.2.1	ISO27002.A6.2.1.17	Політика щодо мобільних пристроїв		Мобільні пристрої	Переконайтеся, що мобільні пристрої фізично захищені від крадіжки, особливо коли вони залишені, наприклад, в автомобілях та інших видах транспорту, готельних номерах, конференц-центрах та місцях проведення зустрічей (наприклад, фізично замкнені)	Фізичний	CC6.7	AC-17, AC-18, AC-19	1.4, 4.1,11.1	6.3.2.1	**1.5.1,4.2.1,4.2.1.1**	Мобільні пристрої та політика дистанційної роботи

Рис. 2.4. Таблиця зіставлення контролів безпеки провідних стандартів аудиту з кібербезпеки (загальний вигляд)

Як видно з рисунків 2.2-2.4, в результаті створення зіставлення, ми отримали таблицю з відповідністю контролів безпеки різних стандартів аудиту. Тобто, ми можемо побачити аналоги для контролю безпеки з одного стандарту в інших. Для прикладу, контролю зі стандарту ISO 27001:2022 «A.8.1 – Кінцеві пристрої користувача» відповідає контроль «A.6.2.1 Політика користування мобільними пристроями» із стандарту ISO 27001:2013, контроль CC6.7 стандарту SOC 2, і одночасно три контролі стандарту NIST SP 800-53 – AC-17, AC-18, AC-19.

2.3 Аналіз переваг і недоліків перехресного впровадження стандартів аудиту з кібербезпеки

Перехресне впровадження стандартів кібербезпеки – це процес одночасного впровадження та використання кількох стандартів кібербезпеки на одному підприємстві чи ОКІ.

Таке впровадження може включати в себе [88]:

- **Впровадження різних стандартів кібербезпеки:** Наприклад, організація може впровадити ISO/IEC 27001, NIST Cybersecurity Framework та CIS Critical Security Controls.
- **Використання різних компонентів з різних стандартів:** Наприклад, організація може використовувати модель зрілості кібербезпеки з NIST Cybersecurity Framework, а також контролі безпеки з Додатку A стандарту ISO/IEC 27001.
- **Інтеграція різних стандартів кібербезпеки:** Наприклад, організація може інтегрувати систему управління ризиками ISO/IEC 27001 з системою моніторингу кібербезпеки NIST Cybersecurity Framework.

Перевагами перехресного впровадження стандартів аудиту з кібербезпеки в організаціях та на об’єктах критичної інфраструктури можуть бути наступні [89-92]:

- **Підвищення загального рівня кібербезпеки:** Перехресне впровадження стандартів кібербезпеки може допомогти об’єктам критичної інфраструктури підвищити загальний рівень кібербезпеки за рахунок створення більш комплексної та багатошарової структури захисту.
- **Зниження ризику кібератак:** Застосування контролів кібербезпеки з різних стандартів може допомогти знизити ризик кібератак, оскільки зловмисникам буде складніше знайти та використати вразливості.
- **Підвищення стійкості до кіберінцидентів:** Перехресне впровадження стандартів аудиту з кібербезпеки може допомогти об’єктам критичної інфраструктури стати більш стійкими до кіберінцидентів, оскільки вони матимуть реалізовані контролі для всебічного охоплення інфраструктури.
- **Підвищення довіри з боку клієнтів та партнерів:** Впровадження стандартів аудиту з кібербезпеки може допомогти підвищити довіру з боку клієнтів та партнерів, оскільки вони будуть більш впевнені, що їхні дані та інформація захищені.

До недоліків перехресного впровадження стандартів аудиту з кібербезпеки на об’єктах критичної інфраструктури можна віднести [88-92]:

- **Висока вартість:** Впровадження та підтримка контролів кібербезпеки з різних стандартів може бути дорогим, адже це потребує значних інвестицій в програмне та апаратне забезпечення, а також у підготовку персоналу.
- **Складність впровадження:** Перехресне впровадження стандартів аудиту з кібербезпеки може бути складним завданням, адже воно потребує ретельної координації та інтеграції різних систем та процесів.
- **Необхідність у кваліфікованих кадрах:** Для успішного впровадження та підтримки контролів кібербезпеки з різних стандартів

необхідні кваліфіковані кадри, які мають знання та досвід роботи з різними стандартами та системами.

- **Ризик конфліктів:** Перехресне впровадження стандартів аудиту з кібербезпеки може призвести до конфліктів між різними стандартами, що може ускладнити роботу та знизити ефективність захисту.

Таким чином, перехресне впровадження стандартів аудиту з кібербезпеки на ОКІ може мати як переваги, так і недоліки. Перед прийняттям рішення про впровадження таких стандартів важливо ретельно зважити всі за і проти, а також врахувати особливості конкретного підприємства, його галузь та профіль ризику.

2.4 Висновки до другого розділу

У другому розділі наведено методологію підвищення захищеності ОКІ за рахунок одночасного впровадження декількох стандартів аудиту з кібербезпеки та наведено обґрунтування ефективності даної методології.

1. У результаті порівняльної оцінки редакцій стандарту ISO 27001, розроблено таблицю відповідності між контролями Додатку А двох останніх редакцій стандарту ISO 27001 – 2013 і 2022 років. Використання розробленої таблиці відповідності скорочує час і ресурси необхідні для впровадження оновленої версії стандарту та приведення СУІБ до відповідності новим вимогам безпеки.

2. На основі проведеного дослідження ряду провідних стандартів аудиту з кібербезпеки, таких як ISO 27001, SOC 2, NIST 800-53 і PCI DSS, розроблено методологію перехресного впровадження стандартів аудиту з кібербезпеки. Розроблена методологія дозволяє організаціям і ОКІ уніфікувати взаємозв'язок між різними стандартами аудиту з кібербезпеки, визначити ступінь кореляції їхніх систем управління інформаційною безпекою вимогам визначених стандартів, а також оцінити відповідність

контролів безпеки, необхідних для досягнення вимог додатковому стандарту безпеки.

3. Вперше створена, в рамках розроблення методології перехресного впровадження стандартів, таблиця зіставлення контролів безпеки дозволяє організаціям і ОКІ забезпечити взаємозв'язок між різними стандартами кібербезпеки та оцінити відповідність їхніх СУІБ вимогам стандартів. Використання даної таблиці зіставлення дозволяє автоматизувати процес визначення унікальних контролів безпеки стандартів, зменшити час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки, і забезпечити ефективний захист ОКІ від кіберзагроз шляхом комплексного впровадження вимог декількох стандартів аудиту одночасно.

4. Дослідження особливостей використання розробленої методології перехресного впровадження стандартів аудиту з кібербезпеки в СУІБ ОКІ дозволило визначити особливості її застосування, що дає змогу ОКІ правильно і ефективно визначити ресурси і залученість персоналу при її використанні. Використання розробленої методології перехресного впровадження стандартів аудиту з кібербезпеки дозволяє організаціям та ОКІ підвищити рівень безпеки своїх активів, збільшити повноту охоплення ризиків, підвищити рівень стійкості до кіберінцидентів та, зрештою, підвищити довіру з боку клієнтів та партнерів.

РОЗДІЛ 3. РОЗРОБЛЕННЯ УНІВЕРСАЛЬНОГО АЛГОРИТМУ І МЕТОДУ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ КІБЕРБЕЗПЕКИ

3.1 Дослідження та оцінка недоліків існуючих методів впровадження стандартів аудиту з кібербезпеки

Чим складніший і детальніший стандарт обрано, тим більше охоплення доменів відповідними контролями безпеки можна очікувати в результаті його впровадження. Загалом це також означає, що організація матимете більш складні і комплексні політики та процедури для відповідності широкому охопленню. Проте дилема, з якою стикаються багато організацій, полягає в тому, що вони прагнуть досягнути відповідності тому чи іншому стандарту, і водночас звести до мінімуму кількість документів і контролів, які повинні підтримувати [93]. Саме тут важливий аспект погодження стратегії інформаційної безпеки з керівництвом компанії і визначення профілю ризику організації на фундаментальному рівні [94-96]:

- **Орієнтація на відповідність** (**Compliance Focused**) – ця стратегія ставить на меті досягнення компромісу шляхом фокусування на мінімально можливому наборі контролів для досягнення відповідності із законом чи стандартом (примітка – цей підхід не зовсім правильний, але дуже поширений).
- **Орієнтація на безпеку** (**Security Focused**) – ця стратегія зосереджується на жорстких інженерних методах захисту і не ставить на меті відповідність з певним стандартом (примітка – такий підхід зустрічається рідко).
- **Орієнтація на відповідність і безпеку (Compliance and Security Focused)** – це цілісний підхід, який зосереджений на забезпеченні захисту систем, програм та служб за замовчуванням (security by design and default), де відповідність розглядається як природний сторонній продукт

правильного поєднання практик конфіденційності та приватності (примітка – це оптимальний підхід, до якого повинні прагнути організації).

Підхід «Орієнтація на відповідність» зустрічається найчастіше і притаманний більшості компаній державного і приватного сектору. Основними перевагами даного підходу є простота, швидкість провадження, і нижча у порівнянні з іншими підходами вартість впровадження стандартів аудиту з кібербезпеки. Цей підхід характеризується тим, що організації впроваджують тільки мінімально необхідний набір практик і процесів, для того, щоб формально відповідати вимогам того чи іншого стандарту і успішно пройти сертифікаційний аудит. Багато організацій вважають такий підхід хорошим компромісом у ситуації коли партнери або клієнти вимагають підтвердження відповідності у формі сертифікату або звіту, виданого третьою стороною, але організація не готова інвестувати у суворі заходи безпеки. Очевидними мінусами такого підходу є невисока стійкість до кіберзагроз і атак.

Підхід «Орієнтація на безпеку» є діаметрально протилежним до підходу орієнтованого на відповідність у контексті матеріальних і людських затрат на впровадження контролів безпеки, і скрупульозності в їх впровадженні. Разом з тим, цей підхід має ряд недоліків. Окрім явно більшої вартості і часу на впровадження, цей підхід часто не ґрунтується на використанні загальновизнаних стандартів інформаційної безпеки і його покриття може носити точковий характер, який спирається не на оцінку ризиків і розуміння бізнес контексту, а на досвід персоналу, відповідального за безпеку. Для прикладу, організація може впровадити жорсткі контролі по захисту і моніторингу мережі, застосовувати IDS/IPS, захист від шкідливого програмного забезпечення, складну сегрегацію, але при цьому в організації може бути повністю відсутній процес навчання персоналу в галузі інформаційної безпеки, або не формалізовані відносини з постачальниками

послуг. Як правило, такий підхід можна зустріти в організаціях, де свого часу стався інцидент інформаційної безпеки, що спонукало керівництво швидко переглянути стратегію безпеки і впровадити жорсткі контролі безпеки; або в організаціях, де персонал відповідальний за інформаційну безпеку не має широкої компетенції в галузі і знання основних стандартів інформаційної безпеки.

І наостанок, підхід «Орієнтація на відповідність і безпеку» є найбільш цілісним і ефективним з погляду забезпечення необхідного рівня інформаційної безпеки в організації. Такий підхід бере до уваги контекст організації, її бізнес цілі, потреби зацікавлених сторін, спирається на результати оцінки ризиків і ґрунтується на використанні визнаних стандартів інформаційної безпеки, що дозволяє цілісно і всебічно забезпечити впровадження і підтримку необхідних безпекових процесів. Такий підхід потребує високої кваліфікації персоналу, відповідального за інформаційну безпеку, оскільки передбачає інтеграцію адміністративних, фізичних і технічних контролів безпеки одночасно.

Відмінності між даними трьома підходами узагальнено у Таблиці 3.1.

Таблиця 3.1

Порівняльна характеристика основних підходів до впровадження безпеки в організації

Критерії порівняння / Підходи	**Орієнтація на відповідність**	**Орієнтація на безпеку**	**Орієнтація на відповідність і безпеку**
Поширеність	Висока поширеність	Середня поширеність	Низька поширеність

Продовження таблиці 3.1

Критерії порівняння / Підходи	**Орієнтація на відповідність**	**Орієнтація на безпеку**	**Орієнтація на відповідність і безпеку**
Особливості	Впровадження мінімально необхідного набору практик і процесів, для того, щоб формально відповідати вимогам стандарту	Впровадження жорстких контролів для протидії основним загрозам, без детального аналізу контексту і застосовних нормативно-правових документів	Впровадження безпекових процесів на основі визнаного стандарту кібербезпеки, на основі оцінки ризиків, і беручи до уваги контекст організації
Недоліки	Невисока стійкість організацій до кіберзагроз і атак	Відсутність комплексного забезпечення безпеки і охоплення усіх найважливіших доменів	Вища ресурсозатратність; необхідність у відповідній кваліфікації персоналу

Відповідно, в рамках даного дисертаційного дослідження, при розробці методології перехресного впровадження стандартів аудиту, за основу береться саме підхід «Орієнтація на безпеку і відповідність» як найбільш

повний і ефективний підхід для побудови практик інформаційної безпеки в організації.

На рисунку 3.1 у вигляді блок схеми зображені основні етапи впровадження стандартів аудиту з кібербезпеки.

Рис. 3.1. Етапи впровадження стандартів аудиту

Відповідно до рисунку 3.1, процес впровадження стандартів аудиту з кібербезпеки включає наступні етапи [97-101]:

1) **Визначення контексту організації** – діяльність направлена на аналіз зовнішнього та внутрішнього середовища, в якому діє організація, з метою зрозуміти вплив цих факторів на її цілі та спроможність досягати їх. Зовнішнє середовище включає такі фактори, як політичні, економічні, соціокультурні, технологічні, правові та екологічні чинники, а також конкурентне середовище та очікування зацікавлених сторін. Внутрішнє середовище включає структуру організації, її культуру, ресурси, процеси та інші внутрішні фактори.

2) **Проведення оцінки на відповідність** – це процес визначення, аналізу та оцінки будь-яких невідповідностей або відхилень наявних практик і процесів від еталонного значення, визначеного стандартом чи іншим нормативним документом, якому організація прагне відповідати.

3) **Проведення оцінки ризиків інформаційної безпеки** – це процес ідентифікації, аналізу та оцінки потенційних загроз, вразливостей та можливих наслідків для інформаційних ресурсів організації. Цей процес допомагає виявити та оцінити ризики для інформаційної безпеки та прийняти відповідні заходи для їх управління.

4) **Розроблення нормативних документів** – це процес створення документів, які встановлюють вимоги до процесів, систем і практик, які виконує компанія для відповідності стандарту або іншому нормативному документу. Такі документи включають політики, процедури, плани, реєстри та інші допоміжні матеріали.

5) **Впровадження контролів інформаційної безпеки** – це процес встановлення та застосування конкретних заходів і правил для захисту інформаційних активів організації від потенційних загроз і ризиків. Ці контролі допомагають забезпечити конфіденційність, цілісність та доступність інформації, а також забезпечують виконання встановлених стандартів та розроблених нормативних документів.

6) **Внутрішній аудит** – це систематична та незалежна оцінка ефективності, дієздатності та відповідності внутрішнім політикам, процедурам та стандартам організації. На практиці він може проводитися із використанням того ж методу і шаблонів, що й оцінка не відповідність.

7) **Постійна підтримка і перегляд** – це процес систематичного оновлення та вдосконалення системи управління інформаційною безпекою організації з метою забезпечення її актуальності, ефективності та відповідності вимогам.

3.2 Розроблення методу проведення оцінки СУІБ на відповідність стандартам аудиту з кібербезпеки

3.2.1 Постановка проблеми проведення оцінки на відповідність

Оцінка на відповідність є невід'ємною та ключовою передумовою перед початком впровадження будь-якого стандарту аудиту з кібербезпеки. Цей етап визначає ступінь відповідності поточних практик, політик та процесів організації вимогам, які встановлює стандарт. Незважаючи на те, що це може здаватися витратним та складним процесом, він є незамінним у забезпеченні успішності та ефективності впровадження [102].

Зокрема, оцінка на відповідність є критичним етапом перед впровадженням нового стандарту ISO 27001, оскільки вона сприяє раціональному підходу до впровадження, мінімізації ризиків та забезпеченню ефективності та надійності інформаційної безпеки в організації [102].

Ось декілька ключових причин, чому оцінка на відповідність є важливою передумовою впровадження стандартів [102]:

- **Виявлення невідповідностей:** Оцінка на відповідність допомагає виявити розриви або невідповідності між існуючими практиками організації та вимогами стандарту. Це дає змогу чітко побачити, де саме потрібні зміни та вдосконалення.
- **Визначення пріоритетів:** Оцінка на відповідність допомагає організації визначити, які аспекти її поточних практик вимагають найбільшої уваги та зусиль для відповідності стандарту.
- **Мінімізація ризиків:** Сучасне цифрове суспільство пов'язане зі значними загрозами інформаційній безпеці. Оцінка на відповідність допомагає ідентифікувати слабкі місця та ризики в існуючих системах, що може бути вирішальним для запобігання можливим інцидентам.

- **Ефективне планування:** Результати оцінки на відповідність допомагають розробити детальний план впровадження змін, який сприяє раціональному та ефективному розгортанню нових практик та політик.
- **Збереження ресурсів:** Оцінка на відповідність дозволяє організації визначити, які аспекти вже відповідають вимогам, тим самим зменшуючи навантаження на ресурси при впровадженні.
- **Забезпечення поступовості:** Процес оцінки на відповідність допомагає організації планувати інтеграцію вимог поетапно, забезпечуючи плавний перехід та мінімізуючи вплив на операційну діяльність.
- **Підвищення свідомості:** У процесі оцінки на відповідність робиться акцент на усвідомлення необхідності змін та виконання вимог стандарту серед працівників, що сприяє внутрішній підтримці.

Отже, оцінка на відповідність є критичним етапом перед впровадженням стандарту ISO 27001, оскільки вона сприяє раціональному підходу до впровадження, мінімізації ризиків та забезпеченню ефективності та надійності інформаційної безпеки в організації [102].

Оскільки компанії тривалий час користувалися попередньою версією стандарту ISO 27001, що датується 2013 роком, і нова версія була представлена лише наприкінці 2022 року, виникає нестача актуальних та релевантних матеріалів, які б могли б допомогти організаціям в ефективній оцінці відповідності їхніх існуючих практик новим вимогам стандарту [102].

У світлі цієї проблеми, важливим є завдання розробити сучасний і актуальний метод оцінки організацій і ОКІ на відповідність новій версії стандарту ISO 27001. Даний метод має на меті надати компаніям і фахівцям з інформаційної безпеки інструмент для систематичного аналізу їхніх

існуючих практик та політик на предмет відповідності новим вимогам та принципам стандарту.

Одним із важливих етапів впровадження ISO 27001 є аналіз на відповідність, який дозволяє ідентифікувати відмінності між існуючими практиками організації та вимогами стандарту [102].

Аналіз останніх досліджень та публікацій в галузі впровадження стандарту ISO 27001 та методів аналізу на відповідність (gap assessment) дозволяє краще розуміти актуальний стан і тенденції у цій сфері. Нижче наведено певні підсумки досліджень, які можуть бути корисними для розробки методу оцінки відповідності організацій новій версії стандарту ISO 27001 [102]:

- **Перехід до нової версії стандарту:** Дослідження демонструють, що багато компаній зіткнулися з викликом переходу з попередньої версії стандарту ISO 27001 на нову. Зміни у вимогах та підходах вимагають від організацій адаптувати свої існуючі системи управління інформаційною безпекою [103].
- **Розроблення методів переходу:** Відсутність релевантних матеріалів для оцінки відповідності може вести до розробки власних методів переходу організацій на нову версію стандарту. Дослідження показують, що успішні підходи до оцінки відповідності включають ретельний аналіз нових вимог та їх порівняння з існуючими практиками [104].
- **Впровадження ризик-орієнтованого підходу:** Останні дослідження наголошують на значущості впровадження ризик-орієнтованого підходу при оцінці відповідності до стандарту ISO 27001. Це дозволяє зосередитися на тих аспектах, які мають найбільший вплив на безпеку інформації [105].
- **Застосування технологій:** Деякі дослідження вказують на важливість застосування технологій для полегшення процесу аналізу на

відповідність та моніторингу відповідності. Автоматизовані інструменти допомагають збирати, аналізувати та звітувати про дані, пов'язані з інформаційною безпекою [9].

- **Оптимізація процесу аудиту:** Дослідження вказують на можливість оптимізації процесу аудиту для оцінки відповідності. Впровадження структурованих аудиторських програм може зробити процес більш ефективним і зменшити зусилля, потрібні для оцінки відповідності [106].
- **Управління змінами:** Дослідження підкреслюють важливість ефективного управління змінами при переході до нової версії стандарту. Організації повинні ретельно планувати та впроваджувати зміни відповідно до нових вимог [107].

Ці підсумки досліджень можуть бути використані для розробки більш конкретного та адаптованого методу оцінки на відповідність новій версії стандарту ISO 27001, яка враховує унікальні потреби організацій та їхніх існуючих практик інформаційної безпеки.

3.2.2 Опис процесу проведення оцінки на відповідність з використанням контрольного списка

Використання контрольного списка для здійснення оцінки на відповідність перед впровадженням стандарту ISO 27001 має велике значення через ряд переваг, які цей інструмент може принести.

Контрольний список виступає як структурована та організована система, яка спрощує процес оцінки та допомагає ефективно ідентифікувати розриви між поточними практиками організації та новими вимогами стандарту.

Важливість використання контрольного списка для оцінки на невідповідності включає такі аспекти [102]:

- **Структурований підхід:** Контрольний список надає структурований підхід для оцінки. Він включає усі ключові вимоги стандарту, розбиті на конкретні елементи, що допомагають систематично пройти крізь процес оцінки.
- **Повнота та вичерпність:** Контрольний список допомагає впевнитися, що жодна важлива деталь не була пропущена під час оцінки. Він охоплює всі аспекти, які повинні бути перевірені для підтвердження відповідності.
- **Підвищення ефективності:** Використання контрольного списка допомагає уникнути непотрібного дублювання та непорозумінь. Усі учасники процесу оцінки працюють з однаковою базою даних, що сприяє збільшенню ефективності та точності.
- **Порівняння та аналіз:** Контрольний список дає можливість здійснювати порівняння між існуючими практиками та новими вимогами. Це допомагає точно визначити, де саме міститься невідповідність.
- **Ясність та документованість:** Використання контрольного списка забезпечує ясність у процесі оцінки та документування результатів. Це допомагає забезпечити прозорість та зручність для майбутнього моніторингу.
- **Послідовність:** Контрольний список встановлює послідовність дій, що сприяє організації процесу оцінки та уникненню пропусків.
- **Внутрішній та зовнішній аудит:** Контрольний список може бути використаний як база для внутрішнього аудиту для попередньої оцінки відповідності перед офіційним сертифікаційним аудитом стандарту.
- **Відстеження прогресу:** Контрольний список дозволяє відстежувати ступінь виконання та впровадження змін в організації протягом часу.

- **Референсний матеріал:** Контрольний список може служити як посібник для персоналу та аудиторів, які відповідають за оцінку відповідності.

Отже, використання контрольного списка для оцінки на відповідність є необхідним елементом перед початком впровадження стандарту ISO 27001, оскільки він сприяє систематизації та ефективності процесу оцінки, забезпечуючи комплексний та вичерпний підхід до вимог стандарту [102]. Окрім цього він надає і ряд інших переваг (Рисунок 3.2).

Рис. 3.2. Переваги використання контрольного списка для проведення оцінки СУІБ на відповідність стандарту ISO 27001

Під час проведення процесу оцінки на відповідність за допомогою контрольного списка потрібно дотримуватися певної послідовності дій (Рисунок 3.3).

Рис. 3.3. Основні кроки процесу проведення оцінки на відповідність за допомогою контрольного списка

Відповідно до наведеного рисунку, **вхідними даними** для процесу проведення оцінки СУІБ на відповідність стандарту ISO 27001 є шаблон контрольного списка, в якому перераховані всі ключові вимоги стандарту, які потрібно перевірити. У контрольний список також включені деталізовані пункти та підпункти, які відповідають кожній вимозі.

На **першому етапі** проводиться поверхневий аналіз списка і визначення застосовних до організації чи ОКІ контрольних пунктів.

На **другому етапі** відбувається збір необхідної інформації про поточні практики, політики та процеси організації чи ОКІ. Це може включати документацію, звіти, процедури та інші ресурси, що стосуються інформаційної безпеки.

На **третьому етапі** для кожного пункту контрольного списка проводиться порівняння поточних практик з вимогами стандарту. Визначається, чи відповідають організаційні практики кожній вимозі, або ж виникли «розриви» або «невідповідності».

На **четвертому етапі** відбувається опис результатів оцінювання. Для виявлених невідповідностей визначається, які конкретно аспекти потрібно вдосконалити або змінити, щоб вони відповідали вимогам стандарту.

На **п’ятому етапі** за допомогою методу експертних оцінок визначається статус і відсоток відповідності наявних практик вимогам стандарту.

На **шостому етапі** проводиться розроблення плану коректуючих дій. Для кожної виявленої невідповідності розробляється план дій, який включає необхідні кроки, відповідальних осіб та терміни впровадження рекомендацій.

У результаті роботи ми отримуємо детальний звіт із результатами оцінки і розробленими коректуючими діями, який можна використовувати для моніторингу та подальшого аудиту.

Процес проведення оцінки на відповідність за допомогою контрольного списка допомагає організаціям та ОКІ систематично та ефективно оцінити свою відповідність до вимог стандарту, виділити області для вдосконалення та забезпечити високий рівень інформаційної безпеки.

Цей процес оцінювання відповідності вимогам стандарту допомагає забезпечити високу якість та відповідність системи до прийнятих стандартів, забезпечуючи ефективну роботу та довіру до результатів [102].

Таким чином, перед початком впровадження стандарту ISO 27001, важливо провести оцінку на відповідність, що допоможе визначити сфери, які потребують покращення і доопрацювання, а також допоможе ефективно пріоритезувати завдання і виділити необхідні ресурси. Разом з тим, використання контрольного списка допоможе зробити цей процес оцінки цілісним і систематичним, і забезпечить повноцінне покриття усіх важливих вимог і контролів стандарту, що у свою чергу допоможе переконатися, що організація відповідає стандарту та вживає усіх необхідних заходів для захисту своїх інформаційних активів [102].

Перехід до нової версії стандарту вимагає від організацій ретельної підготовки та адаптації своїх безпекових практик до нових вимог. Процес оцінки на відповідність стає ключовим етапом в цій підготовці [102].

З врахуванням сучасної динамічної обстановки в галузі інформаційної безпеки, важливою стає не лише сама відповідність стандарту, а й здатність організації адаптуватися до змін та навколишнього середовища. Оцінка на відповідність допомагає ідентифікувати ризики, невідповідності та розриви між поточними практиками та вимогами стандарту. Цей процес дозволяє розробити стратегічний план впровадження змін та вдосконалення, спрямований на забезпечення найвищого рівня інформаційної безпеки.

Використання контрольного списка як інструменту для проведення оцінки на відповідність надає систематичності та структурованості процесу. Він сприяє ефективній ідентифікації невідповідностей, забезпечує повноту та точність перевірки, а також дозволяє легко відслідковувати прогрес у впровадженні змін.

Оцінка на відповідність є важливою передумовою для успішного впровадження нових практик безпеки , вирішення недоліків та забезпечення високого рівня захищеності інформації. Цей процес допомагає організаціям досягти відповідності до стандарту ISO 27001, підвищити рівень свідомості персоналу щодо інформаційної безпеки та забезпечити стійкий та надійний захист від сучасних загроз. Разом з тим, використання контрольного списка допомагає зробити цей процес оцінки цілісним і систематичним і забезпечити повноцінне покриття усіх важливих вимог і контролів стандарту.

3.3 Розроблення методології оцінки ризиків інформаційної безпеки

Проведення оцінки ризиків в рамках впровадження стандартів інформаційної безпеки є надзвичайно важливою складовою процесу забезпечення безпеки інформації в організації [108]. Ось кілька ключових причин, чому це важливо [109-112]:

- **Ідентифікація потенційних загроз і вразливостей:** Оцінка ризиків дозволяє ідентифікувати потенційні загрози та вразливості, які можуть вплинути на інформаційну безпеку організації.
- **Прийняття обґрунтованих рішень:** Аналіз ризиків надає базу для прийняття обґрунтованих рішень щодо призначення ресурсів для запобігання, виявлення та реагування на потенційні загрози.
- **Планування превентивних заходів:** На основі оцінки ризиків можна розробити плани дій для запобігання можливим загрозам і вразливостям.
- **Виявлення пріоритетних областей:** Оцінка ризиків допомагає визначити пріоритетні області, які потребують найбільшої уваги та ресурсів з погляду безпеки.

- **Вдосконалення стратегії безпеки:** На основі результатів оцінки можна вдосконалити стратегію інформаційної безпеки, щоб краще відповідати поточним і майбутнім загрозам.
- **Виконання регуляторних вимог:** Багато галузевих стандартів та законодавчих вимог вимагають проведення оцінки ризиків як невід'ємної частини процесу забезпечення безпеки інформації.

На рисунку 3.4 зображено основні етапи оцінки ризиків інформаційної безпеки в організації.

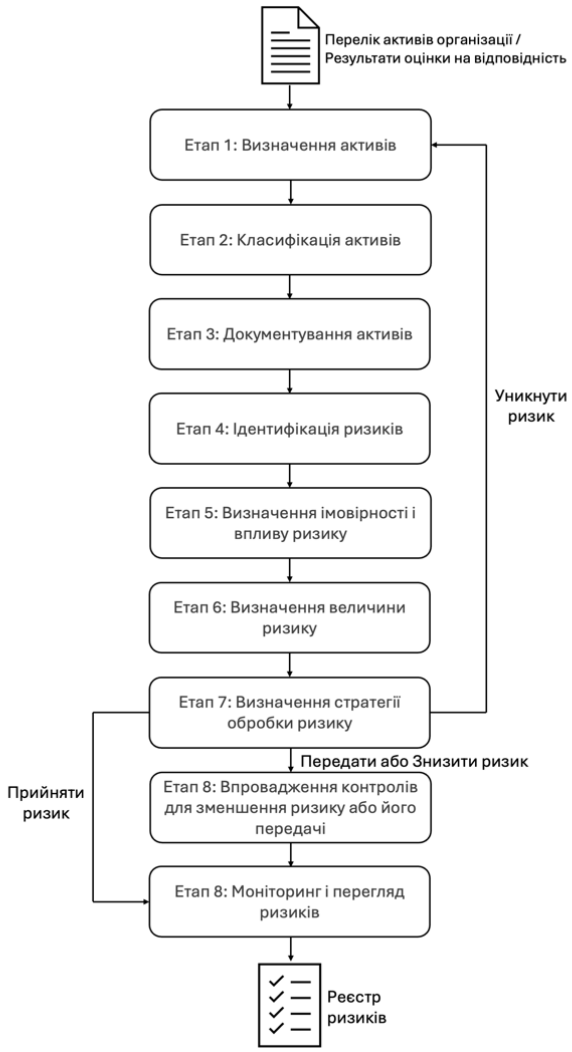


Рис. 3.4. Послідовність етапів оцінки і управління ризиками інформаційної безпеки

Отже, проведення оцінки ризиків допомагає організаціям ефективно керувати своєю інформаційною безпекою та знижувати ймовірність виникнення інцидентів або їх вплив на бізнес-процеси [113].

3.3.1 Ідентифікація активів організації

Початковими етапами оцінки ризиків є **визначення**, **класифікація** і **документування** важливих активів організації, для яких і будуть визначатися ризики.

Актив – це все, що має цінність для організації. У контексті інформаційної безпеки активи можна розділити на три категорії [114]:

- **Фізичні активи:** Обладнання, на якому зберігається або обробляється інформація, наприклад, комп'ютери, сервери, мережеві пристрої, носії даних.
- **Програмні активи:** Програмне забезпечення, яке використовується для обробки або зберігання інформації, наприклад, операційні системи, прикладні програми, бази даних.
- **Інформаційні активи:** Дані, які мають цінність для організації, наприклад, дані про клієнтів, фінансова інформація, інтелектуальна власність.

Ідентифікація активів – це процес виявлення та документування всіх активів організації, які мають цінність в контексті інформаційної безпеки.

Існує кілька способів ідентифікації активів [115]:

- **Інтерв'ю з ключовими співробітниками:** Співробітники, які працюють з різними системами та даними, можуть надати цінну інформацію про активи, які використовуються в організації.
- **Огляд документації:** Організаційна документація, така як політики безпеки, технічні специфікації та інвентарні списки, може містити інформацію про активи.

- **Сканування мережі:** Сканування мережі може допомогти виявити комп'ютери та інші пристрої, які підключені до мережі, а також програмне забезпечення, яке на них встановлене.
- **Аналіз даних:** Аналіз даних може допомогти виявити інформаційні активи, які не завжди очевидні, наприклад, дані, які зберігаються в базах даних або файлових системах.

Після того, як активи ідентифіковані, їх необхідно класифікувати за рівнем важливості та ризику. Це допоможе організації зосередити свої зусилля з захисту на найважливіших активах [116].

Існує кілька способів класифікації активів:

- **Бізнес-критичність:** Цей метод класифікує активи на основі їх впливу на бізнес-процеси організації.
- **Вартість:** Цей метод класифікує активи на основі їх вартості для організації.
- **Ризик:** Цей метод класифікує активи на основі ризику їх втрати або пошкодження.

Після того, як активи ідентифіковані та класифіковані, їх необхідно задокументувати. Документація активів може містити наступну інформацію:

- Назву активу
- Тип активу
- Місцезнаходження активу
- Власника активу
- Рівень важливості активу
- Рівень ризику активу
- Заходи захисту, які застосовуються до активу

Інформація про активи повинна регулярно оновлюватися, щоб відображати зміни в організації. Це допоможе гарантувати, що всі активи правильно ідентифіковані, класифіковані та захищені.

Процес ідентифікації активів – це важливий перший крок у розробці алгоритму оцінки ризиків інформаційної безпеки. Ретельно виконаний процес ідентифікації активів допоможе організації зосередити свої зусилля з захисту на найважливіших активах [117].

3.3.2 Ідентифікація ризиків інформаційної безпеки для активів

Наступним важливим етапом після ідентифікації і класифікації критичних активів компанії, слід провести оцінку ризиків для цих активів.

Ризик можна описати як комбінацію впливу несприятливої події та ймовірності її виникнення.

Управління ризиками – це процес ідентифікації, аналізу, оцінки та встановлення пріоритетів ризиків із наступним скоординованим та економічно-ефективним здійсненням активностей, спрямованих на досягнення мінімізації, моніторингу та контролю ймовірності або впливу несприятливих подій [118].

Процес управління ризиками включає наступні етапи [119]:

- Ідентифікація ризиків
- Аналіз ризиків на основі їхньої імовірності і впливу
- Оцінка ризиків
- Обробка ризиків
- Моніторинг і перегляд ризиків

Процес управління ризиками виконується власниками активів/процесів і може координуватися спеціалістом чи командою, відповідальною за інформаційну безпеку Також, відповідно до найкращих практик безпеки, процес перегляду ризиків повинен проводитися щонайменше щороку або

після проведення значних змін в організації. Переоцінка ризиків повинна враховувати проведені заходи по їх обробці.

3.3.3 Оцінка ризиків на основі розрахунку імовірності настання ризику і впливу

На **етапі ідентифікації ризиків** відбувається визначення основних ризиків організації як комбінацій потенційних загроз та існуючих вразливостей, які можуть спричинити небажаний вплив на роботу організації та її інформаційну безпеку. Ідентифікація ризиків повинна включати всі ризики незалежно від того, чи є їх джерело під контролем організації.

Власники активів/процесів несуть відповідальність за визначення ризиків, пов’язаних із їхніми активами/процесами.

Після визначення ризику власники активів/процесів повинні призначити власника ризику для кожного виявленого ризику. Власник ризику – це особа, яка несе відповідальність і має відповідні повноваження щодо управління, моніторингу та контролю виявленого ризику, включаючи впровадження вибраних заходів обробки і зменшення величини ризику.

Результати ідентифікації ризиків і призначені власники ризиків повинні бути розглянуті та затверджені командою управління організації. Також усі результати ідентифікації ризиків повинні бути відповідним чином задокументовані в реєстрі ризиків чи протоколі ідентифікації ризиків для використання на подальших етапах управління ризиками.

Етап аналізу ризиків спрямований на досягнення розуміння ризику та його природи. Ризик аналізується шляхом визначення його ймовірності (Likelihood) та впливу (Impact). Основною перевагою цього є зниження рівня невизначеності та зосередження на високопріоритетних ризиках.

У межах даної методології, імовірність ризику визначається на основі наявної статистики, історичних даних та/або експертної думки відповідно до наступної шкали (Таблиця 3.2).

Таблиця 3.2

Шкала для визначення імовірності ризику

Імовірність	**Опис**	**Числове значення**
Дуже Низька	Хоча вони ймовірні, ми, ймовірно, ніколи не станемо свідками подій такого характеру	1
Низька	Події такого характеру є рідкістю, але існує реальна ймовірність того, що ми можемо стати їх свідками у майбутньому	2
Середня	Цілком можливо, що ми станемо свідками події такого характеру	5
Висока	Ймовірно, незабаром ми станемо свідками події такого характеру	7
Дуже Висока	Ми неодмінно станемо свідками подій такого характеру. Ймовірно, вони відбуваються прямо зараз	9

Вплив, який може бути спричинений у разі реалізації ризику, визначається згідно зі шкалою, наведеною в таблиці 3.3.

Таблиця 3.3

Шкала для визначення впливу ризику

Вплив	**Опис**	**Числове значення**
Низький	Незначні фінансові втрати. Незначне нормативне порушення (адміністративна відповідальність). Вплив на репутацію відсутній або незначний.	1
Середній	Помірні фінансові втрати. Порушення законодавства середньої тяжкості (адміністративна відповідальність). Негативні відгуки клієнтів.	2
Високий	Значні фінансові втрати. Порушення законодавства середньої тяжкості (адміністративна відповідальність). Дуже негативна реакція клієнтів, втрата одного або кількох клієнтів.	7
Дуже Високий	Дуже значні фінансові втрати. Грубе порушення законодавства (адміністративна або кримінальна відповідальність). Вкрай негативна реакція клієнтів, втрата значної кількості клієнтів.	9

Відповідно, рівень ризику визначається використовуючи наступну формулу:

$$\text{Рівень ризику} = \text{Імовірність} * \text{Вплив} \quad (3.1)$$

Нижче наведено матрицю для визначення величини ризику на основі даних про імовірність і вплив (Таблиця 3.4).

Таблиця 3.4

Матриця для визначення величини ризику

		Імовірність				
		Дуже Низька	Низька	Середня	Висока	Дуже Висока
Вплив	Низький	1	2	5	7	9
	Середній	2	4	10	14	18
	Високий	7	14	35	49	63
	Дуже Високий	9	18	45	63	81

Визначений Рівень ризику може потрапляти в одну із трьох категорій, відповідно до таблиці 3.5.

Таблиця 3.5

Опис Рівнів ризику

	Рівень ризику	**Опис**
Зелений	[1-5] - Низький	Низький ризик, який не потребує жодних заходів по його обробці. Ризик не має впливу на роботу організації, або його вплив дуже слабкий.
Жовтий	[7-14] - Середній	Ризик, який можна прийняти, оскільки він не має істотного впливу на роботу організації. Заходи по обробці ризику можуть застосовуватися, але не є обов'язковими.
Червоний	[18-81] - Високий	Неприйнятний ризик із серйозним негативним впливом на роботу організації. Застосування заходів по обробці ризику є обов'язковим.

Оцінка ризику використовується для визначення необхідності застосування заходів з обробки ризику на основі результатів аналізу ризику та визначеного рівня ризику. Така оцінка використовується для визначення пріоритетності ризиків для подальшого планування їх обробки.

Власники ризиків відповідають за оцінку ризиків, якими вони володіють. Власники ризиків повинні проводити оцінку ризиків відразу після завершення аналізу ризиків. Щоб оцінити ризик, власники ризиків повинні:

- порівняти результати аналізу ризику з критеріями прийнятності ризику;
- якщо застосовно, прийняти відповідне рішення щодо обробки ризиків на основі результатів аналізу витрат і вигод або внутрішнього обговорення;
- визначити пріоритетність неприйнятних ризиків для обробки.

Власники ризиків повинні документувати та зберігати задокументовану інформацію про діяльність з оцінки ризиків та їх результати в реєстрі ризиків.

3.3.4 Визначення стратегії обробки ризику

Після визначення рівня ризику необхідно вжити заходів щодо їх **обробки**. Для кожного ризику слід розглянути один із наступних методів обробки:

- **Прийняти ризик (Accept),** який не відповідає критеріям прийнятності, оскільки ризик не можна змінити або вартість заходів з обробки перевищує вартість активу (тобто вартість ризику). Це також означає, що власник ризику погоджується прийняти вплив реалізації даного ризику.
- **Передати (Transfer)** заходи по обробці ризику на третю сторону (наприклад, страховій компанії, постачальнику послуг тощо).
- **Уникнути ризик (Avoid),** відмовившись від взаємодії з джерелом цього ризику.

- **Знизити/пом’якшити величину ризику (Mitigate)** до прийнятного рівня, запровадивши відповідні засоби контролю.

Заходи, необхідні для обробки ризиків, часові рамки їх виконання а також статус виконання повинні бути визначені та зберігатися в реєстрі ризиків.

3.3.5 Обробка і постійний моніторинг ризиків

Після виконання дій з обробки, ризик, який залишається, називається залишковим ризиком. Залишковий ризик – це ризик, який організація вирішує прийняти, а не обробляти іншим способом.

Як моніторинг, так і перегляд залишкових ризиків повинні бути плановою активністю загального процесу управління ризиками та передбачати регулярну перевірку і перегляд. Власник ризику несе відповідальність за проведення моніторингу та аналізу ризиків, а також впровадження визначених заходів з усунення ризиків.

Переоцінку ризиків слід проводити принаймні раз на рік або частіше у разі значних змін у середовищі організації.

Нижче наведено шаблон для реєстру ризиків організації (Рисунки 3.5 – 3.7). Цей шаблон розроблений у відповідності з найкращими практиками інформаційної безпеки і ґрунтується на міжнародному стандарті ISO 27005 [119]. Таким чином, він може використовуватися як організаціями і ОКІ, які прагнуть досягнути відповідності стандарту ISO 27001, так і будь-якими іншими організаціями, які прагнуть побудувати процес ефективної оцінки і управління ризиками інформаційної безпеки. Розроблений шаблон також представлений у Додатку Г даної дисертаційної роботи.

ID Ризику	Актив/Процес	Опис Ризику	Власник Ризику	Імовірність	Вплив	Рівень Ризику	Варіант Обробки Ризику	Відповідний ISO 27001 Контроль
001	Документація з захисту інформації	Відсутність постійної придатності, адекватності, ефективності керівництва та підтримки інформаційної безпеки в компанії.	Директор	Низька	Середній	Середній	Пом'якшення (Mitigate)	Набір політик інформаційної безпеки має бути визначений, затверджений керівництвом, опублікований і доведений до відома співробітників і відповідних зовнішніх сторін.
002	Обов'язки щодо інформаційної безпеки	Несанкціонована або ненавмисна модифікація або нецільове використання активів організації через відсутність розподілу обов'язків.	Спеціаліст з Інформаційної Безпеки	Середня	Високий	Середній	Пом'якшення (Mitigate)	Конфліктні обов'язки та сфери відповідальності мають бути розділені, щоб зменшити можливості для несанкціонованої чи ненавмисної модифікації чи нецільового використання активів організації.
003	Керування доступом користувачів	Злам пароля через відсутність або неправильну реалізацію системи керування паролями та використання слабких паролів.	Спеціаліст з Інформаційної Безпеки	Висока	Дуже Високий	Високий	Пом'якшення (Mitigate)	Від користувачів вимагається дотримуватись практики організації щодо використання секретної інформації автентифікації.

Рис. 3.5. Фрагмент шаблона реєстру ризиків інформаційної безпеки

Відповідний ISO 27001 Контроль	Номер відповідного контролю ISO 27001	Відповідний ISO 27001 Домен	Контроль	Статус	Залишкова імовірність	Залишковий вплив	Залишковий рівень ризику
Набір політик інформаційної безпеки має бути визначений, затверджений керівництвом, опублікований і доведений до відома співробітників і відповідних зовнішніх сторін.	A.5.1.1	Політики інформаційної безпеки	Ризик зменшується шляхом створення доменно-спеціальних політик щодо впровадження СУІБ.	В процесі			
Конфліктні обов'язки та сфери відповідальності мають бути розділені, щоб зменшити можливості для несанкціонованої чи ненавмисної модифікації чи нецільового використання активів організації.	A.6.1.2	Розподіл обов'язків	Ризик зменшується шляхом опису ролей і обов'язків щодо впровадження та підтримки кожної окремої політики та впровадження процесу контролю змін.	Прийнято після обробки	Низька	Низький	Низький
Від користувачів вимагається дотримуватись практики організації щодо використання секретної інформації автентифікації.	A.9.3.1	Використання секретної інформації для аутентифікації	Створити політику використання складних паролів.	Прийнято після обробки	Низька	Низький	Низький

Рис. 3.6. Фрагмент шаблона реєстру ризиків інформаційної безпеки (продовження)

	ID Ризику	Актив/Процес	Опис Ризику	Власник Ризику	Імовірність	Вплив	Рівень Ризику	Варіант Обробки Ризику	Відповідний ISO 27001 Контроль	Номер відповідного контролю ISO 27001	Відповідний ISO 27001 Домен	Контроль	Статус	Залишкова імовірність	Залишковий вплив	Залишковий рівень ризику
1																
2	001	Документація з захисту інформації	Відсутність постійної придатності, адекватності, ефективності керівництва та підтримки інформаційної безпеки в компанії.	Директор	Низька	Середній	Середній	Пом'якшення (Mitigate)	Набір політик інформаційної безпеки має бути визначений, затверджений керівництвом, опублікований і доведений до відома співробітників і відповідних зовнішніх сторін.	A.5.1.1	Політики інформаційної безпеки	Ризик зменшується шляхом створення доменно-спеціальних політик щодо впровадження СУІБ.	В процесі			
3	002	Обов'язки щодо інформаційної безпеки	Несанкціонована або ненавмисна модифікація або нецільове використання активів організації через відсутність розподілу обов'язків.	Спеціаліст з Інформаційної Безпеки	Середня	Високий	Середній	Пом'якшення (Mitigate)	Конфліктні обов'язки та сфери відповідальності мають бути розділені, щоб зменшити можливості для несанкціонованої чи ненавмисної модифікації чи нецільового використання активів організації.	A.6.1.2	Розподіл обов'язків	Ризик зменшується шляхом опису ролей і обов'язків щодо впровадження та підтримки кожної окремої політики та впровадження процесу контролю змін.	Прийнято після обробки	Низька	Низький	Низький
4	003	Керування доступом користувачів	Злам пароля через відсутність або неправильну реалізацію системи керування паролями та використання слабких паролів.	Спеціаліст з Інформаційної Безпеки	Висока	Дуже Високий	Високий	Пом'якшення (Mitigate)	Від користувачів вимагається дотримуватись практики організації щодо використання секретної інформації автентифікації.	A.9.3.1	Використання секретної інформації для аутентифікації	Створити політику використання складних паролів.	Прийнято після обробки	Низька	Низький	Низький

Рис. 3.7. Фрагмент шаблона реєстру ризиків інформаційної безпеки (загальний вигляд)

Даний шаблон містить наступні поля для заповнення:

- **ID Ризику** – індивідуальний числовий ідентифікатор ризику.
- **Актив/Процес** – назва активу чи процесу, для якого притаманний ризик інформаційної безпеки

- **Опис Ризику** – детальний опис ризику інформаційної безпеки
- **Власник Ризику** – особа або група осіб, які несуть відповідальність за управління конкретним ризиком в організації.
- **Імовірність** – якісне визначення ймовірності того, що певна загроза або подія, яка може призвести до негативних наслідків, відбудеться.
- **Вплив** – характеристика, яка визначається наслідками або шкодою, яку може спричинити виникнення певної загрози або події..
- **Рівень Ризику** – це оцінка імовірності та впливу ризику, що може бути використана для класифікації ризиків та прийняття рішень щодо їх управління. Цей показник визначає, наскільки серйозним є конкретний ризик для організації і наскільки важливо приділити йому увагу.
- **Варіант Обробки Ризику** – визначається на основі оцінки рівня ризику та стратегії управління ризиками. Це означає вибір конкретних заходів або стратегій для зменшення, передачі, уникнення чи прийняття ризику. Такий вибір може бути зроблений з урахуванням ресурсів, цілей організації та інших факторів.
- **Відповідний ISO 27001 Контроль** – контроль зі стандарту ISO 27001 який може бути використаний для реагування на ризик.
- **Номер відповідного контролю ISO 27001** – числовий ідентифікатор відповідного ISO 27001 контролю.
- **Відповідний ISO 27001 Домен** – назва домену зі стандарту ISO 27001 якому належить відповідний контроль.
- **Контроль** – конкретний засіб захисту який застосовується для впливу на визначений ризик.
- **Статус** – статус впровадження визначеного контролю безпеки.
- **Залишкова імовірність** – імовірність реалізації ризику, яка залишається після впровадження контролів по його обробці.

- **Залишковий вплив** – вплив ризику, який залишається після впровадження контролів по його обробці.
- **Залишковий рівень ризику** – це ризик, який організація вирішує прийняти, а не обробляти іншим способом.

3.4 Розроблення методології перехресного впровадження стандартів аудиту з кібербезпеки на основі зіставлення контролів

На основі результатів оцінки на відповідність та проведеної оцінки ризиків, організація чи ОКІ отримує перелік унікальних контролів безпеки на основі стандарту ISO 27001, впровадивши які вона зможе досягнути і підтвердити відповідність своїх безпекових процесів вимогам нормативного стандарту. Окрім того, оскільки контрольний список для оцінки і реєстр ризиків містять прикладні контролі безпеки, дотримуючись рекомендацій цих документів, організація чт ОКІ в змозі забезпечити не тільки формальну відповідність вимогам стандарту, а й забезпечити належний рівень захисту своїх інформаційних активів.

Окрім того, дана методологія дозволяє оцінити ступінь перекриття контролів (у відсотковому відношенні) для перехресного впровадження стандартів аудиту з кібербезпеки. Тобто, визначити, яку частину унікальних контролів стандарту аудиту з кібербезпеки організація вже покрила, маючи впровадженим інший стандарт аудиту і множину контролів, які ще потрібно впровадити для досягнення відповідності додатковим стандартам (Рисунок 3.8).

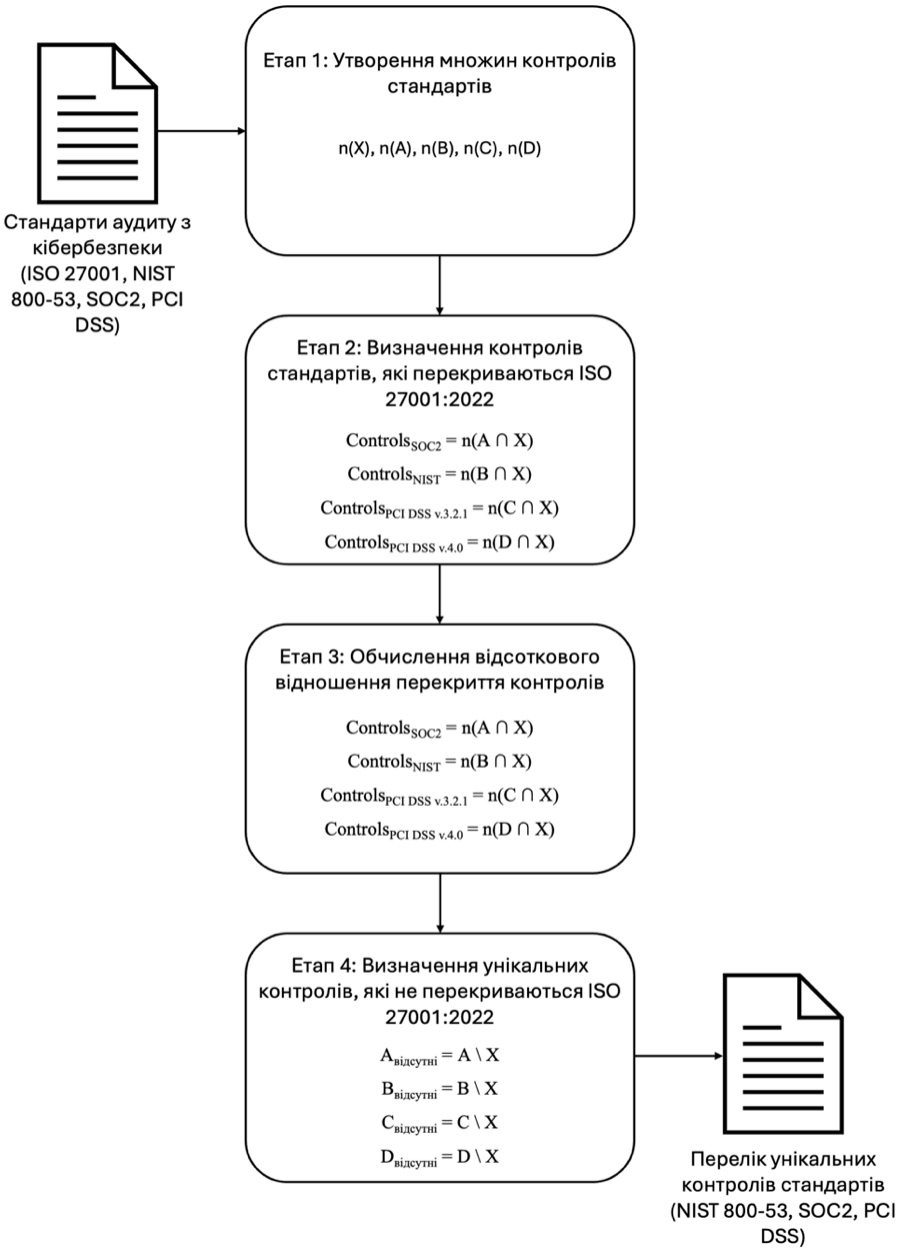


Рис. 3.8. Методологія перехресного впровадження стандартів

Для обчислення відсоткового відношення перекриття контролів введемо наступні позначення:

- X – множина контролів стандарту ISO 27001:2022,
- A – множина контролів стандарту SOC 2,
- B – множина контролів стандарту NIST SP 800-53,

- C – множина контролів стандарту PCI DSS v.3.2.1,
- D – множина контролів стандарту PCI DSS v.4.0,
- n(X) - кількість елементів у множині X,
- n(A) - кількість елементів у множині A,
- n(B) - кількість елементів у множині B,
- n(C) - кількість елементів у множині C,
- n(D) - кількість елементів у множині D.

Відповідно, для того, щоб оцінити яка кількість контролів стандарту SOC 2 перекривається контролями стандарту ISO 27001:2022, нам потрібно визначити кількість елементів, що є спільними для множин A і X.

Таким чином,

$$Controls_{SOC\ 2} = n(A \cap X) \tag{3.2}$$

де:

$Controls_{SOC\ 2}$ – кількість контролів SOC 2, що перекривається ISO 27001:2022.

Тоді відсоткове відношення кількості елементів множини A, які містяться в множині X, тобто відсоткове відношення покриття контролів стандарту SOC 2 стандартом ISO 27001:2022 можна обчислити за формулою:

$$\text{Відсоток (SOC 2)} = \frac{n(A \cap X)}{n(X)} \times 100\% \tag{3.3}$$

Ця формула обчислює відсоткове відношення кількості елементів множини A, які є також присутніми в множині X, відносно загальної кількості елементів у множині X.

Ми також можемо обчислити відсоткове відношення покриття контролів інших стандартів за рахунок контролів стандарту ISO 27001:2022 за наступними формулами:

$$\text{Відсоток (NIST)} = \frac{n(B \cap X)}{n(X)} \times 100\% \quad (3.4)$$

$$\text{Відсоток (PCI DSS v.3.2.1)} = \frac{n(B \cap X)}{n(X)} \times 100\% \quad (3.5)$$

$$\text{Відсоток (PCI DSS v.4.0)} = \frac{n(D \cap X)}{n(X)} \times 100\% \quad (3.6)$$

Дані обчислення допоможуть визначити яку частину контролів стандартів перекрито за рахунок впровадження стандарту ISO 27001:2022.

Ми також можемо визначити множину контролів кожного стандарту, які ще потрібно впровадити для досягнення повної відповідності цьому стандарту. Для прикладу, для визначення унікальних контролів стандарту SOC 2, які не покриваються стандартом ISO скористаємося наступною формулою:

$$A_{\text{відсутні}} = A \setminus X, \quad (3.7)$$

де:

- $A_{\text{відсутні}}$ – множина значень з A, які не містяться в X, тобто контролі зі стандарту SOC 2, які не покриваються ISO 27001:2022;
- A – множина значень A, тобто контролі стандарту SOC 2;
- X – множина значень X, тобто контролі стандарту ISO 27001:2022;
- \ – операція різниці множин, яка повертає всі елементи, що належать множині A, але не належать множині X.

Відповідно, для визначення унікальних контролів інших стандартів, які не покриваються стандартом ISO 27001:2022 ми можемо скористатися наступними формулами:

$$B_{\text{відсутні}} = B \setminus X \text{ (для NIST SP 800-53)} \quad (3.8)$$

$$C_{\text{відсутні}} = C \setminus X \text{ (для PCI DSS v.3.2.1)} \quad (3.9)$$

$$D_{\text{відсутні}} = D \setminus X \text{ (для PCI DSS v.4.0)} \quad (3.10)$$

3.5 Розроблення політик і допоміжних документів для впровадження стандартів аудиту з кібербезпеки

3.5.1 Визначення і огляд основних політик в рамках впровадження стандартів

Розроблення політик і допоміжних документів для впровадження стандартів кібербезпеки – це ключовий етап у забезпеченні ефективного управління кібербезпекою в організації.

Розроблення політик є важливою складовою будь-якої організації з погляду забезпечення керівництва, створення регулятивного середовища та визначення важливих принципів, що впливають на роботу. У контексті кібербезпеки, політика визначає основні правила, вимоги та рекомендації, які організація використовує для захисту своїх інформаційних ресурсів [120].

Нижче наведено декілька аспектів важливості політик кібербезпеки [121-124]:

- **Забезпечення відповідності:** Політика кібербезпеки визначає вимоги та рекомендації, які організація повинна дотримуватися для відповідності законодавству, регулятивним вимогам та міжнародним стандартам аудиту з кібербезпеки.
- **Захист інформації:** Політика встановлює правила та процедури для захисту конфіденційної інформації від несанкціонованого доступу, втрати або витоку.
- **Мінімізація ризиків:** Політика визначає заходи та процедури для виявлення, оцінки та управління ризиками інформаційної безпеки в організації.
- **Підвищення свідомості персоналу:** Політика включає правила та інструкції для персоналу щодо правил безпеки та їх відповідальності у забезпеченні безпеки інформації.

- **Збільшення довіри зацікавлених сторін:** Політика безпеки демонструє зобов'язання організації щодо захисту інформації та може сприяти підвищенню довіри клієнтів, партнерів та інших зацікавлених сторін.

Політика інформаційної безпеки є важливим інструментом для створення безпечного та надійного інформаційного середовища в організації, а також для забезпечення відповідності вимогам законодавства та стандартів безпеки.

При створенні документації необхідно виконати наступні кроки [124-125]:

- **Аналіз вимог стандарту(-ів):** Організація повинна ретельно вивчити вимоги стандартів кібербезпеки, які планує впроваджувати. Це може включати, наприклад, ISO/IEC 27001, NIST SP 800-53 або інші відповідні стандарти.
- **Визначення обсягу документації:** Організація повинна визначити, які конкретні політики, процедури та інші допоміжні документи будуть потрібні для відповідності вимогам стандарту(-ів).
- **Розроблення політик:** Розроблення загальних політик, які визначають загальні принципи та підходи до кібербезпеки в організації. Це може включати політику з керування доступом, політику з управління паролями, політику з обмеження використання програмного забезпечення тощо.
- **Створення процедур:** При необхідності, організація може розробити додаткові процедури для деталізації вимог, викладених в політиках або опису конкретних механізмів чи процесів досягнення відповідності вимогам стандарту чи політики (наприклад, процедура з

реагування на інциденти, процедура резервного копіювання та відновленням даних тощо).

- **Розроблення допоміжних документів:** Окрім політик і процедур, організація повинна також підготувати інші допоміжні документи, такі як навчальні матеріали для персоналу, шаблони документів, переліки контактів, реєстри і журнали ризиків чи подій, документ про сферу застосування тощо, які допоможуть у впровадженні політик та процедур та можуть бути корисними при впровадженні і підтримці системи безпеки.
- **Перегляд і затвердження:** Після розроблення, необхідно провести перегляд розроблених документів керівництвом та зацікавленими сторонами, внести необхідні корективи та отримати затвердження для використання.
- **Впровадження і комунікація:** Наступним кроком є впровадження розроблених політик і документів в організації, надання їх на навчання та інформування персоналу про їх використання та важливість.
- **Моніторинг і оновлення:** Організація повинна постійно відслідковувати виконання політик і процедур та вносити необхідні зміни та оновлення на основі змін в стандартах, технологіях та внутрішніх потребах організації.

Ці кроки допоможуть забезпечити систематичне та комплексне впровадження стандартів аудиту з кібербезпеки в організації чи ОКІ.

Нижче наведено перелік основних політик, розробку яких вимагає більшість стандартів аудиту з кібербезпеки (Таблиця 3.6).

Таблиця 3.6

Перелік основних політик кібербезпеки

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Інформаційної Безпеки	Information Security Policy	Загальна політика, яка встановлює правила, процедури та вимоги, спрямовані на захист конфіденційності, цілісності та доступності інформації, а також забезпечення відповідності вимогам законодавства та стандартів безпеки.
Політика Документування Інформації	Document Management Policy	Набір встановлених правил, процедур та вимог, спрямованих на систематичне збереження, організацію та управління документами і записами з метою забезпечення їх доступності, цілісності, конфіденційності та відповідності вимогам законодавства та стандартів.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Комунікації	Communication Policy	Набір встановлених правил, процедур та стратегій, що визначають способи та засоби взаємодії в межах організації та з її зацікавленими сторонами з метою ефективної передачі інформації, сприяння взаєморозумінню та досягненню спільних цілей.
Політика Управління Ризиками	Risk Management Policy	Набір встановлених правил, процедур та методик, спрямованих на ідентифікацію, аналіз та оцінку потенційних загроз, вразливостей та можливих наслідків для інформаційних ресурсів та діяльності організації з метою вжиття відповідних заходів з управління ризиками.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Внутрішнього Аудиту	Internal Audit Policy	Набір встановлених правил, процедур та методів, спрямованих на систематичний та об'єктивний перегляд та оцінку інформаційних систем та процесів, що забезпечують безпеку даних та інформації в організації, з метою ідентифікації слабких місць, виявлення ризиків та рекомендацій щодо покращення управління інформаційною безпекою.
Політика Перегляду Керівництвом	Management Review Policy	Набір встановлених правил, процедур та практик, які визначають систематичність та процеси перегляду та оцінки стратегій, процедур та контрольних механізмів інформаційної безпеки організації вищим керівництвом для забезпечення відповідності цілям та стандартам безпеки.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Коректуючих Дій	Corrective Action Policy	Набір встановлених правил, процедур та практик, спрямованих на ефективне виявлення, аналіз та виправлення помилок, відхилень від стандартів або невідповідностей у процесах, продукції або послугах організації з метою забезпечення якості та ефективності.
Політика Використання Мобільних Пристроїв	Mobile Devices Policy	Набір встановлених правил, процедур та вимог, що регулюють доступ, використання та захист мобільних пристроїв працівниками організації з метою забезпечення безпеки, конфіденційності та цілісності даних під час їх використання.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Віддаленої Роботи	Teleworking Policy	Набір встановлених правил та вимог, спрямованих на забезпечення безпеки, конфіденційності та продуктивності працівників, які працюють на віддаленій основі, включаючи встановлення технічних засобів, контролю доступу та комунікаційних стандартів.
Політика Захисту Людських Ресурсів	Human Resources Security Policy	Набір встановлених правил, процедур та критеріїв, що визначають процедури для захисту конфіденційної інформації під час найму, роботи та звільнення співробітників, а також встановлює вимоги до керівництва та персоналу щодо безпеки даних.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Класифікації Даних	Information Classification Policy	Набір встановлених правил, процедур та критеріїв, що визначають рівні чутливості інформації, її категоризацію та застосування відповідних заходів забезпечення безпеки для кожної категорії даних.
Політика Управління Активами	Asset Management Policy	Набір встановлених правил, процедур та стратегій, спрямованих на ефективне управління всіма активами організації, включаючи інформаційні ресурси, фізичні ресурси, людські ресурси та інші матеріальні та нематеріальні активи, з метою максимізації їх вартості та захисту від загроз.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Належного Використання Активів	Acceptable Use Policy	Набір встановлених правил, процедур та вимог, спрямованих на забезпечення відповідного, безпечного та ефективного використання всіх ресурсів організації, включаючи інформаційні, фізичні та людські активи, з метою збереження їх цілісності, конфіденційності та доступності.
Політика Контролю Доступу	Access Control Policy	Набір встановлених правил, вимог та технічних заходів, спрямованих на обмеження, моніторинг та керування доступом до інформаційних ресурсів та систем, забезпечення аутентифікації, авторизації та аудиту доступу для забезпечення конфіденційності, цілісності та доступності даних.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Паролів	Password Policy	Набір встановлених правил та вимог щодо створення, використання та управління паролями, спрямованих на забезпечення безпеки інформаційних систем шляхом встановлення відповідних стандартів довжини, складності та частоти зміни паролів.
Політика Шифрування	Encryption Policy	Набір встановлених правил, процедур та вимог, спрямованих на застосування шифрування для захисту конфіденційної інформації під час зберігання, передачі та обробки даних, з метою забезпечення їхньої безпеки та захисту від несанкціонованого доступу.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Фізичної Безпеки	Physical and Environmental Security Policy	Набір встановлених правил, процедур та стратегій, спрямованих на захист фізичних активів, приміщень та обладнання організації від незаконного доступу, крадіжок та інших загроз, що можуть виникнути ззовні та всередині.
Політика Управління Змінами	Change Management Policy	Набір встановлених правил, процедур та практик, спрямованих на систематичне та контрольоване впровадження змін у інформаційних системах, процесах та інфраструктурі організації з метою мінімізації ризиків і забезпечення стабільності та безпеки ділової діяльності.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Резервного Копіювання Даних	Backup Policy	Набір встановлених правил, процедур та стратегій, спрямованих на регулярне та систематичне створення, зберігання та тестування копій важливої інформації для забезпечення можливості відновлення даних в разі аварій, втрати або пошкодження основних джерел даних.
Політика Захисту від Шкідливого Програмного Забезпечення	Malware Protection Policy	Це набір встановлених правил, процедур та технічних заходів, спрямованих на попередження, виявлення та видалення шкідливих програмних засобів, таких як віруси, хробаки та шпигунське програмне забезпечення, для забезпечення безпеки інформаційних систем організації.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Логування і Моніторингу	Logging and Monitoring Policy	Набір встановлених правил, процедур та вимог, спрямованих на систематичний збір, зберігання та аналіз журналів подій і активності в інформаційних системах з метою виявлення вразливостей, аномальних дій та потенційних загроз для забезпечення безпеки інформації.
Політика Встановлення Програмного Забезпечення	Software Installation Policy	Набір встановлених правил, процедур та вимог, що регулюють процес вибору, отримання, встановлення та оновлення програмного забезпечення в організації з метою забезпечення безпеки, ліцензування та сумісності з існуючими системами.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Управління Вразливостями	Vulnerability Management Policy	Набір встановлених правил, процедур та стратегій, спрямованих на ідентифікацію, оцінку, відстеження та виправлення потенційних слабкостей і проблем у безпеці інформаційних систем та інфраструктури організації з метою зниження ризиків та забезпечення відповідності стандартам безпеки.
Політика Захисту Мережі	Network Security Policy	Набір встановлених правил, процедур та технічних заходів, спрямованих на забезпечення безпеки мережевої інфраструктури організації шляхом встановлення правильної конфігурації, моніторингу активності, виявлення та відповіді на загрози, захисту від несанкціонованого доступу та забезпечення надійності мережевого зв'язку.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Використання Інтернету та Електронної Пошти	Internet and Email Usage Policy	Набір встановлених правил, процедур та вимог, що регулюють доступ до Інтернету та використання електронної пошти працівниками організації з метою забезпечення безпеки.
Політика Безпечної Розробки	Secure Development Policy	Набір встановлених правил, процедур та стандартів, спрямованих на інтеграцію безпеки в усі етапи розробки програмного забезпечення з метою запобігання та виявлення потенційних загроз і вразливостей.
Політика Управління Відносинами з Постачальниками	Supplier Relationships Management Policy	Набір встановлених правил, процедур та стратегій, спрямованих на регулювання та оптимізацію взаємодії з постачальниками з метою забезпечення надійності постачання, зменшення ризиків та забезпечення високої якості товарів і послуг.

Продовження таблиці 3.6

Назва документа	**Відповідник англійською мовою**	**Короткий опис**
Політика Реагування на Інциденти	Incident Management Policy	Набір встановлених правил, процедур та стратегій, спрямованих на ефективне виявлення, аналіз, реагування та відновлення після подій, що становлять загрозу безпеці інформації, з метою мінімізації збитків та захисту конфіденційності, цілісності та доступності даних організації.
Політика Забезпечення Безперервності Бізнесу	Business Continuity Management Policy	Набір встановлених стратегій, процедур та планів дій, спрямованих на забезпечення відновлення нормального функціонування організації після виникнення непередбачуваних подій або кризових ситуацій, з метою мінімізації втрат та збереження репутації та стійкості бізнесу.

Наведений перелік політик не є вичерпним, або обов’язковим. Організація сама визначає які документи необхідно розробити і впровадити на основі аналізу контексту, потреб зацікавлених сторін, внутрішніх і

зовнішніх факторів, застосовних ризиків тощо. Разом з тим, запропонований перелік, на основі досліджень і персонального досвіду впровадження стандартів аудиту кібербезпеки, є найпоширенішим і найбільш застосовним у організаціях, які впроваджують процеси інформаційної безпеки і прагнуть досягнення відповідності із провідними стандартами, такими як ISO 27001, NIST SP 800-53 або SOC 2.

У Додатку Д наведено шаблон універсальної Політики Інформаційної Безпеки, який може використовуватися організаціями і ОКІ для створення власного набору внутрішніх політик.

Також у процесі впровадження стандартів аудиту з кібербезпеки виникає потреба створювати іншу документовану інформацію, так звані допоміжні документи (supporting documentation), яка слугує при впровадженні і підтримці стандартів кібербезпеки, вимагається тим чи іншим стандартом, але носить менш сталий і формальний характер, ніж політики.

Прикладами такої документації можуть бути наступні документи:

- Положення про застосування (притаманно для ISO 27001)
- Перелік документованої інформації
- Контакти з групами по інтересам
- Контакти з регуляторними організаціями
- Реєстр активів
- Реєстр ризиків
- Програма навчання і підвищення свідомості
- Журнал дисциплінарних дій
- Журнал інцидентів
- Перелік постачальників
- Результати оцінки постачальників і провайдерів послуг тощо.

3.5.2 Розроблення методології створення політик інформаційної безпеки

У розділі 2.2 дисертації наведено методологію створення перехресного зіставлення між стандартами аудиту з кібербезпеки. Ця методологія дозволяє встановити відповідність між контролями безпеки, що визначені в різних стандартах та рекомендованими документами, де організація може регламентувати ці контролі. Таким чином, у колонці «Відповідна політика інформаційної безпеки» міститься назва документу, який може бути створений для документування вимог стандартів аудиту у формі організаційних політик.

Нижче представлено методологію створення політик інформаційної безпеки на основі зіставлення контролів стандартів аудиту з кібербезпеки (Рисунок 3.9).

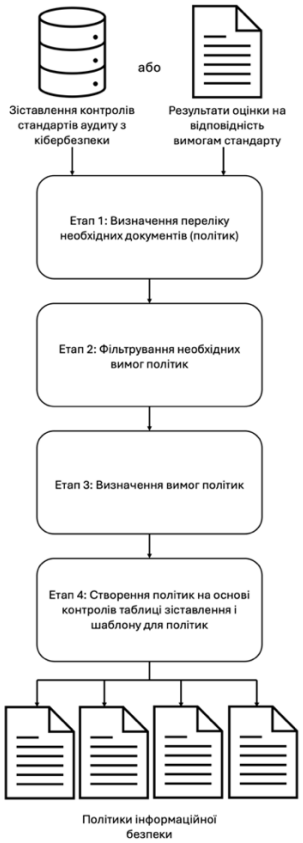


Рис. 3.9. Методологія створення політик інформаційної безпеки

Вхідними даними для розробки політик інформаційної безпеки є таблиця із зіставленням контролів стандартів аудиту з кібербезпеки. Після визначення застосовних стандартів аудиту, організація отримує перелік застосовних контролів безпеки з цих стандартів, які поділені по доменам. Це дозволяє чітко встановити області, на яких потрібно зосередитися при розробці політик безпеки. Такий підхід допомагає систематизувати та організувати процес розробки політик, забезпечуючи повноту та відповідність вимогам інформаційної безпеки.

Перший етап методології полягає в тому, щоб організація визначила перелік необхідних політик інформаційної безпеки. Цей перелік формується на основі результатів оцінки на відповідність та/або за допомогою таблиці з перехресним зіставленням контролів. У цій таблиці (Рисунок 2.2) колонка «Відповідна політика інформаційної безпеки» вказує, куди варто включити тематичні вимоги стандарту(-ів).

Другий етап передбачає фільтрацію за назвою політики, щоб вибрати лише ті контролі та вимоги, які необхідно включити в конкретну політику. Це допомагає забезпечити зосередженість на конкретних вимогах кожного стандарту.

На **третьому етапі** формується перелік відфільтрованих елементів, які будуть визначати вимоги і рекомендації для конкретної політики. На цьому етапі необхідно провести огляд визначених вимог і виключити ті, які не застосовні до організації.

На **четвертому етапі** безпосередньо переносяться вимоги і рекомендації у шаблон політики (див. Додаток Г).

Другий, третій і четвертий етапи повторюються для кожного документа, що створюється для організації.

Таким чином, запропонована методологія дозволяє швидко і ефективно створити політики інформаційної безпеки для відповідності основним

стандартам аудиту з кібербезпеки, таким як ISO 27001, SOC 2, NIST 800-53 і PCI DSS.

3.6 Висновки до третього розділу

У третьому розділі розроблено універсальний метод для оцінки захищеності ОКІ та перевірки стану його відповідності стандартам аудиту з кібербезпеки, розроблено методологію перехресного впровадження стандартів аудиту на основі зіставлення їхніх контролів безпеки, а також представлено методологію створення організаційних політик інформаційної безпеки ОКІ на основі зведеної таблиці із зіставленням контролів безпеки.

Зокрема, проведене дослідження дозволяє виділити наступне:

1. Дослідження основних підходів до впровадження стандартів аудиту з кібербезпеки показали, що підхід «Орієнтація на відповідність і безпеку» є цілісним і ефективним з погляду забезпечення необхідного рівня інформаційної безпеки в організації чи ОКІ, оскільки бере до уваги контекст організації, її бізнес цілі, потреби зацікавлених сторін, спирається на результати оцінки на відповідність і оцінки ризиків, і ґрунтується на використанні визнаних стандартів аудиту з кібербезпеки.

2. Розроблено метод оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні контрольного списка, який містить детальний перелік запитань і перевірок для визначення статусу відповідності контролям безпеки, а також перелік доказів і документів, необхідних для досягнення відповідності. Розроблений метод забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки і, завдяки розробленим в контрольному списку практичним рекомендаціям по впровадження стандарту ISO 27001, скорочує час на впровадження стандарту.

3. Розроблено методологію визначення і оцінки ризиків інформаційної безпеки організацій та ОКІ. Дана методологія, а також розроблений у її рамках універсальний шаблон для ідентифікації і управління ризиками, дозволяє адаптувати їх під потреби різних організацій та ОКІ і досягти відповідності провідним стандартам аудиту з кібербезпеки, таким як ISO 27001, SOC 2, NIST чи PCI DSS, без залучення спеціалістів з інформаційної безпеки.

4. На основі проведеного дослідження провідних стандартів, розроблено методологію перехресного впровадження стандартів аудиту з кібербезпеки на основі застосування зіставлення між їхніми контролями безпеки. Використаний метод зіставлення не лише встановлює відповідність між контролями, але й враховує додаткові рекомендації щодо впровадження конкретних вимог, що робить його комплексним та ефективним у порівнянні з існуючими методами.

5. Розроблено методологію створення політик інформаційної безпеки ОКІ на основі зведеної таблиці із зіставленням контролів безпеки провідних стандартів, таких як ISO 27001, SOC 2, NIST 800-53 і PCI DSS. Ця методологія підвищує ефективність захищеності ОКІ від загроз за рахунок автоматизації і пришвидшення процесу створення політик інформаційної безпеки з забезпеченням покриття усіх найважливіших доменів і контролів безпеки.

РОЗДІЛ 4. РОЗРОБЛЕННЯ СИСТЕМИ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ ЙОГО ВІДПОВІДНОСТІ СТАНДАРТАМ КІБЕРБЕЗПЕКИ

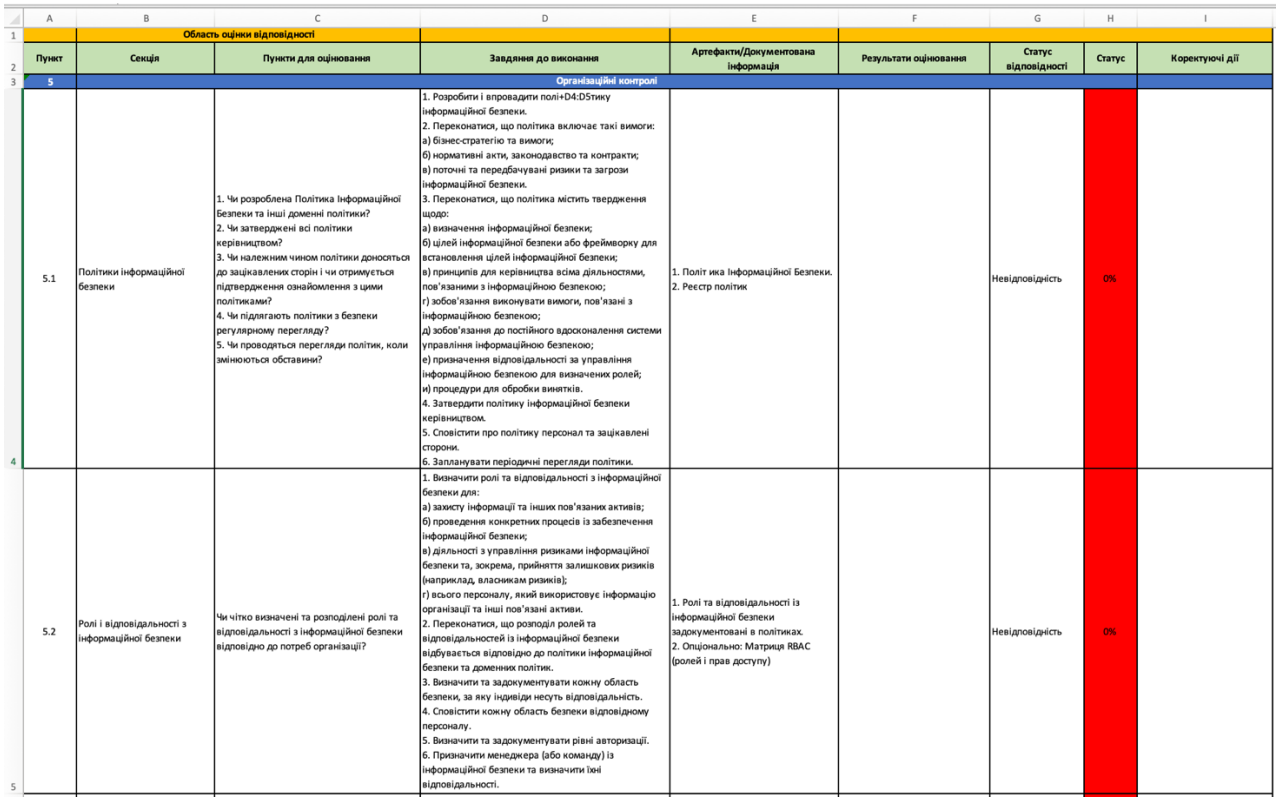
4.1 Розроблення форми оцінювання СУІБ ОКІ на відповідність стандартам аудиту з кібербезпеки

На основі проведеного дослідження основних підходів до забезпечення інформаційної безпеки, встановлено, що першочерговим етапом при впровадженні будь-якого стандарту аудиту з кібербезпеки є аналіз поточного стану організації на відповідність відповідному стандарту з метою виявлення невідповідностей і розробки рекомендацій по досягненню відповідності.

За основу запропонованого методу оцінки на відповідність взято стандарт ISO 27001, зокрема через наступні міркування:

- Він є одним з найпоширеніших стандартів інформаційної безпеки в світі.
- Його значна популярність в Україні, як в державному так і приватному секторі.
- Оскільки стандарт є досить широким і всеосяжним, він покриває більшість спеціалізованих доменів безпеки і включає технічні, фізичні і адміністративні контролі.
- Завдяки своїй ширині покриття, він добре зіставляється із іншими стандартами інформаційної безпеки, такими як NIST SP 800-53, SOC 2, PCI DSS тощо.

Нижче наведено приклад форми оцінювання у вигляді контрольного списка, який використовується для оцінки організацій на відповідність міжнародному стандарту ISO 27001 (Рисунок 4.1).



Область оцінки відповідності								
Пункт	Секція	Пункти для оцінювання	Завдання до виконання	Артефакти/Документована інформація	Результати оцінювання	Статус відповідності	Статус	Коректуючі дії
5			Організаційні контролі					
5.1	Політики інформаційної безпеки	1. Чи розроблена Політика інформаційної безпеки та інші доменні політики? 2. Чи затверджені всі політики керівництвом? 3. Чи належним чином політики доносяться до зацікавлених сторін і чи отримується підтвердження ознайомлення з цими політиками? 4. Чи підлягають політики з безпеки регулярному перегляду? 5. Чи проводяться перегляди політик, коли змінюються обставини?	1. Розробити і впровадити полі+D4:D5тику інформаційної безпеки. 2. Переконатися, що політика включає такі вимоги: а) бізнес-стратегію та вимоги; б) нормативні акти, законодавство та контракти; в) поточні та передбачувані ризики та загрози інформаційної безпеки. 3. Переконатися, що політика містить твердження щодо: а) визначення інформаційної безпеки; б) цілей інформаційної безпеки або фреймворку для встановлення цілей інформаційної безпеки; в) принципів для керівництва всіма діяльностями, пов'язаними з інформаційною безпекою; г) зобов'язання виконувати вимоги, пов'язані з інформаційною безпекою; д) зобов'язання до постійного вдосконалення системи управління інформаційною безпекою; е) призначення відповідальності за управління інформаційною безпекою для визначених ролей; и) процедури для обробки виняткв. 4. Затвердити політику інформаційної безпеки керівництвом. 5. Сповістити про політику персонал та зацікавлені сторони. 6. Запланувати періодичні перегляди політики.	1. Політ ика Інформаційної Безпеки. 2. Реєстр політик		Невідповідність	0%	
5.2	Ролі і відповідальності з інформаційної безпеки	Чи чітко визначені та розподілені ролі та відповідальності з інформаційної безпеки відповідно до потреб організації?	1. Визначити ролі та відповідальності з інформаційної безпеки для: а) захисту інформації та інших пов'язаних активів; б) проведення конкретних процесів із забезпечення інформаційної безпеки; в) діяльності з управління ризиками інформаційної безпеки та, зокрема, прийняття залишкових ризиків (наприклад, власникам ризиків); г) всього персоналу, який використовує інформацію організації та інші пов'язані активи. 2. Переконатися, що розподіл ролей та відповідальностей із інформаційної безпеки відбувається відповідно до політики інформаційної безпеки та доменних політик. 3. Визначити та задокументувати кожну область безпеки, за яку індивіди несуть відповідальність. 4. Сповістити кожну область безпеки відповідному персоналу. 5. Визначити та задокументувати рівні авторизації. 6. Призначити менеджера (або команду) із інформаційної безпеки та визначити їхні відповідальності.	1. Ролі та відповідальності із інформаційної безпеки задокументовані в політиках. 2. Опціонально: Матриця RBAC (ролей і прав доступу)		Невідповідність	0%	

Рис. 4.1. Контрольний список для проведення оцінки на невідповідність згідно вимог стандарту ISO 27001

Даний контрольний список містить наступні секції [102]:

- **Пункт** – числове позначення, яке відповідає конкретному розділу або пункту стандарту. Використовується для швидкої навігації під час оцінювання відповідності.
- **Секція** – назва розділу або підрозділу стандарту, який визначає конкретну тему або область вимог.
- **Пункти для оцінювання** – перелік конкретних вимог стандарту, які підлягають перевірці під час оцінювання відповідності. Вони слугують основою для проведення оцінювання.
- **Завдання для виконання** – перелік конкретних дій або завдань, які потрібно виконати для того, щоб забезпечити відповідність вимогам

стандарту. Вони можуть включати розробку, реалізацію та впровадження практик або процедур.

- **Артефакти/Документована інформація** – додаткові документи, файли, записи або матеріали, які можуть служити доказами виконання вимог стандарту. Вони підтримують доказову базу в процесі оцінювання.
- **Результати оцінювання** – ця секція заповнюється аудитором або оцінювачем під час проведення оцінювання відповідності. Вона містить оцінку того, наскільки наявні контролі і практики відповідають вимогам стандарту.
- **Статус відповідності** – цей статус визначає, наскільки наявні контролі і практики відповідають вимогам стандарту. Він може бути «Відповідає», «Не відповідає» або «Частково відповідає», вказуючи на рівень відповідності.
- **Статус** – цей показник визначає відсоток виконання вимог стандарту відносно загальної кількості вимог.
- **Коректуючі дії** – перелік дій і активностей, які необхідно реалізувати для досягнення повної відповідності до вимог стандарту. Ці дії спрямовані на усунення виявлених невідповідностей та вдосконалення системи управління інформаційною безпекою.

Таким чином, процес проведення оцінки на відповідність за допомогою контрольного списка є структурованим та організованим підходом для перевірки рівня відповідності організації та ОКІ до конкретних вимог стандарту, такого як ISO 27001. Цей процес включає кілька кроків, що допомагають ідентифікувати розриви між поточними практиками організації та вимогами стандарту. Оцінка на відповідність за допомогою контрольного списка може бути виконана внутрішньою або зовнішньою командою та є важливою частиною процесу впровадження стандарту.

4.2 Наповнення системи і тестування взаємодії компонентів системи між собою

У результаті об'єднання розроблених методів і методологій, утворюється уніфікована система для впровадження стандартів аудиту з кібербезпеки в об'єктах критичної інфраструктури.

Основними елементами, які включає система є:

- Контрольний список для проведення оцінки СУІБ на відповідність стандарту ISO 27001 (Додаток В).
- Шаблон і довідкова інформація для проведення оцінки ризиків інформаційної безпеки (Додаток Г).
- Таблиця із перехресним зіставленням контролів провідних стандартів аудиту з кібербезпеки.
- Набір контролів для виконання вимог.
- Універсальна Політика інформаційної безпеки, яка описує вимоги до основних процесів інформаційної безпеки (Додаток Д).

Дані елементи оформлені як додатки до дисертаційного дослідження, і з ними можна ознайомитися в секції Додатки.

4.3 Визначення ефективності роботи методології впровадження стандартів аудиту з кібербезпеки та її переваг над сучасними аналогами

Ефективність роботи методології перехресного впровадження стандартів аудиту з кібербезпеки можна визначити, оцінивши і проаналізувавши наступні показники:

1. Ступінь перехресного покриття контролів між стандартом ISO 27001, який взято за основу розробленої методології, та іншими популярними стандартами аудиту кібербезпеки.

2. Середній час впровадження стандарту кібербезпеки в організації за умови використання розробленої методології у порівнянні із часом на впровадження без неї.

3. Якісне порівняння розробленої методології із аналогічними рішеннями конкурентів на основі персонального досвіду автора.

Щодо **першого показника** – ступеня перехресного покриття контролів, то ця інформація показує, яку частину унікальних контролів стандарту аудиту з кібербезпеки організація вже покрила, маючи впровадженим інший стандарт аудиту. У нашому випадку, ми оцінюємо, яку частину контролів з популярних стандартів аудиту ми перекриваємо, маючи впровадженим стандарт ISO 27001. Дана інформація може бути прорахована для наступних стандартів, які включені в таблицю перехресного зіставлення контролів:

- NIST SP 800-53
- SOC 2 (Trust Services Criteria)
- PCI DSS v.3.2.1
- PCI DSS v.4.0

На рисунку нижче (Рисунок 4.2) у вигляді кругової діаграми зображено перекриття між стандартом ISO 27001 і дослідженими стандартами у відсотковому відношенні.

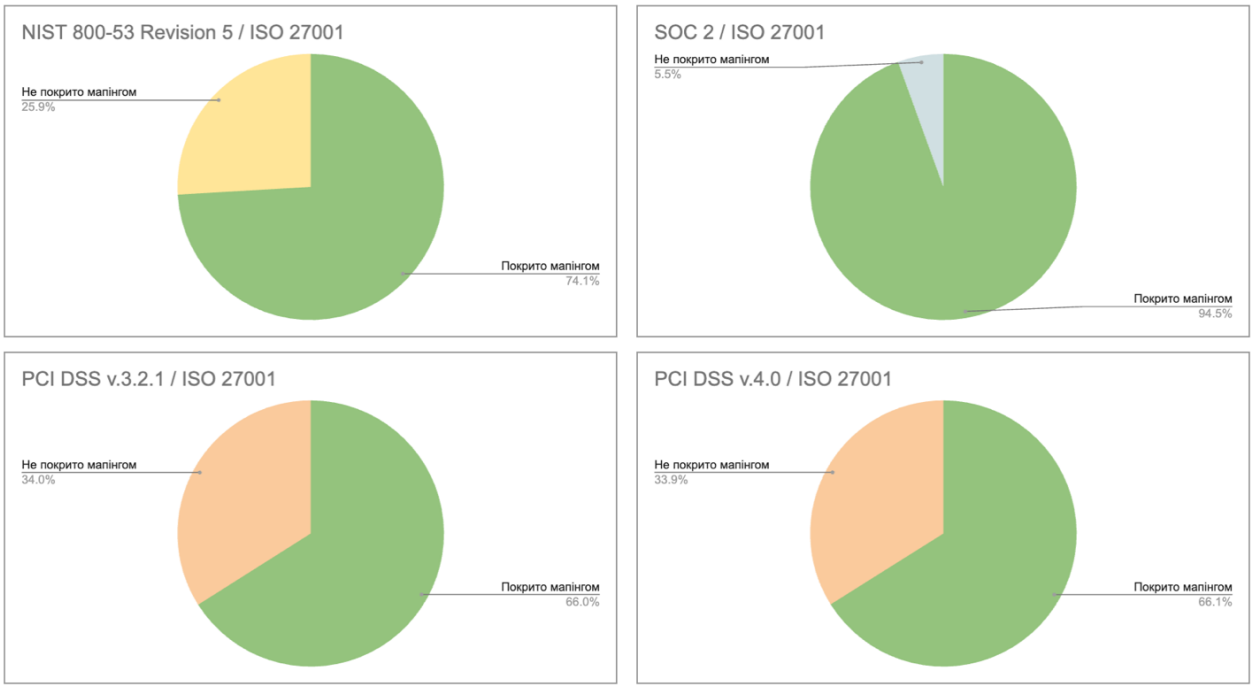


Рис. 4.2. Ступінь перехресного покриття контролів безпеки між стандартом ISO 27001 та іншими провідними стандартами аудиту з кібербезпеки

Як видно з рисунку 4.2, найбільший ступінь покриття має стандарт SOC 2 – 94.5%. Це означає, що вимоги стандарту ISO 27001 на 94.5% відповідають вимогам стандарту SOC 2. Тобто, якщо організація вже впровадила стандарт ISO 27001 і вирішує сертифікуватися також по стандарту SOC 2, їй залишиться впровадити приблизно 5.5% контролів стандарту SOC 2. Якщо детальніше розглянути не покриті у результаті зіставлення контролі, то ми побачимо, що основна їхня кількість відноситься до принципів Цілісність обробки (Processing Integrity) і Приватність (Privacy). Це не дивно, оскільки ці два принципи є досить специфічними, і не достатньо детально розглядаються в стандарті ISO 27001.

На другому місці по ступеню перекриття контролів знаходиться стандарт NIST SP 800-53. За даними аналізу, впровадивши стандарт ISO 27001, компанія зможе перекрити близько 74.1% контролів стандарту NIST

SP 800-53. Відповідно, залишиться впровадити близько 25.9% контролів стандарту NIST SP 800-53 для того, щоб повністю відповідати обом стандартам одночасно. Таке відсоткове відношення пов’язане з тим, що обидва стандарти є досить широкими і покривають найважливіші домени інформаційної безпеки, але NIST SP 800-53 своєю чергою є більш охоплюючим, містить більшу кількість контролів безпеки і їхню більшу деталізацію.

І наостанок, дещо нижчий відсоток перехресної відповідності мають стандарти захисту даних власників карток PCI DSS v.3.2.1 і PCI DSS v.4.0 – 66% і 66.1% відповідно. Це пов’язано з тим, що багато контролів в стандарті PCI DSS мають специфічну сферу застосування, як наприклад, захист даних власників карток, або безпека POS-терміналів тощо. Також певна частина контролів застосовна тільки для хостинг провайдерів або інших специфічних для галузі провайдерів послуг, тому ці контролі також не перекриваються зіставленням.

Результати розрахунку перекриття між стандартами узагальнено в Таблиці 4.1.

Таблиця 4.1

Відповідність між контролями стандартів аудиту з кібербезпеки

Перекриття між стандартами	Відсоток перекриття	Відсоток унікальних неперекритих контролів
NIST SP 800-53 / ISO 27001:2022	74,1%	25,9%
SOC 2 / ISO 27001:2022	94,5%	5,5%

Продовження таблиці 4.1

Перекриття між стандартами	Відсоток перекриття	Відсоток унікальних неперекритих контролів
PCI DSS v.3.2.1 / ISO 27001:2022	66%	34%
PCI DSS v.4.0 / ISO 27001:2022	66,1%	33,9%

Для оцінки **другого показника**, а саме часу впровадження стандарту кібербезпеки в організації за умови використання розробленої методології, то його можна оцінити на основі даних отриманих при впровадженні практичних результатів дисертаційного дослідження в роботу організацій (Таблиця 4.2).

Таблиця 4.2

Показники впровадження стандартів аудиту в організаціях

	ТОВ «Бінарікс Україна»	ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ»	ТОВ «ПІК РІСОРСИС»	Міжнародна маркетингова компанія (NDA)	Компанія по розробці програмного забезпечення (NDA)
К-сть працівників	~150	~100	~250	~400	~150
Стандарти	ISO 27001, ISO 9001	SOC 2	ISO 27001	ISO 27001	ISO 27001, ISO 9001

Продовження таблиці 4.2

	ТОВ «Бінарікс Україна»	ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ»	ТОВ «ПІК РІСОРСИС»	Міжнародна маркетингова компанія (NDA)	Компанія по розробці програмного забезпечення (NDA)
Час впровадження *(Середній показник без методології – 8 міс.)*	7 міс.	4 міс.	5 міс.	5 міс.	6 міс.
Зменшення часу	12% (але для двох стандартів)	50%	37%	37%	25% (але для двох стандартів)

Зокрема, актами впровадження (Додаток А) підтверджено впровадження практичних результатів дисертаційної роботи в діяльності підприємств ТОВ «Бінарікс Україна», ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ», і ТОВ «ПІК РІСОРСИС». Для розрахунку даного показника ефективності також взято до уваги дані про впровадження стандартів аудиту з кібербезпеки у ще двох організаціях, назви яких не розголошується через обмеження, накладені діючими угодами про нерозголошення конфіденційної інформації. Варто відзначити, що оцінювати ефективність виконання таких складних і об’ємних проектів, як впровадження стандарту досить складно через велику кількість факторів, таких як контекст і галузь в якій працює організація, кількість і складність її бізнес процесів, залучення керівництва, наявність ресурсів, чи навіть пріоритетність і критичність впровадження

процесів та контролів. Проте, на основі значного досвіду впровадження стандартів аудиту кібербезпеки, можна зробити наступні висновки:

- Фаза оцінки на відповідність в середньому триває до 4 тижнів.
- Наявність шаблонів політик і довідкової інформації для впровадження контролів сприяють досить значному скороченню часу на впровадження документації і процесів інформаційної безпеки. Виграш у часі впровадження становить приблизно 30-50%. Для оцінки цього показника було взято для порівняння час на впровадження контролів для відповідності стандарту SOC 2 у двох різних організаціях – в одній без використання запропонованої методології, і в іншій – з її використанням. Відповідно часові рамки для впровадження стандарту становили 8 місяців у першому випадку, і 4 – в другому. Як уже сказано, співвідносити ці два показники не зовсім коректно через різницю в специфіці організацій, але загалом, на основі цих цифр можна зробити припущення, що впровадження за допомогою розробленої методології є ефективнішим з погляду затраченого часу у порівнянні з підходом без неї.
- Використання перехресного зіставлення допомагає значно скоротити час впровадження додаткового стандарту аудиту з кібербезпеки. Це підтверджено безпосереднім досвідом автора дисертації, відповідно до якого, впровадження додаткових контролів для досягнення відповідності стандарту SOC 2 з попередньо впровадженим стандартом ISO 27001 зайняло до 6 тижнів, в порівнянні із середнім показником 4-6 місяців для впровадження цього ж стандарту «з нуля».

Також важливо зазначити, що хоча впровадження стандартів аудиту відбувалося у комерційних приватних організаціях, завдяки універсальності розробленої методології, процес і часові рамки впровадження на ОКІ не повинні містити значних розбіжностей.

Наостанок, у рамках аналізу **третього показника**, наведено певні висновки щодо порівняння запропонованої методології перехресного впровадження стандартів аудиту з кібербезпеки з комерційними аналогами, що існують на світовому ринку. Варто зазначити, що дане порівняння носить якісний характер і ґрунтується на власному досвіді автора по розробці і використанню цих систем (Таблиця 4.3).

Таблиця 4.3

Основні недоліки альтернативних комерційних систем для впровадження стандартів аудиту кібербезпеки

Назва системи	**Недоліки**
Vanta	Відсутність функціоналу для початкової оцінки стану системи безпеки і визначення невідповідностей. Занадто загальні шаблони політик. Неефективний модуль управління ризиками.
Drata	Відсутність функціоналу для початкової оцінки стану системи безпеки і визначення невідповідностей. Обмеження щодо охоплення ширшого спектру стандартів відповідності, окрім SOC 2.

Продовження таблиці 4.3

Назва системи	Недоліки
LogicGate	Відсутність функціоналу для початкової оцінки стану системи безпеки і визначення невідповідностей. Складність конфігурації та налаштування, що вимагає досвіду для повної оптимізації можливостей системи.

Як видно з таблиці 4.3, спільним недоліком проаналізованих систем є відсутність чіткого функціоналу для проведення оцінки на відповідність. Як наслідок, впровадження стандартів аудиту з кібербезпеки з використанням цих систем може зайняти більше часу, оскільки на початковому етапі впровадження вони не беруть до уваги специфічні потреби і наявний стан контролів організації чи ОКІ. До інших недоліків можна віднести певну обмеженість покриття стандартів, а також складність у налаштуванні.

Загалом, аналіз цих трьох показників допомагає зрозуміти перспективність і ефективність розробленої методології перехресного впровадження стандартів аудиту з кібербезпеки та які переваги вона може принести в організації і ОКІ порівняно з іншими методами та засобами.

4.4 Висновки до четвертого розділу

У четвертому розділі представлено метод для оцінки організації на відповідність стандарту ISO 27001 та впровадження стандартів аудиту кібербезпеки. Також у розділі проведено оцінку ступеня перехресного покриття стандартів кібербезпеки та оцінено ефективність застосування розробленої методології перехресного впровадження стандартів.

1. На основі дослідження і аналізу існуючих методів впровадження стандартів аудиту з кібербезпеки розроблено метод оцінки відповідності СУІБ ОКІ вимогам стандарту ISO 27001. Цей метод базується на використанні детальної форми оцінювання у вигляді контрольного списка, яка дозволяє систематично перевірити відповідність між актуальним станом інформаційної безпеки та бажаним еталонним станом, який відповідає вимогам стандарту ISO 27001. Контрольний список, розроблений у рамках цього методу, включає в себе детальні пункти оцінки, що охоплюють всі аспекти інформаційної безпеки в організації. Він забезпечує можливість систематичної перевірки відповідності з різними доменами стандарту ISO 27001, такими як політики безпеки, управління доступом, фізична безпека, безпека персоналу, управління ризиками, захист інформації та інші. Таким чином, даний метод надає структурований підхід до оцінки відповідності стандарту ISO 27001 і дозволяє ОКІ ефективно визначати та усувати будь-які невідповідності.

2. Розроблені в рамках перехресного зіставлення контролів безпеки стандартів рекомендації по впровадженню ISO 27001 також корелюються із вимогами інших стандартів аудиту кібербезпеки, такими як SOC 2, NIST 800-53 і PCI DSS, що дозволяє ОКІ не лише досягати відповідності ISO 27001, але й використовувати цей процес для забезпечення вищого ступеня захисту. Такий підхід дозволяє не тільки забезпечити відповідність з одним конкретним стандартом, але і використовувати цей процес для покращення загального рівня кібербезпеки та захисту.

3. Проведено оцінку ефективності роботи запропонованої методології перехресного впровадження стандартів аудиту з кібербезпеки на основі оцінки і аналізу ступеня перехресного покриття контролів між стандартом ISO 27001 та іншими провідними стандартами аудиту з кібербезпеки, середньої тривалості впровадження стандартів кібербезпеки та якісного

порівняння розробленої методології з аналогічними рішеннями конкурентів. На основі проведеного зіставлення контролів безпеки, визначено, що при впровадженні стандарту ISO 27001:2022, ОКІ покриває в середньому від 66% до 94% контролів інших досліджених стандартів. Також, в результаті оцінки тривалості впровадження стандартів, визначено, що запропонована методологія дає змогу впроваджувати стандарти аудиту з кібербезпеки ефективніше та до 50% швидше в порівнянні з традиційними методами.

ВИСНОВКИ

У даній дисертаційній роботі вирішено важливе науково-практичне завдання з підвищення рівня захищеності об'єктів критичної інфраструктури від кіберзагроз за рахунок використання методології перехресного впровадження стандартів аудиту з кібербезпеки. Ця методологія підвищує рівень інформаційної безпеки та захищеності ОКІ, а також зменшує час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки одночасно.

1. Проведений аналіз кібератак на ОКІ, демонструє важливість їхнього належного захисту у зв'язку зі стрімким розвитком інформаційних технологій, масовим переходом до режиму віддаленої роботи та збройною військовою агресією росії проти України. Виявлено, що багато атак було успішно реалізовано через відсутність базових процесів інформаційної безпеки, таких як управління інформаційною безпекою у відносинах з постачальниками, систематичне оновлення програмного забезпечення та недостатнє підвищення обізнаності щодо інформаційної безпеки серед персоналу. Зазначені процеси регулюються провідними стандартами аудиту з кібербезпеки, такими як ISO 27001, SOC 2, NIST 800-53 та PCI DSS. Відповідно, впровадження цих стандартів аудиту здатне значно зменшити ризики та втрати внаслідок кібератак, оскільки надають спільне розуміння для розробки програми кібербезпеки та пропонують організаціям структурований підхід до впровадження політик, процедур та технологій, спрямованих на забезпечення безпеки.

2. На основі проведених досліджень особливостей застосування і впровадження провідних стандартів аудиту з кібербезпеки, таких як ISO 27001, SOC 2, NIST 800-53 і PCI DSS, доведено доцільність і ефективність застосування перехресного впровадження стандартів аудиту з кібербезпеки,

що дозволить забезпечити повне охоплення контролів безпеки та підвищити рівень захисту ОКІ порівняно з будь-яким окремим стандартом.

3. У результаті порівняльної оцінки редакцій стандарту ISO 27001, розроблено таблицю відповідності між контролями Додатку А двох останніх редакцій стандарту ISO 27001 – 2013 і 2022 років. Використання розробленої таблиці відповідності скорочує час і ресурси необхідні для впровадження оновленої версії стандарту та приведення СУІБ до відповідності новим вимогам безпеки.

4. Розроблено методологію перехресного впровадження стандартів аудиту з кібербезпеки на основі застосування зіставлення між їхніми контролями безпеки. Розроблений метод зіставлення не лише встановлює відповідність між контролями, але й враховує додаткові рекомендації щодо впровадження конкретних вимог, що підвищує ефективність захисту ОКІ за рахунок комплексного охоплення контролів інформаційної безпеки.

5. Розроблено метод оцінки СУІБ ОКІ на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні форми оцінювання у вигляді контрольного списка, яка містить детальний перелік запитань і перевірок для визначення статусу відповідності контролям безпеки, а також перелік доказів і документів, необхідних для досягнення відповідності. Розроблений метод забезпечує систематичний і уніфікований підхід до проведення оцінки СУІБ ОКІ, повноту охоплення контролів безпеки і, завдяки розробленим в контрольному списку практичним рекомендаціям по впровадження стандарту ISO 27001, скорочує час на впровадження стандарту.

6. Розроблено методологію визначення і оцінки ризиків інформаційної безпеки організацій та ОКІ. Дана методологія, а також розроблений у її рамках універсальний шаблон для ідентифікації і управління ризиками, дозволяє адаптувати їх під потреби різних організацій та ОКІ, і досягти

відповідності провідним стандартам аудиту з кібербезпеки, таким як ISO 27001, SOC 2, NIST чи PCI DSS, без залучення спеціалістів з інформаційної безпеки.

7. Розроблено методологію створення політик інформаційної безпеки об’єкта критичної інфраструктури на основі зведеної таблиці із зіставленням контролів безпеки провідних стандартів, таких як ISO 27001, SOC 2, NIST 800-53 і PCI DSS. Дана методологія підвищує ефективність захищеності ОКІ від загроз за рахунок автоматизації і пришвидшення процесу створення політик інформаційної безпеки з забезпеченням покриття усіх найважливіших доменів і контролів безпеки.

8. Експериментальним шляхом визначено, що у результаті зіставлення контролів безпеки, при впровадженні стандарту ISO 27001:2022, організація покриває в середньому від 66% до 94% контролів інших досліджених провідних стандартів, що зменшує час і ресурси для досягнення відповідності декільком стандартам аудиту з кібербезпеки одночасно.

9. У результаті порівняльної оцінки тривалості впровадження стандартів, визначено, що запропонована методологія перехресного впровадження стандартів аудиту з кібербезпеки дає змогу впроваджувати стандарти аудиту до 50% швидше в порівнянні з традиційними методами, тим самим забезпечуючи більшу ефективність у створенні універсальної СУІБ ОКІ, що покриває вимоги декількох стандартів аудиту одночасно.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Modeling of security systems for critical infrastructure facilities/ Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych, Ivan Opirskyy and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

2. Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32;

3. Cybersecurity Framework: Types, Components, Functions. [Електронний ресурс] – Режим доступу до ресурсу: https://www.knowledgehut.com/blog/security/cyber-security-frameworks

4. Tom Conkle, Greg Witte, Improving cybersecurity through the use of the cybersecurity framework (2015) 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2015, Volume 3, Pages 2479 – 2486

5. Hamed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview (2022). DOI: 10.3390/electronics11142181

6. M. Syafrizal, S. R. Selamat, N. A. Zakaria, Analysis of cybersecuritystandard and framework components, International Journal of Communi-cation Networks and Information Security 12 (3) (2020) 417–432

7. Cybersecurity compliance: everything you need to know. [Електронний ресурс] – Режим доступу до ресурсу: https://nordlayer.com/learn/regulatory-compliance/cybersecurity-compliance/?gad_source=1&gclid=Cj0KCQjwn7mwBhCiARIsAGoxjaJuB0qBHshTHC_9xCaOAgOWuYiLpDurvGl0gO8DNcF903OyXXHNz0kaAox5EALw_wcB

8. Key benefits of ISO 27001. [Електронний ресурс] – Режим доступу до ресурсу: https://www.itgovernance.co.uk/iso27001-benefits#:~:text=ISO%2027001%20compliance%20helps%20you,your%20claims%20are%20backed%20up.

9. Susukailo V., Opirsky I., Yaremko O. (2022) Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. Springer, Cham. DOI: 10.1007/978-3-030-92435-5_15

10. Курій Є. О., Опірський І. Р. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ ФРЕЙМВОРКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 85): матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 15-16 лютого 2024 р.). – 2024. – С. 34–36.

11. Compliance vs. Security: Striking the Right Balance in Cybersecurity. [Електронний ресурс] – Режим доступу до ресурсу: https://www.tripwire.com/state-of-security/compliance-vs-security-striking-right-balance-cybersecurity#:~:text=The%20difference%20is%20subtle%20but,for%20the%20two%20to%20clash.

12. What Are The ISO 27001 Changes In 2022. [Електронний ресурс] – Режим доступу до ресурсу: https://bestpractice.biz/what-are-the-iso-27001-changes-in-2022/ (Accessed: 15 March 2024).

13. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] / Закон України від 5 жовтня 2017 р.№ 2163-VIII. // Офіційний сайт Верховної Ради України «Законодавство України». – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

14. Кібервійна росії проти України. [Електронний ресурс] – Режим доступу до ресурсу: https://speka.media/kiberviina-rosiyi-proti-ukrayini-9qy4ok

15. Цяпа С. М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України. Інформація і Право. 2021. № 4(39). С. 121–128. DOI: 10.37750/2616-6798.2021.4(39).248832.

16. Putro P.A.W., Sensuse D.I., Wibowo W.S.S. Framework for critical information infrastructure protection in smart government: a case study in Indonesia (2024) Information and Computer Security, 32 (1), pp. 112 - 129, DOI: 10.1108/ICS-03-2023-0031. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85170395135&doi=10.1108%2fICS-03-2023-0031&partnerID=40&md5=16da142372b05c0e9560ce26e4968d1c

17. Czuryk, Małgorzata. (2023). Cybersecurity and Protection of Critical Infrastructure. Studia Iuridica Lublinensia. 32. 43-52. 10.17951/sil.2023.32.5.43-52.

18. The ISO Survey. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/the-iso-survey.html

19. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (із змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку від 10.07.2022 № 343) [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601

20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19 червня 2019 р. № 518.

Дата оновлення: 7.09.2022. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

21. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р.№ 2163-VIII. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

22. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882- IX. Дата оновлення: 15.06.2022. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20#Text

23. Стратегія кібербезпеки України: затверджено Указом Президента України від 14 травня 2021 №447/2021 / офіційний сайт Президента України. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

24. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 6–20.doi: https://doi.org/10.15587/1729-4061.2023.273363

25. Хакерська атака Росії на українську енергосистему: як це було? [Електронний ресурс] – Режим доступу до ресурсу: https://texty.org.ua/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/

26. New wave of cyberattacks against Ukrainian power industry | WeLiveSecurity. [Електронний ресурс] – Режим доступу до ресурсу: https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

27. Нерассказанная история NotPetya – самой разрушительной кибератаки в истории. [Електронний ресурс] – Режим доступу до ресурсу: https://ain.ua/ru/2018/08/24/notpetya-istoriya/ (дата звернення: 13.05.2023).

28. Три года NotPetya. Как это было и готова ли Украина к новым атакам. [Електронний ресурс] – Режим доступу до ресурсу: https://project.liga.net/projects/notpetya_3years/

29. Хакери змогли зламати 70 урядових сайтів, зокрема сайт "Дії". Як це вдалося. [Електронний ресурс] – Режим доступу до ресурсу: https://tech.liga.net/ua/ukraine/article/kak-hakery-smogli-vzlomat-70-pravitelstvennyh-saytov-i-kto-za-etim-mojet-stoyat

30. 10 cybersecurity frameworks you need to know about. [Електронний ресурс] – Режим доступу до ресурсу: https://www.helpnetsecurity.com/2024/01/16/cybersecurity-frameworks/

31. NIST Cybersecurity Framework vs ISO 27001/27002 vs NIST 800-53 vs Secure Controls Framework. [Електронний ресурс] – Режим доступу до ресурсу: https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf

32. Zahoor Ahmed, Soomro Mahmood, Hussain Shah, Javed Ahmed, Information security management needs more holistic approach: A literature review (2016). https://doi.org/10.1016/j.ijinfomgt.2015.11.009

33. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard/82875.html

34. (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard/75652.html

35. (2020) Security and Privacy Controls for Information Systems and Organizations Special Publication (SP) 800-53 Rev 5, U.S. Department of Commerce, 2020, [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

36. Overview Of The Nist Cybersecurity Framework, May 2018. [Електронний ресурс] – Режим доступу до ресурсу: https://1path2020b.websitetotalcare.com/blog/overviewof-thenist-cybersecurity-framework.

37. (2018) PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard version 3.2.1. [Електронний ресурс] – Режим доступу до ресурсу: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

38. PCI DSS: v4.0. [Електронний ресурс] – Режим доступу до ресурсу: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

39. CIS Controls v8, Center for Internet Security, 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisecurity.org/controls/v8/.

40. CIS Controls v8 Mapping to NIST SP 800-53 Rev 5, Center for Internet Security, 2021.

41. HITRUST CSF Framework, HITRUST Alliance, 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://hitrustalliance.net/product-tool/hitrust-csf/

42. HIPAA; Pub. L. 104-191, 110 Stat. 1936, enacted August 21, 1996

43. Cloud Controls Matrix (CCM), Cloud Security Alliance (2021). [Електронний ресурс] – Режим доступу до ресурсу: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

44. (2018) Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, pp. 1-88. European Parliament

45. (2019) ISO/IEC 27701:2019, Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management —

Requirements and Guidelines. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard/71670.html

46. (2017) Trust Services Criteria Issued by the AICPA Assurance Services Executive Committee. [Електронний ресурс] – Режим доступу до ресурсу: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

47. (2012) COBIT 5, A Framework for the Governance and Management of Enterprise IT. ISACA, USA

48. D. Sulistyowati, F. Handayani and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF COBIT ISO/IEC 27002 and PCI DSS", International Journal on Informatics Visualization, vol. 4, no. 4, pp. 225-230, 2020.

49. M. Siponen and R. Willison, "Information Security Management Standards: Problems and Solutions", J. Information & Management, vol. 46, pp. 267-270, 2009.

50. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, I. Opirskyy, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

51. ISO 27001 Implementation Guide: Checklist of Steps, Timing, and Costs involved. [Електронний ресурс] – Режим доступу до ресурсу: https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/

52. SME GUIDE FOR THE IMPLEMENTATION OF ISO/IEC 27001 ON INFORMATION SECURITY MANAGEMENT. [Електронний ресурс] – Режим доступу до ресурсу: https://sbs-sme.eu/sites/default/files/publications/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min%20%281%29.pdf

53. ISO 27001 implementation checklist: a step-by-step guide. [Електронний ресурс] – Режим доступу до ресурсу: https://nordlayer.com/blog/iso-27001-checklist/?gad_source=1&gclid=Cj0KCQjwn7mwBhCiARIsAGoxjaLVEt6adlrmsDEV-knSdVQT0J8AOLxEmYBD1OUIEBYoF0_LQFLVwaUaAqnmEALw_wcB

54. The Main Benefits of ISO/IEC 27001 Certification. [Електронний ресурс] – Режим доступу до ресурсу: https://pecb.com/article/the-main-benefits-of-isoiec-27001-certification

55. ISO 27001 Requirement 4.1 – Understanding the Context of the Organisation. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/4-1-understanding-organisation-and-context/

56. ISO 27001 Requirement 4.3 – Determining The Scope Of The ISMS. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/determining-scope-information-security-management-system/

57. ISO 27001 Requirement 5.1 – Leadership and Commitment. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/leadership-commitment/

58. ISO 27001:2022 Annex A Control 5.4 Management Responsibilities. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/annex-a/5-4-management-responsibilities-2022/

59. ISO 27001 Requirement 6.1 – Actions to Address Risks & Opportunities. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/actions-to-address-risks-opportunities/

60. ISO 27001 Requirement 6.2 – Information Security Objectives & Planning to Achieve Them. [Електронний ресурс] – Режим доступу до

ресурсу: https://www.isms.online/iso-27001/6-2-establishing-measurable-information-security-objectives/

61. ISO 27001 Requirement 7.1 – Resources for ISO 27001. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/7-1-resources/

62. ISO 27001 Requirement 7.2 – Competence. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/7-2-competence/

63. ISO 27001 Requirement 7.3 – Awareness. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/7-3-awareness/

64. ISO 27001 Requirement 7.4 – Communication. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/7-4-communication/

65. ISO 27001 Requirement 8.1 – Operational Planning & Control. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/operational-planning-control/

66. ISO 27001 Requirement 8.2 – Information Security Risk Assessment. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/information-security-risk-assessment/

67. ISO 27001 Requirement 9.1 – Performance Evaluation. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/9-1-monitoring-measurement-analysis-and-evaluation/

68. ISO 27001 Requirement 9.2 – Internal Audit. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/9-2-internal-audit/

69. ISO 27001 Requirement 10.1 – Nonconformities & Corrective Actions. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/10-1-nonconformity-and-corrective-action/

70. ISO 27001 Requirement 10.2 – Continual Improvement. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/10-2-continual-improvement/

71. What is NIST SP 800-53? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cybersaint.io/blog/what-is-nist-800-53#:~:text=The%20NIST%20Special%20Publication%20800,Management%20Act%20(FISMA)%20requirements.

72. NIST 800-53: Definition and Tips for Compliance. [Електронний ресурс] – Режим доступу до ресурсу: https://www.varonis.com/blog/nist-800-53

73. Makhija, Anil. (2021). SOC for Cybersecurity & SOC 2® for Service Organizations – An empirical study on industry's perspective. Journal of Accounting, Finance, Economics, and Social Sciences. 6. 19-29. 10.62458/jafess.160224.6(2)19-29.

74. SOC 2 Compliance: The Complete Introduction. [Електронний ресурс] – Режим доступу до ресурсу: https://www.auditboard.com/blog/soc-2-framework-guide-the-complete-introduction/

75. Why SaaS Start-Ups Should Prioritize SOC 2 Compliance. [Електронний ресурс] – Режим доступу до ресурсу: https://www.forbes.com/sites/troymarkowitz/2021/01/15/why-saas-start-ups-should-prioritize-soc-2-compliance/?sh=2d85b14d51b2

76. Курій Є. О., Опірський І. Р. (2024) Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS // Кібербезпека: освіта, наука, техніка. – Т. 3, № 23. – С. 145–155. DOI: https://doi.org/10.28925/2663-4023.2024.23.145155

77. Mustafa, N. (2023) PCI DSS v4.0: achieving more with limited resources. In: Brighttalk Webinar Series. DOI: 10.13140/RG.2.2.17152.20486

78. Payment Card Industry Security Standards. [Електронний ресурс] – Режим доступу до ресурсу: https://listings.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

79. PCI DSS version 4.0 is here: What you need to know now. [Електронний ресурс] – Режим доступу до ресурсу: https://rsmus.com/insights/services/risk-fraud-cybersecurity/pci-dss-version-4-point-0-is-here-what-you-need-to-know-now.html

80. PCI DSS Summary of Changes: v3.2.1 to v4.0. [Електронний ресурс] – Режим доступу до ресурсу: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

81. Changes to the PCI DSS v4.0 standard and their impact on your organization in 2024. [Електронний ресурс] – Режим доступу до ресурсу: https://my-itspecialist.com/en/changes-to-the-pci-dss-v4-0-standard-and-their-impact-on-your-organization-in-2024#:~:text=8.-,PCI%20DSS%20v4.,their%20business%20and%20security%20needs.

82. Top 11 cybersecurity frameworks in 2023. [Електронний ресурс] – Режим доступу до ресурсу: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks

83. Wijayarathne, Senesh. (2022). ISO 27001 Implementation.

84. Alrehili, Afnan & Alhazmi, Omar. (2024). ISO/IEC 27001 Standard: Analytical and Comparative Overview. In book: Advances in Data-Driven Computing and Intelligent Systems. 10.1007/978-981-99-9524-0_12

85. Kurii, Y. ., & Opirskyy, I. (2023). ISO 27001: АНАЛІЗ ЗМІН ТА ОСОБЛИВОСТІ ВІДПОВІДНОСТІ НОВІЙ ВЕРСІЇ СТАНДАРТУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655

86. ISO 27001 2013 vs. 2022 revision – What has changed? [Електронний ресурс] – Режим доступу до ресурсу: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/

87. Vakhula O., Kurii Y., Opirskyy I., Susukailo V. (2024) Security-as-code concept for fulfilling ISO/IEC 27001:2022 requirements // Paper presented at the CEUR Workshop Proceedings, vol. 3654, . 59–72.

88. Beckers, Kristian & Côté, Isabelle & Fenz, Stefan & Hatebur, Denis & Heisel, Maritta. (2014). A Structured Comparison of Security Standards. 10.1007/978-3-319-07452-8_1.

89. Ensuring Uniform Security: The Role of Cross-Platform Standards. [Електронний ресурс] – Режим доступу до ресурсу: https://www.neumetric.com/uniform-security-cross-platform-standards/

90. Курій Є. О., Опірський І. Р. АНАЛІЗ ПЕРЕВАГ І НЕДОЛІКІВ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ // Materials of the V International Research and Practical Internet Conference «Development Strategies for Modern Education and Science», – 2024. – 2024. – С. 16–17.

91. Understanding IT security frameworks: Types and examples. [Електронний ресурс] – Режим доступу до ресурсу: https://www.onetrust.com/blog/security-framework-types/

92. Beckers, Kristian & Côté, Isabelle & Fenz, Stefan & Hatebur, Denis & Heisel, Maritta. (2014). A Structured Comparison of Security Standards. 10.1007/978-3-319-07452-8_1.

93. What is security compliance management? [Електронний ресурс] – Режим доступу до ресурсу: https://nordlayer.com/learn/regulatory-compliance/compliance-management/?gad_source=1&gclid=Cj0KCQjwztOwBhD7ARIsAPDKnkCBLY

Gcr9VGV6PjSzvJv_s-oRYW29FxLq_ToQkmwPV1wxOkpoQasdoaAlp_EALw_wcB

94. ADOPTING A SECURITY VS COMPLIANCE FOCUSED POSTURE. [Електронний ресурс] – Режим доступу до ресурсу: https://www.archtis.com/adopting-a-security-vs-compliance-focused-posture/

95. Beyond Compliance: Why A Proactive Security Approach Is Imperative. [Електронний ресурс] – Режим доступу до ресурсу: https://www.forbes.com/sites/forbestechcouncil/2023/07/06/beyond-compliance-why-a-proactive-security-approach-is-imperative/?sh=72102dee3283

96. 5 Simple Steps That Ensure Data Security And Compliance For Your Business. [Електронний ресурс] – Режим доступу до ресурсу: https://www.secoda.co/blog/5-simple-steps-that-ensure-data-security-and-compliance-for-your-business

97. ISO 27001 implementation checklist: a step-by-step guide. [Електронний ресурс] – Режим доступу до ресурсу: https://nordlayer.com/blog/iso-27001-checklist/?gad_source=1&gclid=Cj0KCQjwztOwBhD7ARIsAPDKnkB2iBXeoT9svT44huacmo20HDUuG2bRR51UUXYmLSpaw5unPNtkDOcaAj4iEALw_wcB

98. How to implement a cyber security framework – 5 step plan. [Електронний ресурс] – Режим доступу до ресурсу: https://www.nec.co.nz/market-leadership/publications-media/how-to-implement-a-cyber-security-framework-5-step-plan/

99. How to Implement the NIST Cybersecurity Framework? [Електронний ресурс] – Режим доступу до ресурсу: https://www.armis.com/faq/how-to-implement-the-nist-cybersecurity-framework/

100. Ewuga, Sarah & Egieya, Zainab & Omotosho, Adedolapo & Adegbite, Abimbola. (2024). ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY. Finance & Accounting Research Journal. 5. 405-425. 10.51594/farj.v5i12.684.

101. SOC 2 Implementation Guide and Understanding SOC 2 Reports. [Електронний ресурс] – Режим доступу до ресурсу: https://socreports.com/white-papers/soc-2/soc-2-implementation-guide-and-understanding-soc-2-reports

102. Євгеній Курій, Віталій Сусукайло, Іван Опірський (2023). РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001. Ukrainian Information Security Research Journal. 25(3):132-139. DOI: https://doi.org/10.18372/2410-7840.25.17938;

103. Yevhenii KURII, Ivan OPIRSKYY, Leonid BORTNIK ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD // Materials of IXth International Scientific and Technical Conference INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY, May 25–26, 2023. - Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6.

104. MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. [Електронний ресурс] – Режим доступу до ресурсу: https://msecb.com/wp-content/uploads/2023/01/MSECB-Transition-Policy-on-MS-Certification-to-ISO-IEC-27001.pdf?utm_source=sendinblue&utm_campaign=Clients%20ISOIEC%2027001 2012022%20Transition%20Policy&utm_medium=email

105. Pacaiova, H., Nagyova, A. (2019) Risk based thinking – New approach for modern enterprises' management, Advances in Intelligent Systems and ComputingVolume 783, Pages 524 - 5362019 AHFE International Conference on

Human Factors, Business Management and Society, 2018 Orlando21, July 2018, through 25 July 2018, Code 215359

106. What is an ISO 27001 internal audit? [Електронний ресурс] – Режим доступу до ресурсу: https://www.vanta.com/glossary/iso-27001-internal-audit

107. How to manage changes in an ISMS. [Електронний ресурс] – Режим доступу до ресурсу: https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/

108. Shukla, Abhinay & Suri, Pradeep. (2024). Importance of Implementing Effective Cyber Security Controls for Active Cyber Security Risk Management. 10.1007/978-981-99-9550-9_19.

109. Tarakçı, Emin & Gönül, Anıl. (2023). Risk Analysis and Assessment Framework for Cyber Security in Management SystemsRisk Analysis and Assessment Framework for Cyber Security in Management Systems. OHS ACADEMY. 6. 10.38213/ohsacademy.1402624.

110. Shukla, Abhinay & Suri, Pradeep. (2024). Importance of Implementing Effective Cyber Security Controls for Active Cyber Security Risk Management. 10.1007/978-981-99-9550-9_19.

111. Bouke, Mohamed Aly. (2023). Security and Risk Management. 10.1007/979-8-8688-0057-3_3.

112. Rajathi, C. & Rukmani, P.. (2023). Investigation of Assessment Methodologies in Information Security Risk Management. 10.1007/978-981-99-5166-6_26.

113. Cybersecurity risk assessment in 5 steps. [Електронний ресурс] – Режим доступу до ресурсу: https://nordlayer.com/blog/cyber-security-risk-assessment/?gad_source=1&gclid=Cj0KCQjwztOwBhD7ARIsAPDKnkCKqW30ZzH47YKKCCnEuiGe3PKcMbuXGZLxlX5jHA8nlFxl669aN9AaAnGREALw_wcB

114. Identifying Assets for IT Risk Analysis. [Електронний ресурс] – Режим доступу до ресурсу: https://reciprocity.com/blog/identifying-assets-for-it-risk-analysis/

115. Asset-Based Risk Assessment. [Електронний ресурс] – Режим доступу до ресурсу: https://drata.com/glossary/asset-based-risk-assessment

116. Information Classification in Information Security. [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/information-classification-in-information-security/

117. Information Classification - Why it matters? [Електронний ресурс] – Режим доступу до ресурсу: https://pecb.com/article/information-classification--why-it-matters

118. What is a Risk Assessment? [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/risk-assessment

119. (2022) ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection - Guidance on managing information security risks. [Електронний ресурс] – Режим доступу до ресурсу: https://www.iso.org/standard/80585.html

120. Information Security Policy: Examples and 11 Elements of a Successful Policy. [Електронний ресурс] – Режим доступу до ресурсу: https://www.hackerone.com/knowledge-center/information-security-policy#:~:text=An%20information%20security%20policy%20is,and%20distribute%20its%20information%20assets.

121. The importance of an effective information security policy. [Електронний ресурс] – Режим доступу до ресурсу: https://www.qmsuk.com/news/the-importance-of-an-effective-information-security-

policy#:~:text=An%20information%20security%20policy%20is,only%20those%20that%20you%20want.

122. Information Security Policies: Why They Are Important To Your Organization. [Електронний ресурс] – Режим доступу до ресурсу: https://linfordco.com/blog/information-security-policies/

123. IT Security Policy: Importance, Best Practices, & Top Benefits. [Електронний ресурс] – Режим доступу до ресурсу: https://www.esecurityplanet.com/compliance/it-security-policies/

124. Information Security Policy: Must-Have Elements and Tips. [Електронний ресурс] – Режим доступу до ресурсу: https://blog.netwrix.com/information-security-policy/

125. The 12 Elements of an Information Security Policy. [Електронний ресурс] – Режим доступу до ресурсу: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

ДОДАТОК А. АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

АКТ

про впровадження результатів дисертаційної роботи

Курія Євгенія Олеговича

«МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РАХУНОК ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ»

Цей акт підтверджує впровадження методології перехресного впровадження стандартів аудиту з кібербезпеки для покращення та оптимізації процесу дотримання відповідності стандартам інформаційної безпеки, а також для підвищення загального рівня інформаційної безпеки в організації.

Результати дослідження, які включають методологію, наразі активно використовуються для ефективного впровадження і підтримання внутрішніх процесів організації, пов'язаних з інформаційною безпекою, і сприяють забезпеченню статусу відповідності міжнародному стандарту SOC 2.

Директор
ТОВ «ЕЙЧ-ЛАБ СОЛЮШНЗ» _____ Вовченко О.В.

3 квітня 2024 року

binariks

АКТ

про впровадження результатів дисертаційної роботи

Курія Євгенія Олеговича

«МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РАХУНОК ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ»

Комісія у складі голови – директора Товариства з обмеженою відповідальністю «Бінарікс Україна», Шимчака Володимира Павловича, та члена комісії – експерта з кібербезпеки, Масюка Юрія-Богдана Андрійовича, склала цей акт про те, що на основі запропонованих досліджень та розглянутої методології перехресного впровадження стандартів аудиту з кібербезпеки було оптимізовано процес дотримання відповідності стандартам інформаційної безпеки, а також підвищено загальний рівень безпеки організації.

Результати дослідження, які включають методологію, наразі активно використовуються для ефективного впровадження і підтримання внутрішніх процесів організації, пов'язаних з інформаційною безпекою, і сприяють забезпеченню статусу відповідності міжнародним стандартам інформаційної безпеки.

Директор ТОВ «Бінарікс Україна» _____ Шимчак В.П.

Експерт з кібербезпеки ТОВ «Бінарікс Україна» _____ Масюк Ю.А.

АКТ

про впровадження результатів дисертаційної роботи

Курія Євгенія Олеговича

«МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РАХУНОК ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ АУДИТУ З КІБЕРБЕЗПЕКИ»

Комісія у складі голови – директора Товариства з обмеженою відповідальністю «ПІК РІСОРСИС», Пришляка Віктора Леонідовича, та члена комісії – технічного директора Товариства з обмеженою відповідальністю «ПІК РІСОРСИС», Вандакурова Андрія Олександровича, склала цей акт про те, що на основі запропонованих досліджень та розглянутої методології перехресного впровадження стандартів аудиту з кібербезпеки було оптимізовано процес дотримання відповідності стандартам інформаційної безпеки, а також підвищено загальний рівень інформаційної безпеки організації.

Результати дослідження, які включають методологію, наразі активно використовуються для ефективного впровадження і підтримки внутрішніх процесів організації, пов'язаних з інформаційною безпекою, і сприяють забезпеченню статусу відповідності міжнародному стандарту ISO/IEC 27001:2022.

Технічний директор ТОВ
«ПІК РІСОРСИС» _____ Вандакуров А. О.

Директор
ТОВ «ПІК РІСОРСИС» _____ Пришляк В. Л.

ДОДАТОК Б. ОГЛЯД ВІДМІННОСТЕЙ МІЖ ВЕРСІЯМИ 4.0 І 3.2.1 СТАНДАРТУ PCI DSS

Мета контролю	**PCI DSS вимога/контроль**	**Огляд відмінностей між версіями 4.0 і 3.2.1**
Побудуйте і підтримуйте безпечну мережу і системи Build and Maintain a Secure Network and Systems	1. Встановіть і підтримуйте налаштування брандмауера для захисту даних власників карток Install and maintain a firewall configuration to protect cardholder data	Розширено спектр мережевих технологій. Уточнено мету контролю щодо розмежування між довіреними та недовіреними мережами, зокрема бездротовими. Деталізовано та розширено деякі вимоги. Частину вимог було розділено на окремі пункти.
	2. Не використовуйте налаштування за замовчуванням, які надає вендор, для паролів та інших параметрів безпеки Do not use vendor-supplied defaults for system passwords	Додано вимогу 2.1.2 щодо опису, прийняття та виконання обов’язків. Уточнено вимоги щодо небезпечних служб та протоколів.

	and other security parameters	
Захищайте дані власників карток Protect Cardholder Data	3. Захищайте дані власників карток, які зберігаються Protect stored cardholder data	Значно деталізовано вимоги щодо зберігання критичних даних до завершення авторизації (3.2.1, 3.3.2). Без виробничої необхідності дозволяється відображати лише 4 останні цифри під час маскування. Окремо описані вимоги щодо використання хешу. Шифрування на рівні диска або розділу використовується лише для змінних носіїв. Забороняється використовувати однакові ключі для тестового та виробничого середовищ.
	4. Шифруйте передачу даних власників карток через відкриті публічні мережі	Додано вимогу вести інвентаризацію, контроль використання, термін дії всіх довірених ключів та сертифікатів, які використовуються для

	Encrypt transmission of cardholder data across open, public networks	захисту повного номера картки під час його передачі.
Підтримуйте програму по управлінню ризиками Maintain a Vulnerability Management Program	5. Захищайте всі системи від шкідливого програмного забезпечення і регулярно оновлюйте антивірусне програмне забезпечення Protect all systems against malware and regularly update antivirus software or programs	Цей розділ має п'ять нових вимог. Саме у п'ятому розділі вперше з'являється нове для стандарту PCI DSS поняття targeted risk analysis – цільовий аналіз ризику. Версія стандарту 4.0 пропонує організаціям самостійно заповнювати таблицю, шаблон якої наведено у новій версії стандарту, де аналізується той чи інший ризик та робляться висновки щодо його (ризику) прийняття, компенсації, чи уникнення тощо. Також, заповнення даної таблиці вимагає визначати періодичність та частоту сканування систем антивірусними засобами, а також періодичність перевірок систем, які

		вважаються такими, що не піддаються вірусним загрозам. Додано вимогу, що визначає, що антивірус відтепер повинен сканувати всі знімні носії, а також повинен бути організований захист організації від фішингу.
	6. Розробіть і підтримуйте захищені системи і додатки Develop and maintain secure systems and applications	Додано три нові вимоги. Додано вимогу щодо створення та підтримання реєстру всіх користувачів ПЗ, а також всіх ПЗ третіх сторін. Додано вимогу для власників веб-сторінок платіжних систем вести список усіх сценаріїв скрипту на цій сторінці з обґрунтуванням необхідності кожного з них. Використання мережевого екрану для захисту веб-додатків стає обов'язковим для організації.

Впровадьте суворі заходи контролю доступу Implement Strong Access Control Measures	7. Обмежте доступ до даних про власників карток відповідно до потреб бізнесу Restrict access to cardholder data by business need to know	Сьомий розділ отримав три нові вимоги. Необхідно впровадити перевірку всіх облікових записів на легітимність їх існування та прав щонайменше раз на шість місяців, а також окремо виділено вимоги до технічних та сервісних облікових записів.
	8. Ідентифікуйте та автентифікуйте доступ до компонентів системи Identify and authenticate access to system components	У цьому розділі виникло п'ять нових вимог. Особлива увага приділяється багатофакторній автентифікації. Висуваються вимоги до облікових записів, які можна використовувати для інтерактивного входу. Окремо виокремлено вимоги до терміналів точок продажу. Вимога збільшення довжини пароля з 7 до 12 символів. Вимога впровадження багатофакторної

		аутентифікації (MFA) для всіх видів доступу до CDE. Заборона прописувати паролі у файлах та скриптах.
	9. Обмежте фізичний доступ до даних власників карток Restrict physical access to cardholder data	Цільовий аналіз ризику визначає необхідність перевірок пристрою POI на відсутність підробки. Також зазначено, з якою періодичністю мають відбуватися дані перевірки. Окремо виокремлено вимоги до відвідувачів. Змінено вимоги до зберігання, обліку та знищення носіїв.
Регулярно перевіряйте та тестуйте мережі Regularly Monitor and Test Networks	10. Відстежуйте та контролюйте всі доступи до мережевих ресурсів і даних власників карток Track and monitor all access to network resources and cardholder data	Цей розділ вимагає використання автоматичних механізмів для перевірки журналів аудиту. Додано вимогу виявляти, попереджати та оперативно усувати збої критичних систем контролю безпеки.

	11. Регулярно тестуйте системи та процеси безпеки Regularly test security systems and processes	Одинадцятий розділ отримав п'ять нових вимог. Конкретизуються особливості та порядок дій при внутрішньому скануванні на вразливості (проводити яке мають право лише авторизовані компанії), а також додано вимогу, що системи IDS/IPS повинні виявляти та усувати приховані канали передачі шкідливих програм. Додано вимогу до управління всіма знайденими вразливостями (а не лише критичними). З'являється поняття multi-tenant service providers - будь-які дата-центри та хмарні провайдери підпадають під даний контроль. Всі вони повинні будуть проходити додаткову перевірку за програмою A1.

Підтримуйте політику інформаційної безпеки Maintain an Information Security Policy	12. Підтримуйте політику безпеки інформації для всього персоналу Maintain a policy that addresses information security for all personnel	Цей розділ отримав тринадцять нових вимог. Важливо відзначити, що дві вимоги з них є обов'язковими для виконання ще з 2024 року. Це необхідність проводити вже згаданий «targeted risk analysis» щонайменше раз на рік, а також необхідність підтримувати документований опис зони відповідності стандарту в актуальності та проводити перевірку щонайменше раз на рік або за істотних змін даного середовища. Решта нових вимог також зосереджена в основному на документуванні того чи іншого аспекту підтримки організацією відповідності вимогам стандарту PCI DSS. Для постачальників послуг - додано вимогу документувати та підтверджувати сферу

		застосування PCI DSS не рідше ніж кожні 6 місяців. Додалася вимога щодо оновлення програми підвищення поінформованості раз на 12 місяців. Частота навчання персоналу має ґрунтуватися на проведеному аналізі ризиків.

ДОДАТОК В. КОНТРОЛЬНИЙ СПИСОК ДЛЯ ПРОВЕДЕННЯ ОЦІНКИ НА ВІДПОВІДНІСТЬ

	Область оцінки відповідності							
Пункт	**Секція**	**Пункти для оцінювання**	**Завдяння до виконання**	**Артефакти/Документована інформація**	**Результати оцінювання**	**Статус відповідності**	**Статус**	**Коректуючі дії**
5	**Організаційні контролі**							
5.1	Політики інформаційної безпеки	1. Чи розроблена Політика Інформаційної Безпеки та інші доменні політики? 2. Чи затверджені всі політики керівництвом? 3. Чи належним чином політики доносяться до зацікавлених сторін і чи отримується підтвердження ознайомлення з цими політиками? 4. Чи підлягають політики з безпеки регулярному перегляду? 5. Чи проводяться перегляди політик, коли змінюються обставини?	1. Розробити і впровадити полі+D4:D5тику інформаційної безпеки. 2. Переконатися, що політика включає такі вимоги: а) бізнес-стратегію та вимоги; б) нормативні акти, законодавство та контракти; в) поточні та передбачувані ризики та загрози інформаційної безпеки. 3. Переконатися, що політика містить твердження щодо: а) визначення інформаційної безпеки; б) цілей інформаційної безпеки або фреймворку для встановлення цілей інформаційної безпеки; в) принципів для керівництва всіма діяльностями, пов'язаними з інформаційною безпекою; г) зобов'язання виконувати вимоги, пов'язані з інформаційною безпекою; д) зобов'язання до постійного вдосконалення системи управління інформаційною безпекою; е) призначення відповідальності за управління інформаційною безпекою для визначених ролей; и) процедури для обробки винятків. 4. Затвердити політику інформаційної безпеки керівництвом. 5. Сповістити про політику персонал та зацікавлені сторони. 6. Запланувати періодичні перегляди політики. 7. Визначити список подій та змін, при яких буде переглядатися політика.	1. Політика Інформаційної Безпеки. 2. Реєстр політик		Невідповідність	0%	
5.2	Ролі і відповідальності з інформ	Чи чітко визначені та розподілені ролі та відповідальності з інформаційної безпеки відповідно до потреб організації?	1. Визначити ролі та відповідальності з інформаційної безпеки для: а) захисту інформації та інших пов'язаних активів; б) проведення конкретних процесів із забезпечення інформаційної безпеки; в) діяльності з управління ризиками інформаційної безпеки та, зокрема, прийняття залишкових ризиків (наприклад, власникам	1. Ролі та відповідальності із інформаційної безпеки задокументовані в політиках.		Невідповідність	0%	

	аційної безпеки		ризиків); г) всього персоналу, який використовує інформацію організації та інші пов'язані активи. 2. Переконатися, що розподіл ролей та відповідальностей із інформаційної безпеки відбувається відповідно до політики інформаційної безпеки та доменних політик. 3. Визначити та задокументувати кожну область безпеки, за яку індивіди несуть відповідальність. 4. Сповістити кожну область безпеки відповідному персоналу. 5. Визначити та задокументувати рівні авторизації. 6. Призначити менеджера (або команду) із інформаційної безпеки та визначити їхні відповідальності.	2. Опціонально: Матриця RBAC (ролей і прав доступу)				
5.3	Розмежування обов'язків	Було: Чи розмежовані обов'язки та сфери відповідальності, щоб зменшити можливості для несанкціонованої модифікації або зловживання інформацією чи послугами? Стало: Чи розмежовані суперечливі обов'язки та сфери відповідальності, щоб зменшити ризик шахрайства, помилок та обходу засобів контролю інформаційної безпеки та запобігти виконанню однією особою потенційно суперечливих обов'язків одноосібно?	1. Визначити, які обов'язки та сфери відповідальності необхідно розмежувати. 2. Розподілити обов'язки та сфери відповідальності між різними особами. 3. У разі неможливості або недоцільності розподілу обов'язків та сфер відповідальності, розгляньте інші засоби контролю, такі як моніторинг діяльності, аудиторські сліди та нагляд з боку керівництва. 4. Переконайтися, що особам не надаються ролі, що суперечать одна одній. 5. Розглянути можливість використання автоматизованих інструментів для виявлення конфліктів за наявності великої кількості ролей.	1. Ролі та відповідальності із інформаційної безпеки задокументовані в політиках. 2. Опціонально: Матриця RBAC (ролей і прав доступу)		Невідповідність	0%	
5.4	Управлінські обов'язки або Обов'язки менеджменту	Було: 1. Чи залучені керівники (всіх рівнів) до управління безпекою в бізнесі? 2. Чи поведінка та політика керівництва спонукає та заохочує всіх працівників, підрядників та сторонніх користувачів застосовувати заходи безпеки відповідно до встановлених політик та процедур? Стало: 1. Чи залучені керівники (всіх рівнів) до забезпечення безпеки в компанії? 2. Чи поведінка та політика керівництва спонукає та заохочує весь персонал та підрядників застосовувати безпеку відповідно до встановленої політики	1. Визначити та задокументуйте обов'язки керівництва, які повинні включати забезпечення того, щоб персонал а) був належним чином проінструктований про свої ролі та обов'язки в сфері інформаційної безпеки до того, як йому буде надано доступ до інформації та інших пов'язаних з нею активів організації б) були забезпечені інструкціями, які визначають очікування щодо інформаційної безпеки, пов'язані з їхньою роллю в організації c) мають мандат на виконання політики інформаційної безпеки та тематичних політик організації; d) досягти рівня обізнаності з питань інформаційної безпеки, що відповідає їхнім ролям та обов'язкам в організації; e) дотримуватися умов трудового договору, контракту або угоди, включаючи політику інформаційної безпеки організації та відповідні методи роботи; f) підтримувати відповідні навички та кваліфікацію з інформаційної безпеки шляхом постійного професійного навчання;	1. Ролі та відповідальності із інформаційної безпеки задокументовані в політиках. 2. Опціонально: Матриця RBAC (ролей і прав доступу)		Невідповідність	0%	

		інформаційної безпеки, специфічних політик та процедур?	g) там, де це практично можливо, мати конфіденційний канал для повідомлення про порушення політики інформаційної безпеки, тематичних політик або процедур інформаційної безпеки ("викривання"). Це може дозволяти анонімні повідомлення або передбачати положення, які гарантують, що інформація про особу заявника буде відома лише тим, хто має працювати з такими повідомленнями; h) забезпечені достатніми ресурсами та часом на планування проектів для впровадження процесів і засобів контролю, пов'язаних з безпекою організації.					
5.5	Зв'язок з органами влади або Контакт з органами влади також може бути взаємодія	(Залишилось як було в 6.1.3) 1. Чи існує процедура, яка документує, коли і ким буде здійснюватися контакт з відповідними органами (правоохоронними органами тощо)? 2. Чи існує процедура, яка детально описує, як і коли потрібно контактувати з відповідними органами? 3. Чи існує процедура для регулярних контактів та обміну розвідувальною інформацією?	1. Визначте всі відповідні органи, з якими буде встановлено контакт, наприклад, правоохоронні органи, регуляторні органи, органи нагляду, комунальні служби, аварійні служби, постачальники електроенергії, телекомунікаційні провайдери та водопостачальники. 2. Розробити процедуру, яка регулюватиме комунікацію з цими органами. Процедура повинна визначати, коли і хто повинен звертатися до цих органів. Процедура також повинна детально описувати, як своєчасно повідомляти ці органи про виявлені інциденти інформаційної безпеки. 3. Впровадити процедуру реєстрації всіх комунікацій з цими органами. 4. Скласти графік регулярного перегляду та оновлення контактів з органами влади та процедури комунікації. 5. Переконайтися, що контакти та порядок комунікації інтегровані в процеси управління інцидентами інформаційної безпеки організації та планування безперервності бізнесу.	1. Перелік усіх відповідних органів, з якими буде встановлено контакт. 2. Процедура контакту з відповідними органами.		Невідповідність	0%	
5.6	Зв'язок з групами за інтересами	(Залишилось як було в 6.1.4) Чи підтримують відповідні особи в організації активне членство у відповідних групах за інтересами?	1. Обрати групи за інтересами та/або спеціалізовані форуми з питань безпеки та/або професійні асоціації. 2. Створити членську базу. 3. Призначити відповідних осіб в організації для підтримання контактів.	1. Перелік груп за інтересами та/або спеціалізованих форумів з питань безпеки та/або професійних асоціацій.		Невідповідність	0%	
5.7	Розвідка загроз	Чи збирається та аналізується інформація про загрози інформаційній безпеці для отримання розвідданих про загрози?	1. Запровадити процедуру збору та аналізу загроз інформаційній безпеці. 2. Розділити розвідку загроз на три рівні, які необхідно враховувати: а) Стратегічний розвідувальний інтелект: обмін високорівневою інформацією щодо змін у загрозовому середовищі (наприклад, типи зловмисників чи типи атак).	1. Процедура збору та аналізу загроз інформаційній безпеці. 2. Система розвідки загроз.		Невідповідність	0%	

			б) тактична розвідка загроз: інформація про методи, інструменти та технології зловмисників в) оперативна розвідка загроз: детальна інформація про конкретні атаки, включаючи технічні показники. 3. Переконатися, що розвіддані про загрози є а) релевантними (тобто пов'язані із захистом організації); б) мають значення (тобто такою, що надає організації точне та детальне розуміння ландшафту загроз); с) контекстуальні для забезпечення ситуативної обізнаності (тобто додавання контексту до інформації на основі часу подій, де вони відбуваються) часу подій, місця, де вони відбуваються, попереднього досвіду та поширеності в подібних організаціях); г) дієвою (тобто організація може швидко та ефективно реагувати на інформацію). 4. Переконатися, що розвідка про загрози включає: а) встановлення цілей для створення розвідувальних даних про загрози; b) виявлення, перевірка та вибір внутрішніх і зовнішніх джерел інформації, які є необхідними та прийнятними для надання інформації, необхідної для виробництва розвідки про загрози; в) збір інформації з обраних джерел, які можуть бути внутрішніми та зовнішніми; d) обробка зібраної інформації для підготовки її до аналізу (наприклад, шляхом перекладу, форматування або підтвердження інформації); е) аналіз інформації, щоб зрозуміти, наскільки вона пов’язана з організацією та є значущою для неї; f) передача та розповсюдження відповідним особам у форматі, який можна зрозуміти. 5. Визначити метод і відповідних осіб для спільного обміну інформацією про загрози з іншими організаціями.				
5.8	Інформаційна безпека в управлінні проектами	1. Чи всі проекти проходять певну форму оцінки інформаційної безпеки? 2. Чи визначаються вимоги до інформаційної безпеки при впровадженні нових систем? 3. Чи визначаються та виконуються вимоги безпеки при вдосконаленні або модернізації систем?	1.Оцінити та усунути ризики інформаційної безпеки в проектах. 2.Забезпечити ідентифікацію та врахування вимог щодо інформаційної безпеки на етапах початкового планування та проектування. 3.Розглянути та усувайте ризики інформаційної безпеки, пов'язані з виконанням проекту. 4.Переглянути та оцінюйте ефективність усунення ризиків інформаційної безпеки. 5.Визначити та призначайте ролі та відповідальності, пов'язані з інформаційною безпекою в межах проекту.	1. Вимоги до інформаційної безпеки в управлінні проектами.		Невідповідність	0%	

			6.Визначити вимоги до продуктів проекту щодо інформаційної безпеки. 7.Забезпечити, що підходи до розробки проекту підтримують інформаційну безпеку.					
5.9	Інвентаризація інформації та інших пов'язаних з нею активів	Було: 8.1.1 1. Чи проводиться інвентаризація всіх активів, пов'язаних з інформацією та засобами обробки інформації? 2. Чи є інвентаризація точною і чи підтримується вона в актуальному стані? 8.1.2 Всі інформаційні активи повинні мати чітко визначеного власника, який усвідомлює свої обов'язки. Стало: 1. Чи існує інвентаризація інформаційних та інших пов'язаних з ними активів (включаючи власників)? 2. Чи є інвентаризація точною і підтримується в актуальному стані? 3. Чи закріплено право власності на ідентифіковану інформацію та інші пов'язані з нею активи за окремою особою або групою осіб? 4. Чи визначена класифікація для ідентифікованої інформації та інших пов'язаних з нею активів? 5. Чи впроваджено процес, що забезпечує своєчасне визначення права власності на активи? 6. Чи існує процес, який забезпечує передачу права власності при створенні активів або при передачі активів організації? 7. Чи існує процес, який забезпечує перепризначення права власності на активи, коли поточні власники активів звільняються або змінюють роботу?	1.Визначити інформаційні та інші пов'язані активи. 2.Класифікувати активи та визначте їхнє розташування. 3.Визначити важливість цих активів з точки зору інформаційної безпеки. 4.Забезпечити зберігання документації відповідно до відведених або існуючих інвентарів, якщо це необхідно. 5.Для забезпечення точності інвентаря інформаційних та інших пов'язаних активів впровадити такі процеси: a) регулярні перегляди визначених інформаційних та інших пов'язаних активів з використанням інвентарю активів; b) автоматичне забезпечення оновлення інвентаря при встановленні, зміні або видаленні активу. 6.Впровадити процес призначення та перепризначення власності активів. 7.Сповістити та підтвердити власників їхніх обов'язків та відповідальності за належне управління активом протягом всього циклу його життя.	1. Інвентаризація інформації та інших пов'язаних з нею активів. 2. Політика або процедура управління активами. (Процедури для проведення регулярних перевірок ідентифікованої інформації та інших пов'язаних з нею активів на відповідність інвентаризації активів та автоматичного оновлення інвентаризації в процесі встановлення, зміни або видалення активу). 3. Процедура передачі та перепризначення права власності на активи.		Невідповідність	0%	

5.10	Допустиме використання інформації та інших пов'язаних з нею активів	Було: 8.1.3 1. Чи існує прийнятна політика використання для кожного класу/типу інформаційних активів? 2. Чи ознайомлені користувачі з цією політикою перед використанням? 8.2.3 1. Чи існує процедура поводження з кожною класифікацією інформації? 2. Чи ознайомлені користувачі інформаційних активів з цією процедурою? Стало: 1. Чи існують політика прийнятного використання та процедури поводження з кожним класом/типом інформаційних активів? 2. Чи ознайомлені користувачі з цією політикою перед використанням? 3. Чи існує процедура поводження з кожною класифікацією інформації? 4. Чи ознайомлені користувачі інформаційних активів з цією процедурою?	1. Розробити політику щодо прийнятного використання інформації та інших пов'язаних з нею активів для конкретної теми. 2. Переконайтися, що ця політика містить чіткі вказівки щодо того, як особи повинні використовувати інформацію та інші пов'язані з нею активи, а також зазначає наступне: а) очікувану та неприйнятну поведінку осіб з точки зору інформаційної безпеки б) дозволене та заборонене використання інформації та інших пов'язаних з нею активів в) моніторинг діяльності, що здійснюється організацією. 3. Встановити прийнятні процедури використання для повного життєвого циклу інформації відповідно до її класифікації та визначених ризиків, які включають: а) обмеження доступу, що підтримують вимоги захисту для кожного рівня класифікації; б) ведення обліку авторизованих користувачів інформації та інших пов'язаних з нею активів в) захист тимчасових або постійних копій інформації до рівня, що відповідає рівню захисту оригінальної інформації; г) зберігання активів, пов'язаних з інформацією, відповідно до специфікацій виробників; е) чітке маркування всіх копій носіїв інформації (електронних або фізичних) до відома уповноваженого одержувача уповноваженого одержувача; f) дозвіл на видалення інформації та інших пов'язаних з нею активів та підтримувані методи видалення. 4. Довести цю політику до відома всіх, хто використовує або обробляє інформацію та інші пов'язані з нею активи. 5. Встановити процес ідентифікації та контролю за використанням активів третіх осіб та будь-яких активів організації, пов'язаних з такими зовнішніми активами	1. Політика допустимого виокористання.		Невідповідність	0%	
5.11	Повернення активів	Чи існує процес, який гарантує, що весь персонал та інші зацікавлені особи повернуть активи організації після припинення або зміни їхнього трудового договору, контракту чи угоди?	1. Визначити та задокументуйте всю інформацію та інші пов'язані з нею активи, що підлягають поверненню, які можуть включати а) кінцеві пристрої користувачів б) портативні пристрої зберігання даних с) спеціальне обладнання г) обладнання для автентифікації (наприклад, механічні ключі, фізичні токени та смарт-картки) для інформаційних систем, сайтів та фізичних архівів; д) фізичні копії інформації. 2. Запровадити процедуру повернення всіх раніше виданих фізичних та електронних активів при зміні або розірванні трудового договору, контракту чи угоди з персоналом.	1. Інвентаризація активів. 2. Політика управління активами або процес повернення всіх раніше виданих фізичних та електронних активів.		Невідповідність	0%	

			3. Встановити процедури відстеження та передачі всієї відповідної інформації до організації та її безпечного видалення з обладнання, яке персонал або інші зацікавлені сторони купують в організації після зміни або розірвання трудового договору, контракту чи угоди з персоналом. 4. Встановити формальний процес документування та передачі знань та інформації, які є важливими для поточної діяльності, при зміні або розірванні трудового договору, контракту або угоди з персоналом. 5. Повідомлення про звільнення, 6. Обмежити використання інформації, яка зберігається на активах, що не належать організації, за допомогою управління правами доступу або криптографії.					
5.12	Класифікація даних	Було: 8.2.1 1. Чи існує політика, що регулює засекречування інформації? 2. Чи існує процес, за допомогою якого вся інформація може бути належним чином засекречена? Стало: 1. Чи існує процес, за допомогою якого вся інформація може бути належним чином засекречена? 2. Чи існує політика, що регулює засекречування інформації за певною тематикою? 3. Чи ця політика належним чином доведена до відома відповідних зацікавлених сторін?	1.Встановити політику класифікації інформації. 2.Сповістити про цю політику всіх зацікавлених сторін. 3.Забезпечити, щоб схема класифікації враховувала вимоги до конфіденційності, цілісності, доступності та потреб зацікавлених сторін. 4.Визначити та задокументуйте відповідальність власників класифікованої інформації. 5.Впровадити процес регулярного перегляду, аналізу та оновлення схеми класифікації інформації. 6.Забезпечити, щоб схема класифікації була відповідною тематичній політиці щодо контролю доступу та враховувала конкретні бізнес-потреби організації. 7.Забезпечити сталість та загальне розуміння схеми класифікації інформації. 8.Розглянути процедури для ідентифікації та класифікації інформації в угодах, які включають обмін інформацією з іншими організаціями/сторонами. 9.Розглянути життєвий цикл інформації та перегляньте класифікацію, щоб уникнути перекласифікації чи недостатньої класифікації.	1. Політика засекречування інформації. 2. Порядок регулярного перегляду, аналізу та актуалізації схеми засекречування інформації. 3. Процедури ідентифікації та класифікації інформації в угодах.		Невідповідність	0%	
5.13	Маркування інформації	Чи існує процес або процедура для забезпечення належного позначення грифу секретності інформації на кожному активі?	1.Розробити та впровадьте набір процедур для маркування інформації та інших пов'язаних активів відповідно до схеми класифікації інформації, прийнятої організацією. 2.Визначити техніки маркування. 3.Використати метадані для цифрової інформації. 4.Сповістити та навчайте персонал та інших зацікавлених сторін щодо цих процедур. 5.Застосувати класифікаційні мітки до виводу з систем. 6.Оцінити потенційні негативні ефекти.	1. Процедури маркування інформації та інших пов'язаних з нею активів або політика класифікації інформації, яка визначає вимоги до маркування.		Невідповідність	0%	

5.14	Передавання інформації	Було: 13.2.1., 13.2.2, 13.2.3 1. Чи регулює політика організації передачу інформації? 2. Чи доступні процедури передачі даних усім працівникам? 3. Чи існують відповідні технічні засоби контролю для запобігання несанкціонованій передачі даних? Чи містять контракти із зовнішніми сторонами та угоди всередині організації детальні вимоги до захисту ділової інформації під час передачі? Чи охоплює політика безпеки передачу інформації під час використання систем електронних повідомлень? Стало: 1. Чи існує політика щодо передачі інформації? 2. Чи доведена ця політика належним чином до відома відповідних зацікавлених сторін? 3. Чи існують угоди про передачу інформації з третіми сторонами?	1. Розробити політику передачі інформації. 2. Довести цю політику до відома всіх відповідних зацікавлених сторін. 3. Розробити правила, процедури та угоди про передачу інформації, які відображають класифікацію інформації, що передається, і повинні включати a) засоби контролю, призначені для захисту переданої інформації від перехоплення, несанкціонованого доступу, копіювання, модифікації, неправильної маршрутизації, знищення та відмови в обслуговуванні, включаючи рівні контролю доступу, відповідні до класифікації відповідної інформації, та будь-які спеціальні засоби контролю, необхідні для захисту конфіденційної інформації, наприклад, використання криптографічних методів; b) засоби контролю для забезпечення відстежуваності та недопущення відмови від інформації, включаючи підтримку ланцюга відповідального зберігання інформації під час транзиту; c) визначення відповідних контактів, пов'язаних з передачею, включаючи власників інформації, власників ризиків, співробітників служби безпеки та зберігачів інформації, залежно від обставин; d) обов'язки та відповідальність у випадку інцидентів з інформаційною безпекою, таких як втрата фізичних носіїв інформації або даних; e) використання узгодженої системи маркування для чутливої або критичної інформації, що забезпечує негайне розуміння значення маркування та належний захист інформації; f) надійність та доступність послуги передачі даних; g) політика або керівні принципи щодо прийнятного використання засобів передачі інформації для конкретної теми; h) інструкції щодо зберігання та утилізації всіх ділових документів, включаючи повідомлення; i) врахування будь-яких інших відповідних правових, законодавчих, регуляторних та договірних вимог, пов'язаних з передачею інформації (наприклад, вимог до електронних підписів). 4.Укласти угоди про передачу інформації з третіми сторонами.	1. Політика передачі інформації. 2. Правила та процедури передачі інформації. 3. Угоди про передачу інформації з третіми особами.		Невідповідність	0%	
5.15	Контролі доступу	Було: 9.1.1. 9.1.2 1. Чи існує задокументована політика контролю доступу? 2. Чи базується політика на бізнес-вимогах? 3. Чи доведена політика до відома	1. Встановити політику контролю доступу. 2. Впровадити правила контролю доступу, зіставивши відповідні права та обмеження доступу з відповідними суб'єктами, враховуючи а) узгодженість між правами доступу та класифікацією інформації; б) узгодженість між правами доступу та потребами і вимогами до безпеки фізичного периметру	1. Політика контролю доступу або політика управління доступом. 2. Процедури		Невідповідність	0%	

		належним чином? Чи існують засоби контролю, які гарантують, що користувачі мають доступ лише до тих мережевих ресурсів, на використання яких вони мають спеціальний дозвіл і які необхідні для виконання їхніх обов'язків? Стало: 1. Чи існують правила контролю фізичного та логічного доступу до інформації та інших пов'язаних з нею активів? 2. Чи базуються ці правила на вимогах бізнес- та інформаційної безпеки? 3. Чи визначаються вимоги інформаційної безпеки та бізнесу, пов'язані з контролем доступу, власниками інформації та інших пов'язаних з нею активів? 4. Чи існує політика контролю доступу для конкретної теми? 5. Чи повідомляється ця політика належним чином?	c) врахування всіх типів доступних з'єднань у розподілених середовищах, щоб суб'єктам надавався доступ лише до інформації та інших пов'язаних з нею активів, включаючи мережі та мережеві послуги, які вони мають право використовувати; d) розглянути, як можуть бути відображені елементи або фактори, що мають відношення до динамічного контролю доступу. 3. Впровадити принцип найменших привілеїв, коли доступ, як правило, заборонений, якщо він прямо не дозволений. 4. Розробити та задокументувати процедури, які підтримують впровадження правил контролю доступу. 5. Визначити та розподіліть обов'язки щодо контролю доступу. 6. Оцінити та обрати відповідні моделі контролю доступу, такі як MAC, DAC, RBAC або ABAC, виходячи з потреб та вимог організації.	підтримки реалізації правил контролю доступу.				
5.16	Управління ідентифікаційними даними	Було: 9.2.1. 1. Чи існує офіційний процес реєстрації доступу користувачів? Стало: 1. Чи існує процес управління повним життєвим циклом ідентичностей? 2. Чи існує допоміжний процес для обробки змін до інформації, пов'язаної з ідентифікаційними даними користувачів? 3. Чи забезпечують ідентичності третіх сторін необхідний рівень довіри? 4. Чи відомі будь-які пов'язані з цим ризики та чи достатньо вони враховані?	1. Розробити та впровадити процеси управління ідентифікаційними даними, які мають забезпечити, щоб a) для ідентифікаторів, присвоєних особам, конкретний ідентифікатор пов'язувався лише з однією особою, щоб можна було притягнути цю особу до відповідальності за дії, вчинені з використанням цього конкретного ідентифікатора; b) ідентифікатори, присвоєні кільком особам (наприклад, спільні ідентифікатори), дозволені лише тоді, коли вони необхідні з ділових або оперативних причин, і підлягають спеціальному затвердженню та документуванню; c) ідентифікатори, присвоєні об'єктам, що не є людьми, підлягають відповідному окремому затвердженню та незалежному постійному нагляду; d) ідентичності відключалися або своєчасно видалялися, якщо вони більше не потрібні (наприклад, якщо пов'язані з ними сутності видаляються або більше не використовуються, або якщо особа, пов'язана з ідентичністю, покинула організацію чи змінила роль);	1. Процедура управління ідентифікацією або Політика управління доступом з вимогами до управління ідентифікацією. 2. Процедура роботи з ідентифікаційною інформацією користувачів.		Невідповідність	0%	

			e) у конкретному домені одна особа співвідноситься з одним об'єктом [тобто уникається співставлення кількох осіб з одним об'єктом в одному контексті (дублікатів)]; f) ведуться записи всіх важливих подій, що стосуються використання та управління ідентифікаційними даними користувачів та автентифікаційною інформацією. 2. Розробити допоміжний процес для обробки змін в ідентифікаційній інформації користувача, який може включати повторну перевірку довірених документів, пов'язаних з особою. 3. Оцінити та забезпечити, щоб ідентифікаційні дані третіх осіб відповідали необхідному рівню довіри, а пов'язані з ними ризики були відомі та належним чином враховані. 4. Переконайтеся, що процес надання або відкликання прав доступу до ідентифікаційних даних узгоджується з відповідними рішеннями про надання дозволів або повноважень.					
5.17	Інформація для автентифікації	Було: 9.2.4, 9.3.1., 9.4.3 Чи існує формальний процес управління для контролю за розподілом секретної автентифікаційної інформації? 1. Чи існує політичний документ, що охоплює практику організації щодо поводження з секретною автентифікаційною інформацією? 2. Чи доведена вона до відома всіх користувачів? 1. Чи є системи паролів інтерактивними? 2. Чи потрібні складні паролі? Стало: 1. Чи існує процес управління для розподілу та управління автентифікаційною інформацією? 2. Чи проінструктований персонал щодо належного поводження з автентифікаційною інформацією?	1. Розробити та впровадити процес управління для розподілу та управління автентифікаційною інформацією, який гарантує, що а) персональні паролі або персональні ідентифікаційні номери (PIN-коди), що генеруються автоматично під час реєстрації як тимчасова секретна автентифікаційна інформація, не можуть бути вгадані та унікальні для кожної особи, і що користувачі зобов'язані змінювати їх після першого використання; б) встановлені процедури для перевірки особи користувача перед наданням нової, заміни або тимчасової автентифікаційної інформації; c) автентифікаційна інформація, включаючи тимчасову автентифікаційну інформацію, передається користувачам у безпечний спосіб (наприклад, автентифікованим та захищеним каналом) та уникається використання незахищених (відкритих текстових) повідомлень електронної пошти для цієї мети; d) користувачі підтверджують отримання автентифікаційної інформації; e) інформація для автентифікації за замовчуванням, визначена заздалегідь або надана постачальниками, змінюється одразу після встановлення систем або програмного забезпечення; f) ведеться облік важливих подій, пов'язаних з розподілом та управлінням автентифікаційною інформацією, забезпечується їхня конфіденційність, а також затверджується метод ведення обліку (наприклад, за допомогою затвердженого інструменту для зберігання паролів). 2. Визначити обов'язки користувачів щодо поводження з автентифікаційною інформацією. 3. Впровадити систему управління паролями.	1. Процедура управління розподілом секретної автентифікаційної інформації. 2. Система управління паролями. 3. Політика паролів.		Невідповідність	0%	

			4. Вести облік важливих подій, пов'язаних з розподілом та управлінням автентифікаційною інформацією, забезпечуючи їх конфіденційність. 5. Розглянути можливість використання єдиного входу (SSO) або інших інструментів управління автентифікацією (наприклад, сховища паролів), щоб зменшити кількість автентифікаційних даних, які користувачі повинні захищати, та підвищити ефективність контролю автентифікації. 6. Регулярно переглядати та оновлювати процеси та процедури управління автентифікаційною інформацією. 7. Проводити тренінги для навчання персоналу належному поводженню з автентифікаційною інформацією. 8. Забезпечити відповідність чинним законодавчим та нормативним вимогам щодо управління та захисту автентифікаційної інформації. 9. Проводити періодичні аудити або оцінки для перевірки ефективності процесу управління автентифікаційною інформацією.					
5.18	Права доступу	Було: 9.2.2, 9.2.5, 9.2.6 Чи існує формальний процес надання доступу користувачам для призначення прав доступу для всіх типів користувачів та послуг? 1. Чи існує процес регулярного перегляду власниками активів прав доступу до своїх активів? 2. Чи перевіряється цей процес перегляду? Чи існує процес, який гарантує, що права доступу користувача будуть видалені після закінчення трудового договору або контракту, або скориговані після зміни ролі? 1. Чи є системи паролів інтерактивними? 2. Чи потрібні складні паролі? Стало: 1. Чи існує процес надання, перегляду, модифікації прав доступу до інформації та інших пов'язаних з нею активів? 2. Чи існує процес регулярного перегляду прав доступу?	1. Встановити процедуру надання або відкликання прав доступу, яка повинна включати a) отримання дозволу від власника інформації та інших пов'язаних з нею активів на використання інформації та інших пов'язаних з нею активів. Окреме затвердження прав доступу керівництвом також може бути доречним; б) врахування бізнес-вимог, а також політики та правил організації щодо контролю доступу до конкретної тематики в) розглянути питання про розподіл обов'язків, включаючи розподіл ролей затвердження та реалізації прав доступу, а також розмежування конфліктуючих ролей; d) забезпечення видалення прав доступу, коли комусь не потрібен доступ до інформації та інших пов'язаних з нею активів, зокрема забезпечення своєчасного видалення прав доступу користувачів, які звільнилися з організації; e) розглянути можливість надання тимчасових прав доступу на обмежений період часу та відкликання їх після закінчення терміну дії, зокрема, для тимчасового персоналу або тимчасового доступу, необхідного персоналу; f) перевірка того, що рівень наданого доступу відповідає політиці управління доступом для конкретної теми та узгоджується з іншими вимогами інформаційної безпеки, такими як розподіл обов'язків; g) забезпечення того, щоб права доступу активувалися (наприклад, постачальниками послуг) лише після успішного завершення процедур авторизації;	1. Політика управління доступом або процедура надання або відкликання прав доступу до інформації та інших пов'язаних з нею активів. 2. Процедура регулярного перегляду прав доступу. 3. Процедура перегляду, коригування або відкликання прав доступу перед зміною або припиненням трудових відносин.		Невідповідність	0%	

		3. Чи існує процес, який гарантує, що права доступу користувача будуть видалені після закінчення трудового договору або контракту, або скориговані після зміни ролі?	h) ведення центрального обліку прав доступу, наданих ідентифікатору користувача (ідентифікатору, логічному або фізичному) для доступу до інформації та інших пов'язаних з нею активів; i) модифікація прав доступу користувачів, які змінили роль або посаду; к) видалення або коригування фізичних та логічних прав доступу, що може бути здійснено шляхом вилучення, анулювання або заміни ключів, автентифікаційної інформації, ідентифікаційних карток або підписок; k) ведення обліку змін логічних та фізичних прав доступу користувачів. 2. Розглянути процес регулярного перегляду прав доступу. 3. Розглянути процес перегляду, коригування або видалення прав доступу перед змінами або припиненням трудових відносин. 4. Встановіть ролі доступу користувачів на основі бізнес-вимог, які узагальнюють ряд прав доступу в типові профілі доступу користувачів. 5. Включіть в контракти пункти, що стосуються санкцій за спроби несанкціонованого доступу. 6. Знизити ризики, пов'язані з клонуванням прав доступу.					
5.19	Інформаційна безпека у взаємодії з постачальниками	Було: 15.1.1 1. Чи включено питання інформаційної безпеки в контракти, укладені з постачальниками та надавачами послуг? 2. Чи існує загальноорганізаційний підхід до управління ризиками у взаємодії з постачальниками? Стало: 1. Чи існує політика управління ризиками інформаційної безпеки, пов'язаними з використанням продуктів або послуг постачальника?	1. Розробити політику взаємодії з постачальниками. 2. Довести цю політику до відома всіх відповідних зацікавлених сторін. 3. Визначити та впровадити процеси та процедури для усунення ризиків безпеки, пов'язаних з використанням продуктів та послуг, що надаються постачальниками. 4. Забезпечити, щоб такі процеси та процедури включали ті, які має впроваджувати організація, а також ті, які організація вимагає впровадити від постачальника, як-от а) визначення та документування типів постачальників (наприклад, послуг ІКТ, логістики, комунальних послуг, фінансових послуг, компонентів інфраструктури ІКТ), які можуть впливати на конфіденційність, цілісність та доступність інформації організації б) визначення того, як оцінювати та обирати постачальників відповідно до чутливості інформації, продуктів та послуг (наприклад, за допомогою аналізу ринку, рекомендацій клієнтів, вивчення документів, оцінки на місці, сертифікації); с) оцінювання та вибір продуктів чи послуг постачальника, які мають адекватні засоби контролю інформаційної безпеки, та їх перевірка; зокрема, точність та повнота засобів контролю, впроваджених постачальником, які забезпечують цілісність інформації та обробки інформації постачальника, а отже, і	1. Політика безпеки постачальника (Політика безпеки зовнішнього постачальника).		Невідповідність	0%	

			інформаційну безпеку організації; d) визначення інформації, послуг ІКТ та фізичної інфраструктури організації, до яких постачальники можуть мати доступ, відстежувати, контролювати або використовувати; e) визначення типів компонентів інфраструктури ІКТ та послуг, що надаються постачальниками, які можуть впливати на конфіденційність, цілісність та доступність інформації організації; f) оцінка та управління ризиками інформаційної безпеки, пов'язаними з 1) використанням постачальниками інформації та інших пов'язаних з нею активів організації, включаючи ризики, що походять від потенційно зловмисного персоналу постачальника 2) несправністю або вразливістю продуктів (включаючи програмні компоненти та підкомпоненти, що використовуються в цих продуктах) або послуг, що надаються постачальниками; g) моніторинг дотримання встановлених вимог інформаційної безпеки для кожного типу постачальника та типу доступу, включаючи перевірку третьою стороною та валідацію продуктів; h) пом'якшення наслідків невідповідності постачальника, незалежно від того, чи було це виявлено в ході моніторингу або іншими способами; i) вирішення інцидентів та непередбачуваних ситуацій, пов'язаних з продукцією та послугами постачальника, включаючи відповідальність як організації, так і постачальників; j) відмовостійкість та, за необхідності, заходи з відновлення та реагування на непередбачувані ситуації для забезпечення доступності інформації постачальника та обробки інформації, а отже, доступності інформації організації; k) інформування та навчання персоналу організації, який взаємодіє з персоналом постачальника, щодо відповідних правил взаємодії, тематичних політик, процесів та процедур, а також поведінки залежно від типу постачальника та рівня доступу постачальника до систем та інформації організації; l) управління необхідною передачею інформації, інших пов'язаних з нею активів та всього іншого, що потребує змін, а також забезпечення підтримки інформаційної безпеки протягом усього періоду передачі; m) вимоги щодо забезпечення безпечного припинення відносин з постачальником, включаючи 1) скасування прав доступу 2) поводження з інформацією 3) визначення права власності на інтелектуальну власність, розроблену під час співпраці				

			4) перенесення інформації у разі зміни постачальника або переходу на інсорсинг 6) управління записами;					
5.20	Вирішення питань інформаційної безпеки в угодах з постачальниками	Було: 15.1.2. 1. Чи надаються постачальникам задокументовані вимоги до безпеки? 2. Чи контролюється та відстежується доступ постачальників до інформаційних активів та інфраструктури? Стало (БЕЗ ЗМІН:: 1. Чи надаються постачальникам задокументовані вимоги безпеки? 2. Чи контролюється та відстежується доступ постачальників до інформаційних активів та інфраструктури?	1. Укласти та задокументуйте угоди з постачальниками, щоб забезпечити чітке розуміння між організацією та постачальником щодо зобов'язань обох сторін виконувати відповідні вимоги інформаційної безпеки. 2. Створити та вести реєстр угод із зовнішніми сторонами, щоб відстежувати, куди йде їхня інформація. 3. Запровадити процес регулярного перегляду, перевірки та оновлення угод із зовнішніми сторонами, щоб переконатися, що вони все ще необхідні та відповідають цілям, а також містять відповідні положення щодо інформаційної безпеки.	1. Політика безпеки постачальника (Політика безпеки зовнішнього постачальника).		Невідповідність	0%	
5.21	Управління інформаційною безпекою в ланцюгу постачання інформаційно-комунікаційних технологій (ІКТ)	Було: 15.1.3 Чи включають угоди з постачальниками вимоги щодо забезпечення інформаційної безпеки в ланцюжку постачання послуг та продуктів? Стало: 1. Чи існує політика управління ризиками інформаційної безпеки, пов'язаними з ланцюгом постачання продуктів та послуг ІКТ?	1. Визначити та впровадити процеси та процедури для управління ризиками інформаційної безпеки, пов'язаними з ланцюжком постачання продуктів та послуг ІКТ, які повинні враховувати наступні теми: а) визначення вимог до інформаційної безпеки, що застосовуються до придбання продуктів та послуг ІКТ; б) вимога до постачальників послуг ІКТ поширювати вимоги безпеки організації по всьому ланцюгу постачання, якщо вони укладають субпідрядні договори на частини послуг ІКТ, що надаються організації; с) вимагати, щоб постачальники продуктів ІКТ поширювали відповідні практики безпеки по всьому ланцюгу постачання, якщо ці продукти включають компоненти, придбані або отримані від інших постачальників або інших суб'єктів (наприклад, субпідрядних розробників програмного забезпечення та постачальників апаратних компонентів) г) вимагати від постачальників продуктів ІКТ надання інформації, що описує програмні компоненти, які використовуються в продуктах; е) вимагати від постачальників продуктів ІКТ надання інформації, що описує реалізовані функції безпеки їхніх продуктів та конфігурацію, необхідну для їхньої безпечної роботи; f) впровадження процесу моніторингу та прийнятних методів перевірки відповідності поставлених продуктів та послуг ІКТ	1. Реєстр безпеки сторонніх постачальників. 2. Вимоги до інформаційної безпеки для ІТК (інформаційно-комунікаційних технологій).		Невідповідність	0%	

			заявленим вимогам безпеки. Прикладами таких методів перевірки постачальників можуть бути тестування на проникнення та підтвердження або валідація атестацій третьої сторони щодо операцій постачальника з інформаційної безпеки; g) впровадження процесу ідентифікації та документування компонентів продукту або послуги, які є критично важливими для підтримання функціональності і тому потребують підвищеної уваги, перевірки та подальшого контролю, особливо якщо вони створені за межами організації, особливо якщо постачальник передає аспекти компонентів продукту або послуги на аутсорсинг іншим постачальникам; h) отримання впевненості в тому, що критичні компоненти та їх походження можна простежити по всьому ланцюгу постачання; i) отримання впевненості в тому, що поставлені продукти ІКТ функціонують відповідно до очікувань без будь-яких неочікуваних або небажаних особливостей; j) впровадження процесів, які гарантують, що компоненти від постачальників є справжніми і не відрізняються від їхньої специфікації. Приклади таких заходів включають маркування проти несанкціонованого втручання, перевірку криптографічного хешу або цифровий підпис. Моніторинг продуктивності, що не відповідає специфікації, може бути індикатором втручання або підробки. Запобігання та виявлення несанкціонованого втручання повинно здійснюватися на різних етапах життєвого циклу розробки системи, включаючи проектування, розробку, інтеграцію, експлуатацію та технічне обслуговування; k) отримання гарантій того, що продукти ІКТ досягають необхідних рівнів безпеки, наприклад, через офіційну сертифікацію або схему оцінювання, таку як Угода про визнання загальних критеріїв (Common Criteria Recognition Arrangement) l) визначення правил обміну інформацією щодо ланцюга постачання та будь-яких потенційних проблем і компромісів між організацією та постачальниками; m) впровадження конкретних процесів для управління життєвим циклом і доступністю компонентів ІКТ та пов'язаними з ними ризиками безпеки. Це включає управління ризиками відсутності компонентів через те, що постачальники більше не працюють, або постачальники більше не надають ці компоненти через технологічний прогрес. Слід розглянути можливість визначення альтернативного постачальника та процес передачі програмного забезпечення та компетенції альтернативному постачальнику. 2. Переконатися, що ІКТ придбані з надійних джерел, і враховуйте				

			репутацію постачальника при прийнятті надійних рішень щодо систем контролю якості.					
5.22	Моніторинг, аналіз та управління змінами послуг постачальників	Було: 15.2.1, 15.2.2 Чи підлягають постачальники регулярній перевірці та аудиту? Чи підлягають зміни у наданні послуг процесу управління, який включає оцінку безпеки та ризиків? Стало: 1. Чи підлягають перевірці та оцінці практики інформаційної безпеки постачальника та надання послуг? 2. Чи змінюються практики інформаційної безпеки постачальника та надання послуг за необхідності? 3. ***	1. Призначити особу або групу осіб, відповідальних за управління відносинами з постачальниками та моніторинг практики інформаційної безпеки і надання послуг. 2. Запровадити процес регулярного моніторингу, аналізу та управління змінами в рівнях якості послуг постачальників для забезпечення дотримання умов угод з постачальниками.	1. Політика безпеки постачальника (Політика безпеки зовнішнього постачальників).		Невідповідність	0%	
5.23	Інформаційна безпека при використанні хмарних сервісів	1. Чи існує політика щодо використання хмарних сервісів, включаючи процеси придбання, використання, управління та виходу з хмарних сервісів? 2. Чи доведена вона до відома всіх відповідних зацікавлених сторін? 3. ?	1. Розробити політику використання хмарних сервісів (політику використання хмарних сервісів) 2. Довести цю політику до відома всіх відповідних зацікавлених сторін. 3. Визначити та доведіть до відома процес управління ризиками інформаційної безпеки, пов'язаними з використанням хмарних сервісів. 4. Чітко визначити обов'язки постачальника хмарних послуг та організації як замовника хмарних послуг. 5. Визначити наступне: а) всі відповідні вимоги до інформаційної безпеки, пов'язані з використанням хмарних сервісів; б) критерії вибору хмарних сервісів та сферу використання хмарних сервісів с) ролі та обов'язки, пов'язані з використанням хмарних сервісів та управлінням ними г) якими засобами контролю інформаційної безпеки керує постачальник хмарних послуг, а якими - організація як замовник хмарних послуг; е) як отримати та використовувати можливості інформаційної безпеки, що надаються постачальником хмарних послуг; f) як отримати впевненість щодо засобів контролю інформаційної безпеки, впроваджених постачальниками хмарних послуг; g) як управляти засобами контролю, інтерфейсами та змінами в сервісах, коли організація використовує декілька хмарних сервісів,	1. Політика безпеки хмари. 2. Угоди про надання хмарних послуг.		Невідповідність	0%	

			зокрема від різних постачальників хмарних сервісів; h) процедури реагування на інциденти інформаційної безпеки, що виникають у зв'язку з використанням хмарних сервісів; i) підхід до моніторингу, аналізу та оцінки поточного використання хмарних сервісів для управління ризиками інформаційної безпеки; к) як змінити або припинити використання хмарних сервісів, включаючи стратегії виходу з хмарних сервісів. 6. Проаналізувати та оцінити угоди про хмарні сервіси з постачальниками хмарних послуг та переконатися, що ці угоди враховують вимоги організації щодо конфіденційності, цілісності, доступності та обробки інформації, а також відповідні цілі щодо рівня хмарних сервісів та цілі щодо якості хмарних сервісів. 7. Проводити оцінку ризиків для виявлення ризиків, пов'язаних з використанням хмарних сервісів. 8. Забезпечити, щоб будь-які залишкові ризики, пов'язані з використанням хмарних сервісів, були чітко визначені та прийняті відповідним керівництвом організації. 9. Переконатися, що угоди між постачальниками хмарних послуг та організацією включають наступні положення: а) надання рішень, що базуються на прийнятих в галузі стандартах архітектури та інфраструктури; б) управління контролем доступу до хмарного сервісу відповідно до вимог організації в) впровадження рішень для моніторингу та захисту від шкідливого програмного забезпечення г) обробка та зберігання конфіденційної інформації організації у затверджених місцях (наприклад, у певній країні чи регіоні) або в межах певної юрисдикції чи під її юрисдикцією; е) надання спеціалізованої підтримки у випадку інциденту інформаційної безпеки в середовищі хмарних сервісів; f) забезпечення дотримання вимог інформаційної безпеки організації у випадку подальшої передачі хмарних послуг на субпідряд зовнішньому постачальнику (або заборона передачі хмарних послуг на субпідряд); g) підтримка організації у зборі цифрових доказів з урахуванням законів та правил щодо цифрових доказів у різних юрисдикціях; h) забезпечення належної підтримки та доступності послуг протягом відповідного періоду часу, коли організація захоче вийти з хмарного сервісу; i) забезпечення необхідного резервного копіювання даних та інформації про конфігурацію, а також безпечного управління резервними копіями, залежно від можливостей постачальника хмарних послуг, яким користується організація, виступаючи в ролі				

			замовника хмарних послуг; к) надання та повернення інформації, такої як конфігураційні файли, вихідний код та дані, що є власністю організації, яка виступає в якості замовника хмарних послуг, за запитом під час надання послуг або при припиненні надання послуг. 10. Розглянути, чи повинні такі угоди вимагати від постачальників хмарних послуг надавати попереднє повідомлення до внесення будь-яких суттєвих змін, що впливають на клієнта, до способу надання послуг організації, включаючи а) зміни в технічній інфраструктурі (наприклад, переміщення, реконфігурація або зміни в апаратному чи програмному забезпеченні), які впливають або змінюють пропозицію хмарних послуг б) обробку або зберігання інформації в новій географічній або юридичній юрисдикції; в) використання постачальників хмарних послуг або інших субпідрядників (включаючи зміну існуючих або залучення нових сторін). 11. Налагодити регулярну комунікацію з постачальниками хмарних послуг з метою обміну інформацією про інформаційну безпеку та моніторингу характеристик послуг, а також повідомляти про порушення зобов'язань, передбачених угодами.					
5.24	Планування та підготовка до управління інцидентами інформаційної безпеки	Було: 16.1.1 Чи чітко визначені та задокументовані обов'язки керівництва в процесах управління інцидентами? Стало: 1. Чи чітко визначені та задокументовані процеси управління інцидентами інформаційної безпеки, ролі та обов'язки в процесах управління інцидентами? 2. Чи доведено їх до відома відповідних внутрішніх та зовнішніх зацікавлених сторін?	1. Визначити процеси управління інцидентами інформаційної безпеки, ролі та обов'язки, враховуючи наступне: а) встановлення загального методу звітування про події інформаційної безпеки, включаючи контактну особу; б) створення процесу управління інцидентами для забезпечення організації можливостями управління інцидентами інформаційної безпеки, включаючи адміністрування, документування, виявлення, сортування, визначення пріоритетів, аналіз, комунікацію та координацію зацікавлених сторін; c) створення процесу реагування на інциденти, щоб забезпечити організацію можливостями для оцінки, реагування та отримання уроків з інцидентів інформаційної безпеки; d) допуск лише компетентного персоналу до вирішення питань, пов'язаних з інцидентами інформаційної безпеки в організації. Такий персонал повинен бути забезпечений процедурною документацією та періодичним навчанням; e) створення процесу для визначення необхідного навчання, сертифікації та постійного професійного розвитку для персоналу, що реагує на інциденти. 2. Довести їх до відома відповідних внутрішніх та зовнішніх зацікавлених сторін.	1. Політика управління інцидентами. 2. План реагування на інциденти. 3. Реєстр інцидентів. 4. Задокументовані процедури звітності.		Невідповідність	0%	

			3. Впровадити процедури управління інцидентами. 4. Обговорити та узгодити з керівництвом цілі управління інцидентами інформаційної безпеки. 5. Переконатися, що відповідальні особи за управління інцидентами інформаційної безпеки розуміють пріоритети організації щодо обробки інцидентів інформаційної безпеки, включаючи часові рамки вирішення на основі потенційних наслідків та серйозності. 6. Забезпечити створення плану управління інцидентами інформаційної безпеки з урахуванням різних сценаріїв, а також розробити та впровадити процедури для наступних видів діяльності: a) оцінка подій інформаційної безпеки відповідно до критеріїв того, що є інцидентом інформаційної безпеки; б) моніторинг, виявлення, класифікація, аналіз та звітування про події та інциденти інформаційної безпеки (за допомогою людини або автоматизованих засобів) в) управління інцидентами інформаційної безпеки до завершення, включаючи реагування та ескалацію, відповідно до типу та категорії інциденту, можливу активацію кризового управління та активацію планів безперервності, контрольоване відновлення після інциденту та комунікацію з внутрішніми та зовнішніми зацікавленими сторонами; d) координація з внутрішніми та зовнішніми зацікавленими сторонами, такими як органи влади, зовнішні зацікавлені групи та форуми, постачальники та клієнти; e) ведення журналів діяльності з управління інцидентами; f) обробка доказів; g) аналіз першопричини або процедури розтину; h) визначення отриманих уроків та будь-яких необхідних вдосконалень процедур управління інцидентами або засобів контролю інформаційної безпеки в цілому. 7. Встановити процедури звітування, які повинні включати а) дії, яких слід вжити у разі виникнення інциденту інформаційної безпеки (наприклад, негайно зафіксувати всі відповідні деталі, такі як несправність, що виникла, та повідомлення на екрані, негайно повідомити контактну особу та вжити лише скоординованих заходів); б) використання форм інцидентів для підтримки персоналу у виконанні всіх необхідних дій при повідомленні про інциденти інформаційної безпеки; в) відповідні процеси зворотного зв'язку для забезпечення того, щоб особи, які повідомляють про інциденти інформаційної				

			безпеки, були поінформовані, наскільки це можливо, про результати після того, як проблема була вирішена та закрита; d) створення звітів про інциденти. 8. Враховувати будь-які зовнішні вимоги щодо звітування про інциденти відповідним зацікавленим сторонам у визначені строки. 9. Налагодити процес координації реагування та обміну інформацією про інциденти інформаційної безпеки із зовнішніми організаціями за необхідності.					
5.25	Оцінка та прийняття рішень щодо подій у сфері інформаційної безпеки	Було: 16.1.4 Чи існує процес, який забезпечує належну оцінку та класифікацію подій інформаційної безпеки? Стало: Чи існує процес, що забезпечує належну оцінку та категоризацію подій інформаційної безпеки?	1. Розробити схему категоризації та пріоритезації інцидентів інформаційної безпеки, яка включає критерії віднесення подій до інцидентів інформаційної безпеки. 2. Призначити відповідальну особу як контактну особу для оцінки та категоризації подій інформаційної безпеки за узгодженою схемою. 3. Налагодити процес оцінки та прийняття рішень щодо кожної події інформаційної безпеки з урахуванням схеми категоризації та визначення пріоритетів. 4. Створити журнал або базу даних для зберігання результатів оцінок та прийнятих рішень щодо подій інформаційної безпеки з метою подальшого використання та перевірки.	1. Політика управління інцидентами. 2. План реагування на інциденти. 3. Задокументовані процедури звітності.		Невідповідність	0%	
5.26	Реагування на інциденти інформаційної безпеки	БЕЗ ЗМІН:Чи існує процес реагування на інциденти, який відображає класифікацію та серйозність інцидентів інформаційної безпеки?	1. Розробити та задокументувати процедури реагування на інциденти інформаційної безпеки. 2. Довести ці процедури до відома всіх відповідних зацікавлених сторін. 3. Створити групу, відповідальну за реагування на інциденти інформаційної безпеки. 4. Переконатися, що реагування включає наступне: a) ізоляцію, якщо наслідки інциденту можуть поширитися, систем, які постраждали від інциденту; б) збір доказів якомога швидше після інциденту c) ескалацію, за необхідності, включаючи заходи з управління кризовими ситуаціями та, можливо, залучення планів безперервності бізнесу; d) забезпечення належної реєстрації всіх заходів реагування для подальшого аналізу; e) інформування про існування інциденту інформаційної безпеки або будь-які відповідні деталі інциденту всім відповідним внутрішнім та зовнішнім зацікавленим сторонам, дотримуючись принципу необхідності знати; f) координація дій з внутрішніми та зовнішніми сторонами, такими як органи влади, зовнішні зацікавлені групи та форуми, постачальники та клієнти, з метою підвищення ефективності реагування та мінімізації наслідків для інших організацій;	1. Політика управління інцидентами. 2. План реагування на інциденти.		Невідповідність	0%	

			g) після успішного вирішення інциденту, офіційне закриття та реєстрація інциденту; h) проведення судової експертизи інформаційної безпеки, за необхідності; i) проведення аналізу після інциденту для виявлення першопричини. Забезпечити його документування та інформування відповідно до визначених процедур; к) виявлення та усунення вразливостей та слабких місць в інформаційній безпеці, в тому числі тих, що стосуються засобів контролю, які спричинили інцидент, сприяли йому або не змогли йому запобігти.					
5.27	Навчання на інцидентах інформаційної безпеки	Було 16.1.6 Чи існує процес або структура, яка дозволяє організації вчитися на інцидентах інформаційної безпеки та зменшувати вплив / ймовірність майбутніх подій? Стало: Чи існує процес або структура, яка дозволяє організації вчитися на інцидентах інформаційної безпеки та посилювати і вдосконалювати засоби контролю інформаційної безпеки?	1. Встановити процедури для кількісної оцінки та моніторингу типів, обсягів та вартості інцидентів інформаційної безпеки. 2. На основі інформації, отриманої в результаті оцінки інцидентів інформаційної безпеки, впровадити наступне: а) вдосконалити план управління інцидентами, включаючи сценарії та процедури реагування на інциденти; б) виявити повторювані або серйозні інциденти та їх причини для оновлення оцінки ризиків інформаційної безпеки організації, а також визначити та впровадити необхідні додаткові засоби контролю для зменшення ймовірності або наслідків майбутніх подібних інцидентів. Механізми для цього включають збір, кількісну оцінку та моніторинг інформації про типи інцидентів, їх обсяги та витрати; c) підвищити рівень обізнаності та підготовки користувачів шляхом надання прикладів того, що може статися, як реагувати на такі інциденти та як уникнути їх у майбутньому.	1.Політика управління інцидентами. 2.Процедури вивчення уроків з інцидентів.		Невідповідність	0%	
5.28	Збір доказової бази	Було: 16.1.7 1. Чи існує політика готовності до криміналістичної експертизи? 2. У випадку інциденту інформаційної безпеки чи збираються відповідні дані таким чином, щоб їх можна було використати як докази?	1. Розробити внутрішні процедури управління доказами, пов'язаними з подіями інформаційної безпеки. 2. Проаналізувати та врахуйте вимоги різних юрисдикцій, щоб гарантувати, що процедури управління доказами максимізують шанси на прийняття доказів у відповідних юрисдикціях. 3) Забезпечити, щоб ці внутрішні процедури містили інструкції щодо ідентифікації, збору та отримання доказів на основі різних типів носіїв інформації, пристроїв та стану пристроїв (наприклад, увімкненого чи вимкненого). 4. Забезпечити, щоб процедури управління доказами були встановлені таким чином, щоб докази збиралися та зберігалися у спосіб, прийнятний для національних судів або інших дисциплінарних органів. 5. Забезпечити наступне: а) записи є повними та не були підроблені в будь-який спосіб; b) копії електронних доказів, ймовірно, ідентичні оригіналам	1. Політика управління інцидентами. 2. Процедури управління доказами.		Невідповідність	0%	

			c) будь-яка інформаційна система, з якої були зібрані докази, працювала належним чином під час запису доказів. 6. Вивчити наявні сертифікати або відповідні засоби кваліфікації для персоналу та інструментів, задіяних в управлінні доказами. 7. Розробити процеси для вирішення ситуацій, коли цифрові докази виходять за межі організації або юрисдикції. 8. Залучити юридичну консультацію або правоохоронні органи на ранніх стадіях у ситуаціях, коли розглядається можливість судового позову, для отримання рекомендацій щодо необхідних доказів.					
5.29	Інформаційна безпека під час збоїв у роботі	Було: 17.1.1, 17.1.2, 17.1.3 Чи включено інформаційну безпеку до планів забезпечення безперервності діяльності організації? Чи задокументовані, впроваджені та підтримуються в робочому стані процеси забезпечення безперервності надання послуг у несприятливих ситуаціях, які здійснює служба інформаційної безпеки організації? Чи підтверджуються та перевіряються плани безперервності через регулярні проміжки часу? Стало: 1. Чи включено питання інформаційної безпеки до планів забезпечення безперервності діяльності організації? 2. Чи чітко визначені вимоги до адаптації засобів контролю інформаційної безпеки під час збоїв? 3. Чи перевіряються, аналізуються та оцінюються плани інформаційної безпеки організації для підтримання або відновлення безпеки інформації критично важливих бізнес-процесів після переривання або збою?	0. Розробити політику безперервності бізнесу. 1. Визначити вимоги до адаптації засобів контролю інформаційної безпеки під час збоїв. 2. Включити вимоги інформаційної безпеки в процеси управління безперервністю бізнесу в організації. 3. Розробити та впровадити плани забезпечення безперервності бізнесу для підтримки або відновлення безпеки інформації критично важливих бізнес-процесів під час та після переривання або збою, включаючи відповідні часові рамки. 4. Встановити процедуру перегляду та оцінки таких планів через регулярні проміжки часу. 5. Впровадити та підтримувати засоби контролю інформаційної безпеки, допоміжні системи та інструменти в рамках планів забезпечення безперервності діяльності та безперервності ІКТ. 6. Впровадити процеси для забезпечення постійної підтримки існуючих засобів контролю інформаційної безпеки під час збоїв у роботі.	1. Політика безперервності бізнесу та/або плани безперервності бізнесу. 2. Плани аварійного відновлення для підтримки або відновлення безпеки інформації критично важливих бізнес-процесів.		Невідповідність	0%	
5.30	Готовність ІКТ до безпере	Організація повинна визначити та обрати стратегії забезпечення безперервності ІКТ, які враховують варіанти дій до, під час та після збоїв. На основі цих стратегій слід розробити,	Встановити політику контингентності бізнесу. Провести аналіз впливу на бізнес (BIA) для ідентифікації та визначення пріоритетів критичних бізнес-процесів, пов'язаних із послугами інформаційно-комунікаційних технологій (ІКТ), а також їхні об'єкти відновлення (RTO) та об'єкти відновлення точки (RPO).	1. Політика безперервності бізнесу. 2. Резюме аналізу впливу		Невідповідність	0%	

	рвності бізнесу	впровадити та протестувати плани для забезпечення необхідного рівня доступності послуг ІКТ та у необхідні терміни після переривання або збою критично важливих процесів. Чи існує процедура захисту цілей безперервності діяльності та вимог до безперервності ІКТ?	На основі результатів BIA та оцінки ризиків ідентифікувати та оберати стратегії ІКТ-контингентності для перед, під час та після збою. Розробити та впровадити плани ІКТ-контингентності, включаючи процедури реагування та відновлення для управління перебоями в ІКТ-сервісах. Забезпечити, що: a) встановлена відповідна організаційна структура для підготовки, пом'якшення та реагування на перебіг, підтримана персоналом з необхідною відповідальністю, повноваженнями та компетентністю; b) плани ІКТ-контингентності, включаючи процедури реагування та відновлення, які визначають, як організація планує управляти перебоями в ІКТ-сервісах: регулярно оцінюються через вправи та тести; схвалені керівництвом; c) плани ІКТ-контингентності включають таку інформацію ІКТ-контингентності: характеристики продуктивності та потужності для відповідності вимогам та цілям контингентності бізнесу, визначеним в BIA; RTO для кожного пріоритетного ІКТ-сервісу та процедури для відновлення цих компонентів; RPO для пріоритетних ресурсів ІКТ, визначених як інформація, та процедури для відновлення цієї інформації.	на бізнес. 3. Цілі та стратегія безперервності бізнесу. 4. План забезпечення безперервності бізнесу.				
5.31	Юридичні, законодавчі, регулятивні та договірні вимоги	Було: 18.1.1, 18.1.5 1. Чи визначила та задокументувала організація всі відповідні законодавчі, регуляторні або договірні вимоги, пов'язані з безпекою? 2. Чи задокументовано дотримання вимог? Чи захищені засоби криптографічного контролю згідно з усіма відповідними угодами, законодавчими та нормативними актами? Стало: 1. Чи визначила та задокументувала організація всі відповідні законодавчі, нормативні та договірні вимоги, пов'язані з безпекою? 2. Чи задокументовано дотримання	1. Визначити та задокументуйте всі відповідні правові, статутні, регуляторні та договірні вимоги, пов'язані з інформаційною безпекою. 2. Налагодити процес регулярного перегляду та моніторингу змін у законодавстві та нормативних актах, щоб бути в курсі будь-яких модифікацій або нових вимог. 3. Визначити та задокументувати конкретні процеси та індивідуальні обов'язки для забезпечення відповідності визначеним правовим, законодавчим, нормативним та договірним вимогам. 4. Забезпечити дотримання відповідних угод, законів та нормативно-правових актів, що стосуються наступних пунктів: а) обмеження на імпорт або експорт комп'ютерного обладнання та програмного забезпечення для виконання криптографічних функцій; б) обмеження на імпорт або експорт комп'ютерного обладнання та програмного забезпечення, яке призначене для додавання до нього криптографічних функцій в) обмеження на використання криптографії;	1. Задокументували всі юридичні, законодавчі, нормативні та договірні вимоги, пов'язані з інформаційною безпекою.		Невідповідність	0%	

		вимог? 3. Чи захищені засоби криптографічного контролю згідно з усіма відповідними угодами, законами та нормативними актами?	d) обов'язкові або дискреційні методи доступу органів влади країн до зашифрованої інформації; e) дійсність цифрових підписів, печаток та сертифікатів. 5. Включити вимоги щодо інформаційної безпеки в контракти з клієнтами, постачальниками та страхові контракти, якщо це необхідно.					
5.32	Права на інтелектуальну власність	Було: 18.1.2 1. Чи веде організація облік усіх прав інтелектуальної власності та використання власних програмних продуктів? 2. Чи здійснює організація моніторинг використання неліцензійного програмного забезпечення? Стало: 1. Чи існує процедура захисту прав інтелектуальної власності? 2. Чи здійснює організація контроль за використанням неліцензійного програмного забезпечення?	1. Розробити та оприлюднити політику щодо прав інтелектуальної власності. 2. Опублікувати процедури, які описують відповідне використання програмного забезпечення та інформаційних продуктів, забезпечуючи дотримання прав інтелектуальної власності. 3. Запровадити процедури придбання програмного забезпечення для перевірки автентичності та легітимності джерел, а також для забезпечення дотримання авторських прав. 4. Розробити точні реєстри активів, які ідентифікують і відстежують всі активи, що підлягають захисту прав інтелектуальної власності. 5. Впровадити контроль та перевірки, щоб забезпечити встановлення лише авторизованого програмного забезпечення та ліцензійних продуктів, а також дотримання умов ліцензії. 6. Розробити процедури отримання та використання даних із зовнішніх джерел, забезпечуючи дотримання угод про обмін даними та вимог законодавства. 7. Провести тренінги та інформаційні програми для навчання персоналу щодо законів про авторське право, прав інтелектуальної власності та обмежень на копіювання службових матеріалів.	1. Задокументовані права інтелектуальної власності.. **Додатково:** *Задокументовані точні реєстри активів, які ідентифікують і відстежують всі активи, що підлягають захисту прав інтелектуальної власності.*		Невідповідність	0%	
5.33	Protection of records	Було: 18.1.3 Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual and business requirements? Стало: Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legal, regulatory, contractual and business requirements?	1.Встановити політику документів і записів (політика управління записами). 2.Випустити керівні принципи, які визначають належне зберігання, обробку, ланцюжок зберігання та видалення записів, забезпечуючи запобігання маніпуляціям та відповідність політиці управління документами організації. 3.Створити графік зберігання, визначаючи записи та період часу, протягом якого вони повинні бути збережені. 4.Впровадити процедури зберігання і обробки, які забезпечують ідентифікацію записів, дотримання термінів їх зберігання, відповідність відповідним законодавчим та нормативним актам, запобігання несанкціонованому доступу і звільненню. 5.Класифікувати записи на основі класифікації інформаційної безпеки (Враховувати класифікацію інформаційної безпеки при категоризації та захисті конкретних організаційних записів, призначенні терміни зберігання та визначення типу допустимих носіїв інформації).	1. Політика управління документами та записами (політика управління записами). **Додатково:** *1.Нормативні документи, що визначають правильне зберігання, оброблення, ланцюг володіння та утилізацію*		Невідповідність	0%	

			6.Вибрати системи зберігання даних, які дозволяють отримати необхідні записи в прийнятні терміни та формат, враховуючи потреби та вимоги організації. 7.Встановити процедури для забезпечення доступності та читабельності електронних записів протягом усього періоду їх зберігання, захищаючи від втрат через зміни технології. Зберігати необхідні криптографічні ключі та програми, пов'язані з зашифрованими архівами або цифровими підписами. 8.Здійснити процедури зберігання та обробки записів відповідно до рекомендацій виробників носіїв інформації. Розглянути можливість погіршення стану ЗМІ та встановити відповідні заходи щодо зниження ризиків.	*записів.* *2.Графік зберігання, який визначає види записів та період часу, на який вони повинні зберігатися.*				
5.34	Конфіденційність та захист персональних даних (PII)	Було: 18.1.4 1. Чи ідентифіковані та належним чином класифіковані персональні дані? 2. Чи захищені персональні дані відповідно до чинного законодавства? Стало: 1. Чи ідентифіковані та належним чином класифіковані персональні дані? 2. Чи захищені персональні дані згідно з відповідними законами та нормативно-правовими актами?	1.Встановити політику конфіденційності та захисту особисто визначеної інформації (ОВІ) та сповістити про неї всіх зацікавлених сторін. 2.Розробити та впровадити процедури для збереження конфіденційності та захисту ОВІ. Сповістити про них всіх зацікавлених сторін, які беруть участь у обробці ОВІ. 3.Призначити керівника з питань конфіденційності або еквівалентну роль, яка буде відповідальна за надання порад щодо конфіденційності та захисту ОВІ. Чітко визначити ролі та відповідальності персоналу, постачальників послуг та інших зацікавлених сторін, які беруть участь у роботі з ОВІ. 4.Забезпечити дотримання всіх відповідних законодавчих, нормативних актів та контрактних вимог, що стосуються збереження конфіденційності та захисту ОВІ. 5.Впровадити відповідні технічні та організаційні заходи для захисту ОВІ від несанкціонованого доступу, розголошення, зміни та знищення.	1.Політика щодо конфіденційності та захисту особисто визначеної інформації (ОВІ).		Невідповідність	0%	
5.35	Незалежна перевірка інформаційної безпеки	БЕЗ ЗМІН:1. Чи підлягає підхід організації до управління інформаційною безпекою регулярній незалежній перевірці? 2. Чи підлягає впровадження засобів контролю безпеки регулярній незалежній перевірці?	1. Впровадити процеси для проведення періодичних незалежних перевірок підходу організації до управління інформаційною безпекою. 2. Забезпечити, щоб перевірку проводили особи, незалежні від сфери, що перевіряється, та з відповідною компетенцією. 3. Запровадити процес звітування керівництву про результати незалежних перевірок та документування записів про результати перевірок. 4. Встановити процедуру ініціювання керівництвом коригувальних дій для усунення виявлених недоліків у підходах організації до забезпечення інформаційної безпеки та її реалізації. 5. Розглянути можливість проведення незалежних перевірок інформаційної безпеки у разі виникнення значних змін, таких як	1. Процедура внутрішнього аудиту.		Невідповідність	0%	

			зміни в законодавстві та нормативно-правових актах, значні інциденти, нові бізнес-проекти, зміни у використанні продуктів чи послуг або значні зміни в засобах та процедурах контролю інформаційної безпеки.					
5.36	Дотримання політик, правил і стандартів інформаційної безпеки	Було: 18.2.2, 18.2.3 1. Чи доручає організація керівникам регулярно перевіряти дотримання політики та процедур у межах їхньої сфери відповідальності? 2. Чи ведеться облік цих перевірок? Чи проводить організація регулярні перевірки технічних вимог до своїх інформаційних систем? Стало: 1. Чи проводять відповідні особи в організації регулярну перевірку дотримання політик, правил та стандартів у межах своєї сфери відповідальності? 2. Чи ведуться записи цих перевірок? 3. ?	1. Запровадити процес регулярної перевірки дотримання політики інформаційної безпеки організації, тематичних політик, правил і стандартів. Розгляньте можливість використання автоматичних інструментів вимірювання та звітності для ефективних та результативних перевірок. 2. Розробити інструкції щодо того, як керівники, власники послуг, продуктів чи інформації визначають, як перевіряти дотримання вимог інформаційної безпеки, визначених у політиці інформаційної безпеки, тематичних політиках, правилах, стандартах та інших застосовних нормативних документах. 3. Налагодити процес виявлення причин невідповідності вимогам. 4. Впровадити процес оцінки та впровадження відповідних коригувальних дій. 5. Впровадити процес перевірки результативності вжитих коригувальних дій з метою перевірки їх ефективності та виявлення будь-яких недоліків або слабких місць. 6. Впровадити процес реєстрації та зберігання результатів аналізу та коригувальних дій.	1. Задокументовано всі юридичні, законодавчі, нормативні та договірні вимоги, пов'язані з інформаційною безпекою. **Додатково:**: *2.Процедура регулярної перевірки дотримання вимог інформаційної безпеки організації.*		Невідповідність	0%	
5.37	Задокументовані операційні процеси	Було: 12.1.1 1. Чи добре задокументовані операційні процедури? 2. Чи доступні процедури всім користувачам, які їх потребують? Стало: 1. Чи добре задокументовані операційні процедури для засобів обробки інформації? 2. Чи доступні процедури всім користувачам, які їх потребують?	1. Визначити операційні дії, пов'язані з інформаційною безпекою, які потребують задокументованих процедур, наприклад, дії, що виконуються кількома особами, дії, що виконуються рідко, нові дії, що становлять ризики, або дії, що передаються новому персоналу. 2. Підготувати задокументовані процедури для визначених операційних дій. 3. Переконатися, що такі процедури визначають a) відповідальних осіб; б) безпечне встановлення та конфігурацію систем c) обробку та обробку інформації, як автоматизовану, так і ручну; d) резервне копіювання та відмовостійкість e) вимоги до планування, включаючи взаємозалежності з іншими системами; f) інструкції щодо обробки помилок або інших виняткових умов (наприклад, обмежень на використання службових програм), які можуть виникнути під час виконання завдання; g) контакти для підтримки та ескалації, включаючи контакти зовнішньої підтримки у випадку неочікуваних операційних або технічних труднощів; h) інструкції щодо поводження з носіями інформації;	1.Здокументовані операційні дії, пов'язані з інформаційною безпекою. 2.Процедури для визначених операційних дій.		Невідповідність	0%	

			і) процедури перезапуску та відновлення системи для використання у випадку збою системи; j) управління аудиторським слідом та інформацією системного журналу, а також системами відеомоніторингу; k) процедури моніторингу, такі як пропускна здатність, продуктивність та безпека; l) інструкції з технічного обслуговування. 3. Запровадити процес регулярного перегляду та оновлення задокументованих операційних процедур.					
6	**People controls**							
6.1	Перевірка	БЕЗ ЗМІН:1. Чи проводиться перевірка біографічних даних усіх нових кандидатів на роботу? 2. Чи затверджуються ці перевірки відповідним органом управління? 3. Чи відповідають перевірки відповідним законам, правилам та етичним нормам? 4. Чи підтверджується рівень необхідних перевірок оцінкою бізнес-ризиків?	1. Запровадити процес перевірки для всього персоналу, включаючи штатних, позаштатних, тимчасових працівників та підрядників. 2. Переконатися, що вимоги щодо скринінгу включені до контрактних угод між організацією та постачальниками послуг. 3. Запровадити процес збору та обробки інформації про всіх кандидатів, які розглядаються на посади в організації, забезпечуючи дотримання відповідного законодавства та юрисдикційних вимог. За необхідності, заздалегідь інформувати кандидатів про заходи з перевірки. 4. При визначенні необхідного рівня перевірки враховуйте бізнес-вимоги, класифікацію інформації та передбачувані ризики. 5. Встановити процедуру перевірки, яка повинна враховувати всі відповідні закони про конфіденційність, захист персональних даних та трудове законодавство і, де це дозволено, включати наступне: а) наявність задовільних рекомендацій (наприклад, ділових та особистих рекомендацій) б) перевірку (на повноту і точність) біографії заявника в) підтвердження заявленої академічної та професійної кваліфікації; г) незалежна перевірка особи (наприклад, паспорт або інший прийнятний документ, виданий відповідними органами); е) більш детальна перевірка, наприклад, перевірка кредитної історії або перевірка судимостей, якщо кандидат претендує на відповідальну посаду. 6. Переконатися, що кандидати, найняті на посади з інформаційної безпеки, мають необхідну компетентність і їм можна довіряти у виконанні своїх обов'язків, особливо на критично важливих посадах. Враховуйте специфічні вимоги та обов'язки, пов'язані з роллю у сфері безпеки. 7. Визначити критерії та обмеження для проведення перевірок, зокрема, хто має право проводити перевірки, як і коли вони	1.Процедура перевірки інформації про особу (перевірка анкетних даних). 2.Політика безпеки кадрів (політика безпеки у сфері управління персоналом).		Невідповідність	0%	

			проводяться, а також причини для їх проведення. 8. Впровадити періодичні верифікаційні перевірки. 9. Впровадити відповідні пом'якшувальні засоби контролю до завершення перевірки у випадках, коли перевірка не може бути завершена вчасно.					
6.2	Умови працевлаштування	Було: 7.1.2 1. Чи всіх співробітників, підрядників та сторонніх користувачів просять підписати угоди про конфіденційність та нерозголошення? 2. Чи передбачено в трудових договорах/договорах про надання послуг необхідність захисту комерційної інформації? Стало: 1. Чи всіх працівників просять підписати угоди про конфіденційність та нерозголошення? 2. Чи передбачено в трудових договорах необхідність захисту комерційної інформації?	1. Переглянути та оновіть трудові угоди, щоб чітко визначити обов'язки персоналу та організації щодо інформаційної безпеки. Проаналізуйте політику інформаційної безпеки організації, тематичні політики та законодавчі вимоги. 2. Розглянути можливість уточнення та включення наступних пунктів: a) угоди про конфіденційність або нерозголошення, які співробітники, що мають доступ до конфіденційної інформації, повинні підписати до того, як їм буде надано доступ до інформації та інших пов'язаних з нею активів; б) юридичні обов'язки та права [наприклад, щодо законів про авторське право або законодавства про захист даних c) обов'язки щодо класифікації інформації та управління інформацією та іншими пов'язаними з нею активами організації, засобами обробки інформації та інформаційними послугами, що надаються персоналом; d) обов'язки щодо обробки інформації, отриманої від зацікавлених сторін; e) дії, яких слід вжити, якщо персонал нехтує вимогами безпеки організації. 3. Забезпечити, щоб ролі та обов'язки з інформаційної безпеки були доведені до відома кандидатів під час процесу працевлаштування. 4. Переконатися, що існує процес регулярного перегляду умов та положень щодо інформаційної безпеки в трудових договорах, враховуючи зміни в законах, нормативних актах, політиці інформаційної безпеки або політиках, що стосуються конкретної тематики. 5. Визначити, чи повинні обов'язки, зазначені в умовах трудового договору, продовжуватись протягом певного періоду після закінчення трудових відносин.	1. Трудові контрактні угоди.		Невідповідність	0%	
6.3	Поінформованість, освіта та навчання з	Було: 7.2.2 Чи всі співробітники, підрядники та сторонні користувачі проходять регулярне навчання з питань безпеки відповідно до їхньої ролі та функцій в організації?	1. Розробити програму підвищення обізнаності, навчання та тренінгів з інформаційної безпеки, узгоджену з політикою інформаційної безпеки організації, політиками з конкретних питань та відповідними процедурами. 2. Переконатися, що програма включає положення про регулярне оновлення та охоплює новий персонал, переведення та зміну ролей в організації.	1. Задокументована програма підвищення обізнаності, освіти та тренінгів з		Невідповідність	0%	

	питань інформ аційної безпеки	Стало: Чи всі співробітники та відповідні зацікавлені сторони проходять регулярне навчання з питань безпеки відповідно до їх ролі та функцій в організації?	3. Спланувати та проводьте періодичну оцінку розуміння персоналом інформаційної безпеки наприкінці кожного виду діяльності. 4. Розробити програму підвищення обізнаності, орієнтовану на конкретні ролі, як для внутрішнього, так і для зовнішнього персоналу. 5. Планувати різноманітні заходи з підвищення обізнаності, використовуючи як фізичні, так і віртуальні канали. Наприклад, кампанії, буклети, плакати, інформаційні бюлетені, веб-сайти, інформаційні сесії, брифінги, модулі електронного навчання та електронні листи. 6. Переконатися, що програма підвищення обізнаності охоплює такі загальні аспекти, як а) прихильність керівництва до інформаційної безпеки в організації б) ознайомлення з чинними правилами та зобов'язаннями щодо інформаційної безпеки та їх дотримання, беручи до уваги політику інформаційної безпеки та тематичні політики, стандарти, закони, статути, нормативні акти, контракти та угоди; с) особисту відповідальність за власні дії та бездіяльність, а також загальну відповідальність за безпеку та захист інформації, що належить організації та зацікавленим сторонам; г) базові процедури інформаційної безпеки [наприклад, повідомлення про інциденти інформаційної безпеки] та базові засоби контролю [наприклад, безпека паролів]; е) контактні особи та ресурси для отримання додаткової інформації та консультацій з питань інформаційної безпеки, включаючи додаткові матеріали з інформаційної безпеки. 7. Визначити, підготувати та впровадити план навчання для технічних команд, зосередивши увагу на підтримці необхідних рівнів безпеки для пристроїв, систем, додатків та послуг. 8. Заповнити прогалини у навичках шляхом проведення додаткового навчання, якщо це необхідно. 9. Розглянути різні форми навчання та навчальні програми (наприклад, лекції або самонавчання, наставництво з боку експертів або консультантів (навчання на робочому місці), ротація співробітників для виконання різних видів діяльності, залучення вже кваліфікованих людей та наймання консультантів). 9. Заохочувати технічний персонал оновлювати свої знання за допомогою інформаційних бюлетенів, журналів, конференцій та професійних заходів. 10. Розробити програму підвищення обізнаності, щоб зосередити увагу не лише на питаннях "що" і "як", а й на "чому" інформаційної	інформаційної безпеки. 2. Задокументований план навчання, адаптований для технічних команд, з акцентом на підтримці необхідних рівнів безпеки для пристроїв, систем, додатків та сервісів.			

			безпеки, підкреслюючи потенційний вплив поведінки персоналу на організацію. 11. Інтегрувати обізнаність, освіту та навчання з питань інформаційної безпеки в загальну підготовку з управління інформацією, ІКТ, безпеки, конфіденційності та захисту інформації, якщо це необхідно.					
6.4	Дисциплінарний процес	Було: 7.2.3 1. Чи існує офіційний дисциплінарний процес, який дозволяє організації вживати заходів проти працівників, які порушили інформаційну безпеку? 2. Чи доведено це до відома всіх працівників? Стало: 1. Чи існує офіційний дисциплінарний процес, який дозволяє організації вживати заходів проти персоналу та інших відповідних зацікавлених сторін, які порушили політику інформаційної безпеки? 2. Чи повідомляється про це всім працівникам та іншим відповідним зацікавленим сторонам?	1. Запровадити формальний дисциплінарний процес для реагування на порушення політики інформаційної безпеки. 2. Довесим встановлений процес до відома всього персоналу та відповідних зацікавлених сторін. 3. Переконатися, що дисциплінарний процес не розпочинається без попередньої перевірки порушення політики інформаційної безпеки. 4. Структурувати дисциплінарний процес таким чином, щоб забезпечити поетапне реагування, беручи до уваги такі фактори, як а) характер (хто, що, коли, як) і серйозність порушення та його наслідки б) чи було порушення навмисним (зловмисним) або ненавмисним (випадковим) с) чи було це перше або повторне порушення; г) чи був порушник належним чином підготовлений. 5. Переконатися, що механізм реагування враховує правові, статутні, регуляторні, договірні, бізнес-вимоги та інші необхідні фактори. 6. Переконатися, що дисциплінарний процес використовується як стримуючий фактор для запобігання подальшим порушенням політики інформаційної безпеки, тематичних політик та процедур інформаційної безпеки. 7. Визначити критерії навмисних порушень політики інформаційної безпеки. 8. Встановити процедури для негайних дій при виявленні навмисних порушень політики. 9. Впровадити заходи щодо захисту персональних даних осіб, на яких накладено дисциплінарні стягнення, відповідно до чинних вимог. 10. Розробити та впровадити систему винагород для визнання та заохочення відмінної поведінки щодо інформаційної безпеки.	1.Дисциплінарний процес. 2.Політика безпеки кадрів (управління персоналом).		Невідповідність	0%	
6.5	Обов'язки після звільнення або зміни	Було: 7.3.1 1. Чи існує задокументований процес припинення або зміни трудових обов'язків?	1. Визначити, які обов'язки та відповідальність за інформаційну безпеку залишаються чинними після звільнення або зміни місця роботи, включаючи такі аспекти, як конфіденційність, інтелектуальна власність та інші отримані знання, а також обов'язки, що містяться в будь-якій іншій угоді про	1.Дисциплінарний процес. 2.Політика безпеки кадрів		Невідповідність	0%	

	місця роботи	2. Чи доведені до відома працівника або підрядника будь-які обов'язки з інформаційної безпеки, які продовжують діяти після припинення трудових відносин? 3. Чи здатна організація забезпечити дотримання будь-яких обов'язків, які залишаються після закінчення трудових відносин? Стало: 1. Чи існує задокументований процес припинення або зміни трудових обов'язків? 2. Чи доведено до відома відповідного персоналу або інших зацікавлених осіб будь-які обов'язки з інформаційної безпеки, які продовжують діяти після закінчення трудових відносин? 3. Чи здатна організація забезпечити дотримання будь-яких обов'язків, які продовжують діяти після припинення трудових відносин?	конфіденційність. 2. Включити ці обов'язки в умови трудового договору, контракти або угоди, укладені з окремими особами. 3. Запровадити процес управління змінами у сфері зайнятості або відповідальності, що поєднує в собі припинення поточної ролі та початок виконання нової ролі. 4. Визначити ролі та обов'язки з інформаційної безпеки, які виконують особи, що звільняються або змінюють роботу, та забезпечити їх передачу іншій особі. 5. Налагодити процес інформування персоналу, інших зацікавлених сторін та відповідних контактів, таких як клієнти та постачальники, про зміни в ролях, обов'язках та операційних процедурах. 6. Застосовути процедуру звільнення або зміни роботи до зовнішнього персоналу, наприклад, постачальників, коли відбувається звільнення або зміна роботи в організації. 7. Призначити відділ кадрів або відповідний персонал відповідальним за загальний процес звільнення, забезпечивши їхню співпрацю з керівником для управління аспектами інформаційної безпеки, пов'язаними з цими процедурами. 8. Забезпечити, щоб у випадку персоналу, наданого через зовнішню сторону, процес звільнення здійснювався зовнішньою стороною відповідно до контракту між організацією та зовнішньою стороною.	(управління персоналом).				
6.6	Угоди про конфіденційність або нерозголошення	БЕЗ ЗМІН: 1. Чи підписують працівники, підрядники та агенти угоди про конфіденційність або нерозголошення? 2. Чи підлягають ці угоди регулярному перегляду? 3. Чи ведеться облік угод?	1. Визначити потреби організації в захисті інформації, які мають бути відображені в угодах про конфіденційність або нерозголошення (NDA). 2. Задокументувати визначені вимоги щодо конфіденційності на основі вимог інформаційної безпеки організації, включаючи тип інформації, яка буде оброблятися, рівень її секретності, її використання та допустимий доступ для іншої сторони. 3. Включити ключові елементи в угоди про конфіденційність або нерозголошення: a) визначення інформації, що підлягає захисту (наприклад, конфіденційна інформація) б) очікуваний термін дії угоди, включаючи випадки, коли може виникнути необхідність зберігати конфіденційність на невизначений термін або до моменту, коли інформація стане загальнодоступною; c) необхідні дії у випадку розірвання угоди; d) обов'язки та дії підписантів щодо уникнення несанкціонованого розголошення інформації; e) право власності на інформацію, комерційну таємницю та	1. Угоди про конфіденційність або нерозголошення.		Невідповідність	0%	

			інтелектуальну власність, і як це пов'язано із захистом конфіденційної інформації; f) дозволене використання конфіденційної інформації та права підписантів на використання інформації; g) право на аудит та моніторинг діяльності, пов'язаної з конфіденційною інформацією, за особливо важливих обставин; h) процес повідомлення та звітування про несанкціоноване розголошення або витік конфіденційної інформації; i) умови повернення або знищення інформації при розірванні угоди; j) очікувані дії, які будуть вжиті у випадку недотримання угоди. 4. Розглянути дотримання угод про конфіденційність та нерозголошення для юрисдикції, до якої вони застосовуються. 5. Забезпечити періодичний перегляд вимог до угод про конфіденційність та нерозголошення, а також у разі виникнення змін, що впливають на ці вимоги. 6. Довестии задокументовані угоди про конфіденційність та нерозголошення до відома всього відповідного персоналу та зацікавлених сторін. 7. Переконатися, що угоди підписані відповідним персоналом та іншими зацікавленими сторонами.				
6.7	Віддалена робота	Було: 6.2.2 1. Чи існує політика щодо дистанційної роботи? 2. Чи є на це дозвіл керівництва? 3. Чи існує встановлений процес отримання доступу для віддалених працівників? 4. Чи надаються дистанційним працівникам поради та обладнання для захисту їхніх активів? Стало: 1. Чи існує політика щодо віддаленої роботи? 2. Чи має це схвалення керівництва? 3. Чи існує встановлений процес отримання доступу для віддалених працівників? 4. Чи надаються віддаленим працівникам консультації та обладнання для захисту їхніх активів?	1. Розробити політику щодо дистанційної роботи, яка б визначала відповідні умови та обмеження. 2. Врахувати наступні аспекти: a) існуюча або запропонована фізична безпека віддаленого робочого місця, беручи до уваги фізичну безпеку місця розташування та місцевого середовища, включаючи різні юрисдикції, в яких перебуває персонал; б) правила та механізми безпеки для віддаленого фізичного середовища, такі як шафи, що замикаються, безпечне транспортування між локаціями та правила віддаленого доступу, вільний робочий стіл, друк та утилізація інформації та інших пов'язаних з нею активів, а також звітування про події в сфері інформаційної безпеки; c) очікуване фізичне віддалене робоче середовище d) вимоги до безпеки зв'язку, враховуючи потребу у віддаленому доступі до систем організації, чутливість інформації, що підлягає доступу та передачі через канал зв'язку, а також чутливість систем та додатків; e) використання віддаленого доступу, такого як доступ до віртуального робочого столу, що підтримує обробку та зберігання інформації на обладнанні, яке знаходиться у приватній власності; f) загроза несанкціонованого доступу до інформації або ресурсів з	1.Політика віддаленої роботи / Політика телекомунікації		Невідповідність	0%	

			боку інших осіб на віддаленому робочому місці (наприклад, сім'ї та друзів) g) загроза несанкціонованого доступу до інформації або ресурсів з боку інших осіб у громадських місцях; h) використання домашніх мереж та мереж загального користування, а також вимоги або обмеження щодо конфігурації бездротових мережевих сервісів; i) використання заходів безпеки, таких як брандмауери та захист від шкідливого програмного забезпечення; j) безпечні механізми розгортання та ініціалізації систем у віддаленому режимі; k) безпечні механізми автентифікації та надання привілеїв доступу з урахуванням вразливості механізмів однофакторної автентифікації, якщо дозволено віддалений доступ до мережі організації. 3. Впровадити керівні принципи та заходи, які включають a) надання відповідного обладнання та меблів для зберігання для віддаленої роботи, де використання приватного обладнання, яке не перебуває під контролем організації, не дозволяється; б) визначення дозволеної роботи, класифікацію інформації, яка може зберігатися, а також внутрішніх систем та послуг, до яких дистанційний працівник має право доступу; в) проведення навчання для тих, хто працює віддалено, і тих, хто надає підтримку. Це повинно включати в себе навчання безпечному веденню бізнесу під час віддаленої роботи; d) надання відповідного комунікаційного обладнання, включаючи методи захисту віддаленого доступу, такі як вимоги щодо блокування екрану пристрою та таймерів бездіяльності; увімкнення відстеження місцезнаходження пристрою; встановлення можливостей віддаленого стирання даних; e) фізична безпека; f) правила та вказівки щодо доступу членів сім'ї та відвідувачів до обладнання та інформації; g) надання підтримки та обслуговування апаратного та програмного забезпечення; h) забезпечення страхування; i) процедури резервного копіювання та безперервності бізнесу; j) аудит та моніторинг безпеки; к) відкликання повноважень і прав доступу та повернення обладнання після завершення дистанційної роботи.				
6.8	Звітування про події	Було: 16.1.1, 16.1.3 Чи чітко визначені та задокументовані	1. Розробити та задокументувати чіткий механізм, за допомогою якого персонал може повідомляти про події, що спостерігаються або підозрюються в сфері інформаційної безпеки.	1. Задокументований механізм		Невідповідність	0%	

	інформ аційної безпеки	обов'язки керівництва в процесах управління інцидентами? 1. Чи існує процес звітування про виявлені слабкі місця в інформаційній безпеці? 2. Чи широко розповсюджується інформація про цей процес? 3. Чи існує процес розгляду та своєчасного реагування на звіти? Стало: 1. Чи існує процес звітування про спостережувані або підозрювані події в сфері інформаційної безпеки? 2. Чи широко розповсюджується інформація про цей процес? 3. Чи всі користувачі та персонал усвідомлюють свій обов'язок повідомляти про події інформаційної безпеки якомога швидше?	2. Проінформувати весь персонал про їхній обов'язок повідомляти про події інформаційної безпеки якомога швидше. 3. Надати чіткі інструкції щодо процедури повідомлення про події інформаційної безпеки та контактної особи, якій слід повідомляти про такі події. 4. Надати чіткі приклади ситуацій, які слід враховувати при повідомленні про інциденти інформаційної безпеки, які включають а) неефективні засоби контролю інформаційної безпеки; б) порушення конфіденційності, цілісності або очікуваної доступності інформації в) людські помилки г) недотримання політики інформаційної безпеки, тематичних політик або застосовних стандартів; е) порушення заходів фізичної безпеки f) системні зміни, які не пройшли через процес управління змінами; g) несправності або інша аномальна системна поведінка програмного чи апаратного забезпечення h) порушення доступу; і) вразливості; к) підозра на зараження шкідливим програмним забезпеченням. 5. Порадити персоналу та користувачам не намагатися довести підозри щодо вразливостей інформаційної безпеки та потенційних наслідків цього.	звітності щодо спостережених або підозрюваних подій у сфері інформаційної безпеки.				
7			**Physical controls**					
7.1	Периме три фізично го захисту	Було: 11.1.1 1. Чи існує визначений периметр безпеки? 2. Чи відокремлені та належним чином контролюються зони конфіденційної або критично важливої інформації? Так: 1. Чи існує визначений периметр безпеки? 2. Чи відокремлені та належним чином контролюються зони конфіденційної або критично важливої інформації?	0. Політика фізичної та екологічної безпеки. 1. Визначити та задокументуйте периметри фізичної безпеки, а також розташування та міцність кожного з них, виходячи з вимог безпеки, пов'язаних з активами, що знаходяться в межах цих периметрів. 2. Провести перевірку фізичної конструкції периметрів, щоб переконатися, що вони є надійними та не мають прогалин, через які може статися несанкціонований доступ. 3. Впровадити механізми контролю, такі як решітки, сигналізація та замки на всіх зовнішніх дверях, щоб запобігти несанкціонованому доступу. 4. Вжити заходів для захисту вікон та вентиляційних отворів на першому поверсі від можливого несанкціонованого доступу. 5. Встановити системи сигналізації та налагодити процес регулярного моніторингу і тестування всіх протипожежних дверей і стін на необхідний рівень вогнестійкості. 6. Визначити безпечні зони в межах периметра безпеки на основі	1.Політика фізичної та екологічної безпеки. 2.Системи сигналізації. 3.Документовані безпечні зони в межах безпекових периметрів.		Невідповід ність	0%	

			чутливості даних та активів, які вони містять, і створити додаткові бар'єри та периметри для контролю фізичного доступу між зонами з різними вимогами до безпеки всередині периметра безпеки. 7. Розробити плани посилення заходів фізичної безпеки в періоди підвищеної загрози.					
7.2	Фізичний вхід	Було: 11.1.2, 11.1.6 Чи мають безпечні зони відповідні системи контролю доступу, щоб забезпечити доступ лише уповноваженому персоналу? 1. Чи є окремі зони доставки / завантаження? 2. Чи контролюється доступ до цих зон? 3. Чи ізольований доступ із зон завантаження від приміщень для обробки інформації? Стало: 1. Чи мають безпечні зони відповідні системи контролю доступу та точки доступу, щоб забезпечити доступ лише уповноваженому персоналу? 2. Чи є окремі зони доставки/завантаження? 3. Чи контролюється доступ до цих зон? 4. Чи ізольований доступ із зон завантаження від приміщень для обробки інформації?	1. Визначити та встановіть контроль над усіма точками доступу, щоб уникнути несанкціонованого доступу. 2. Ізолювати зони доставки та завантаження від приміщень, де обробляється інформація. 3. Розглянути наступні рекомендації: a) обмежити доступ до об'єктів і будівель лише для уповноваженого персоналу. Процес управління правами доступу до фізичних зон повинен включати надання, періодичну перевірку, оновлення та відкликання дозволів; б) безпечне ведення та моніторинг фізичного журналу або електронного аудиторського сліду всіх доступів, а також захист усіх журналів та конфіденційної інформації про автентифікацію; c) створення та впровадження процесу та технічних механізмів для управління доступом до зон, де обробляється або зберігається інформація. Механізми автентифікації включають використання карток доступу, біометричних даних або двофакторної автентифікації, наприклад, картки доступу та секретного PIN-коду. Для доступу до чутливих зон слід розглянути можливість встановлення подвійних захисних дверей; d) створення зони прийому, яка контролюється персоналом, або інших засобів контролю фізичного доступу на територію або в будівлю; e) перевірка та огляд особистих речей персоналу та зацікавлених осіб при вході та виході; f) вимагати від усього персоналу та зацікавлених осіб носити видиме посвідчення особи та негайно повідомляти охорону про появу відвідувачів без супроводу або осіб без видимого посвідчення особи. Для кращої ідентифікації постійних працівників, постачальників та відвідувачів слід розглянути можливість використання бейджів, які легко розрізнити; g) надання персоналу постачальника обмеженого доступу до захищених зон або засобів обробки інформації лише за необхідності. Такий доступ має бути санкціонованим та контрольованим; h) приділяти особливу увагу безпеці фізичного доступу у випадку будівель, в яких зберігаються активи кількох організацій; i) розробка заходів фізичної безпеки таким чином, щоб їх можна було посилити, коли ймовірність фізичних інцидентів зростає;	1. Політика фізичної та екологічної безпеки. 2. Система контролю доступу. 3. Охорона.		Невідповідність	0%	

			j) захист інших точок входу, таких як аварійні виходи, від несанкціонованого доступу; k) налагодження процесу управління ключами для забезпечення управління фізичними ключами або автентифікаційною інформацією (наприклад, коди замків, комбіновані замки до офісів, кімнат та приміщень, таких як шафи для ключів), а також забезпечення ведення журналу або щорічного аудиту ключів та контролю доступу до фізичних ключів або автентифікаційної інформації. 4. Впровадити процедури управління відвідувачами, які включають а) автентифікацію особи відвідувачів за допомогою відповідних засобів; б) реєстрацію дати та часу входу та виходу відвідувачів в) надання доступу відвідувачам лише для конкретних, дозволених цілей та з інструкціями щодо вимог безпеки на території та порядку дій у надзвичайних ситуаціях; г) нагляд за всіма відвідувачами, якщо тільки не надано чіткого винятку. 5. Налагодити процес контролю в зонах доставки та завантаження, враховуючи наступні рекомендації: а) обмежити доступ до зон доставки та завантаження ззовні будівлі лише ідентифікованим та уповноваженим персоналом; б) спроектувати зони доставки та завантаження таким чином, щоб вантажити та розвантажувати вантажі без несанкціонованого доступу персоналу, який здійснює доставку, до інших частин будівлі с) замикати зовнішні двері зон доставки та завантаження, коли відчиняються двері в зони з обмеженим доступом; d) огляд і перевірка вхідних відправлень на наявність вибухових речовин, хімікатів або інших небезпечних матеріалів до того, як вони будуть винесені із зон доставки і завантаження; е) реєструвати вантажі, що надходять, відповідно до процедур управління активами при надходженні на об'єкт f) фізичне розділення вхідних і вихідних вантажів, де це можливо; g) перевірка вхідних поставок на предмет виявлення ознак несанкціонованого втручання в дорозі. У разі виявлення фактів несанкціонованого втручання слід негайно повідомити про це співробітникам служби безпеки.				
7.3	Охорона офісів, приміщ	Було: 11.1.3 1. Чи були спроектовані та сконфігуровані офіси, кімнати та	1. Розмістити критично важливі об'єкти у зонах, до яких заборонено доступ сторонніх осіб. 2. Переконатися, що будівлі є непримітними і не вказують на їхнє призначення.	1. Політика фізичної та екологічної безпеки.		Невідповідність	0%	

	ень та об'єктів	приміщення з урахуванням вимог безпеки? 2. Чи існують процеси для підтримки безпеки (наприклад, замикання на ключ, прибирання столів тощо)? Стало: 1. Чи була розроблена та впроваджена фізична безпека офісів, кімнат та приміщень? 2. Чи існують процеси для підтримання безпеки (наприклад, замикання на ключ, звільнення столів тощо)?	3. Уникати розміщення знаків ззовні або всередині будівлі, які б вказували на наявність діяльності з обробки інформації. 4. Налаштувати приміщення таким чином, щоб конфіденційну інформацію або діяльність не було видно або чутно ззовні. 5. Розглянути можливість впровадження електромагнітного екранування, якщо це необхідно. 6. Не допускати, щоб довідники, внутрішні телефонні книги та доступні в Інтернеті карти, які визначають місця розташування об'єктів обробки конфіденційної інформації, були легкодоступними для несанкціонованих осіб.	2. Система контролю доступу. 3. Охорона. 4. Системи пожежної сигналізації та захисту. 5. Системи відеоспостереження. 6. Системи охолодження.				
7.4	Моніторинг фізичної безпеки	1. Чи розроблені та впроваджені системи спостереження для моніторингу фізичних приміщень? 2. Чи здійснюється постійний моніторинг доступу до будівель, в яких розміщені критичні системи? 3. Чи задокументовано та зберігається конфіденційність розробки систем моніторингу? 4. Чи належним чином захищені системи моніторингу від несанкціонованого доступу та дистанційного вимкнення? 5. Чи проводиться регулярне тестування системи моніторингу? 6. Чи відповідає система моніторингу всім законам та нормативним актам, включаючи законодавство про захист даних та захист персональних даних?	1. Впровадити системи спостереження, такі як охорона, охоронна сигналізація та системи відеоспостереження. 2. Розглянути можливість використання програмного забезпечення для управління інформацією про фізичну безпеку або постачальника послуг моніторингу. 3. Встановити системи відеомоніторингу для фіксації доступу до чутливих зон. 4. Встановити контактні, звукові або рухові детектори згідно з відповідними стандартами. 5. Забезпечити конфіденційність дизайну та деталей систем моніторингу, щоб запобігти непоміченим вторгненням. 6. Вживати заходів захисту для запобігання несанкціонованому доступу до інформації, отриманої в результаті спостереження. 7. Закріпити пульт управління системою сигналізації в зоні, що охороняється, за допомогою механізмів, захищених від несанкціонованого доступу. 8. Визначити план регулярного тестування систем моніторингу та датчиків для забезпечення їхньої належної роботи. 9. Переконатися, що механізми моніторингу та запису відповідають місцевим законам, правилам та поважають особисту приватність.	1. Політика фізичної та екологічної безпеки. 2. Системи спостереження, такі як охоронці, сигналізації для виявлення вторгнень та системи відеоспостереження.		Невідповідність	0%	
7.5	Захист від фізичних та екологічних загроз	Було: 11.1.4 Чи розроблені заходи фізичного захисту для запобігання стихійним лихам, зловмисним атакам або нещасним випадкам? Стало:	1. Проводити оцінку ризиків перед початком роботи на фізичному об'єкті та через регулярні проміжки часу після цього. 2. Отримати консультацію спеціаліста для управління ризиками, пов'язаними з фізичними та екологічними загрозами, такими як пожежа, повінь, землетрус, громадські заворушення, токсичні відходи, викиди в навколишнє середовище та інші. 3. Оцінювати місцеву топографію та міські загрози під час вибору місця розташування та будівництва фізичних приміщень. 4. Впроваджувати відповідні засоби контролю для виявлених	1. Оцінено ризики та визначено контрзаходи для фізичних та екологічних загроз, таких як пожежа, повінь, землетрус,		Невідповідність	0%	

		Чи були розроблені заходи захисту від фізичних та екологічних загроз?	загроз у наступних контекстах, як приклади: а) пожежа: встановлення та налаштування систем, здатних виявляти пожежі на ранній стадії та надсилати сигнали тривоги або запускати системи пожежогасіння, щоб запобігти пошкодженню вогнем носіїв інформації та пов'язаних з ними систем обробки інформації. Гасіння пожежі повинно здійснюватися з використанням найбільш підходящої речовини з урахуванням навколишнього середовища (наприклад, газ у закритих приміщеннях); б) затоплення: встановлення систем, здатних виявляти затоплення на ранній стадії, під підлогою приміщень, що містять носії інформації або системи обробки інформації. Водяні насоси або еквівалентні засоби повинні бути легко доступні на випадок затоплення; в) перепади напруги: впровадження систем, здатних захистити як серверні, так і клієнтські інформаційні системи від перепадів напруги або подібних подій для мінімізації наслідків таких подій; г) вибухові речовини та зброя: проведення вибіркових перевірок на наявність вибухових речовин або зброї у персоналу, транспортних засобах або товарах, які потрапляють на об'єкти з оброблення чутливої інформації. 5. Розглянути можливість використання сейфів або інших форм безпечних сховищ для захисту інформації від катастроф. 6. Враховувати принципи запобігання злочинам через дизайн середовища при розробці засобів контролю для захисту середовища організації та зменшення міських загроз.	громадські заворушення, токсичні відходи, викиди в навколишнє середовище та інші.				
7.6	Робота в безпечних зонах	БЕЗ ЗМІН: 1. Чи існують безпечні зони? 2. Якщо вони існують, чи мають безпечні зони відповідну політику та процеси? 3. Чи впроваджуються та контролюються ці політики та процеси?	1. Визначити та позначте безпечні зони у вашій організації, де знаходиться конфіденційна інформація та активи. 2. Інформувати персонал про існування безпечної зони або про діяльність у ній лише за принципом службової необхідності. 3. Вживати заходів для уникнення роботи без нагляду в захищених зонах як з міркувань безпеки, так і для зменшення ймовірності зловмисних дій. 4. Вживати заходів для фізичного блокування та періодичної перевірки вільних безпечних зон. 5. Впровадити правила, що забороняють використання фото-, відео-, аудіо- чи іншого записуючого обладнання, включаючи камери на кінцевих пристроях користувачів, якщо на це немає дозволу. 6. Встановити контроль за носінням та використанням кінцевих пристроїв користувачів у безпечних зонах. 7. Забезпечити, щоб процедури на випадок надзвичайних ситуацій	1. Задокументовані безпечні зони, де знаходиться конфіденційна інформація та активи. **Додатково:** 2. *Правила, що забороняють використання фото-, відео-, аудіо- чи іншого записуючого обладнання, включаючи камери на*		Невідповідність	0%	

			були розміщені на видному та доступному місці в захищених зонах.	*кінцевих пристроях користувачів, якщо на це немає дозволу.*				
7.7	Чистий стіл і чистий екран	БЕЗ ЗМІН: 1. Чи існує чітка політика щодо чистого робочого столу та екрану? 2. Чи добре вона виконується?	1. Встановити чітку політику " чистого столу" та "чистого екрану" і довести її до відома всіх зацікавлених сторін. 2. Запровадити правила надійного зберігання конфіденційної або критично важливої ділової інформації (наприклад, на папері або на електронних носіях), коли вона не використовується або офіс звільняється. 3. Впровадити та забезпечити дотримання інструкцій щодо захисту кінцевих пристроїв користувачів за допомогою ключових замків або інших засобів безпеки, коли вони не використовуються або залишаються без нагляду. 4. Впровадити та забезпечити дотримання інструкцій щодо залишення кінцевих пристроїв користувачів у вимкненому стані або захищеними за допомогою механізму блокування екрану та клавіатури, що контролюється механізмом автентифікації користувача, коли вони залишаються без нагляду. 5. Впровадити правила негайного збору вихідних даних з принтерів або багатофункціональних пристроїв. Розгляньте можливість використання принтерів з функціями автентифікації. 6. Впровадити механізми безпечного зберігання та знищення документів і знімних носіїв, що містять конфіденційну інформацію. 7. Встановити правила та інструкції щодо конфігурації спливаючих вікон на екранах. 8. Впровадити інструкції щодо видалення конфіденційної або критично важливої інформації на дошках та інших типах дисплеїв, коли вона більше не потрібна.	1. Політика порожнього столу та чистого екрану.		Невідповідність	0%	
7.8	Розміщення та захист обладнання	БЕЗ ЗМІН: 1. Чи визначені та враховані екологічні ризики при виборі місця розташування обладнання? 2. Чи враховуються ризики несанкціонованого доступу / перехожих при розміщенні обладнання?	1. Розробити план розміщення обладнання, щоб мінімізувати непотрібний доступ до робочих зон та уникнути несанкціонованого доступу. 2. Впровадити рекомендації щодо ретельного розміщення обладнання для обробки конфіденційних даних, щоб запобігти несанкціонованому перегляду. 3. Визначити потенційні фізичні та екологічні загрози [наприклад, крадіжка, пожежа, вибухові речовини, дим, вода (або збій у водопостачанні), пил, вібрація, хімічний вплив, перешкоди в електропостачанні, перешкоди в комунікаціях, електромагнітне випромінювання та вандалізм] та впровадити засоби контролю для їх мінімізації. 4. Встановити та забезпечити дотримання правил щодо прийому	1. Політика порожнього столу та чистого екрану.		Невідповідність	0%	

			їжі, пиття та куріння в безпосередній близькості до засобів обробки інформації. 5. Впровадити систему моніторингу умов навколишнього середовища, таких як температура та вологість, які можуть впливати на роботу засобів обробки інформації. 6. Застосувати блискавкозахист до всіх будівель та встановити блискавкозахисні фільтри на всіх вхідних лініях електропередач та зв'язку. 7. Впровадити спеціальні методи захисту, такі як мембрани для клавіатури, для обладнання, що використовується в промислових умовах. 8. Впровадити рекомендації щодо захисту обладнання, яке обробляє конфіденційну інформацію, щоб мінімізувати ризик витоку інформації через електромагнітне випромінювання. 9. Фізично відокремити засоби обробки інформації, якими керує організація, від тих, якими вона не керує.					
7.9	Безпека активів за межами приміщення	БЕЗ ЗМІН: 1. Чи існує політика безпеки активів за межами офісу? 2. Чи широко поширена ця політика?	1. Розробити політику щодо надання дозволу на використання всіх пристроїв, які зберігають або обробляють інформацію за межами приміщень організації. 2. Встановити правила, які гарантують, що обладнання та носії інформації, винесені за межі приміщення, не залишаються без нагляду в громадських та незахищених місцях. 3. Впровадити процедури для постійного дотримання інструкцій виробників щодо захисту обладнання (наприклад, захист від впливу сильних електромагнітних полів, води, тепла, вологості, пилу). 4. Створити і ввести журнал, який визначає ланцюжок відповідальності за обладнання, включаючи принаймні імена та організації осіб, відповідальних за обладнання, для випадків, коли обладнання, що знаходиться за межами приміщення, передається між різними особами або зацікавленими сторонами. 5. Впровадити процес авторизації та реєстрації вивезення обладнання та носіїв інформації з приміщень організації з метою збереження аудиторського сліду. 6. Впровадити заходи для захисту від перегляду інформації на пристрої в громадських місцях. 7. Впровадити відстеження місцезнаходження та можливість віддаленого очищення пристроїв. 8. Впровадити моніторинг фізичної безпеки стаціонарно встановленого поза приміщенням обладнання. 9. Забезпечити захист обладнання за межами приміщення від фізичних та екологічних загроз. 10. Впровадити фізичний контроль доступу та захист від	1. Вимоги до авторизації використання активів за межами робочого місця.		Невідповідність	0%	

			несанкціонованого доступу до стаціонарного обладнання, встановленого поза приміщенням. 11. Впровадити логічний контроль доступу до стаціонарно встановленого поза приміщенням обладнання.					
7.10	Носії інформації	Було: 8.3.1, 8.3.2, 8.3.3, 11.2.5 1. Чи існує політика щодо знімних носіїв інформації? 2. Чи існує процес управління змінними носіями? 3. Чи доведено політику та процес(и) до відома всіх працівників, які використовують знімні носії? Чи існує офіційна процедура, що регулює порядок утилізації знімних носіїв? 1. Чи існує задокументована політика та процес, що детально описує, як слід транспортувати фізичні носії? 2. Чи захищені носії під час транспортування від несанкціонованого доступу, зловживань чи корупції? 1. Чи існує процес контролю за тим, як активи вивозяться з місця події? 2. Чи застосовується цей процес? 3. Чи проводяться вибіркові перевірки? Стало: 1. Чи існує політика, що регулює носії інформації? 2. Чи існує процес управління носіями інформації? 3. Чи доведено політику та процес(и) до відома всіх працівників, які використовують носії інформації? 4. Чи існує офіційна процедура, що регулює повторне використання або утилізацію знімних носіїв? 5. Чи існує політика або процес, що детально описує, як слід поводитися з пошкодженими пристроями, що містять конфіденційні дані? ???	1. Розробити та оприлюднити політику управління знімними носіями інформації. 2. Впровадити процес авторизації та реєстрації вилучення носіїв інформації з приміщень організації з метою збереження аудиторського сліду. 3. Встановити правила зберігання всіх носіїв інформації в безпечному, захищеному середовищі відповідно до їхньої інформаційної класифікації та захисту від загроз навколишнього середовища (таких як спека, волога, вологість, електронне поле або старіння) відповідно до специфікацій виробників. 4. Забезпечити використання криптографічних методів для захисту інформації на знімних носіях, якщо конфіденційність або цілісність інформації є важливими міркуваннями. 5. Впровадити процес перенесення інформації на нові носії до того, як вона стане нечитабельною. 6. Забезпечити зберігання декількох копій цінної інформації на окремих носіях для подальшого зниження ризику випадкового пошкодження або втрати інформації. 7. Створити реєстр змінних носіїв інформації, щоб обмежити ймовірність втрати інформації. 8. Запровадити процедури безпечного повторного використання або утилізації носіїв інформації. 9. Визначити предмети, які потребують безпечної утилізації. 10. Реєструвати утилізацію чутливих предметів для збереження аудиторського сліду. 11. Враховувати ефект агрегації при накопиченні носіїв інформації для утилізації. 12. Провести оцінку ризиків щодо пошкоджених пристроїв, які містять конфіденційні дані. 13. Розглянути можливість додаткового фізичного захисту носіїв інформації, якщо конфіденційна інформація не зашифрована.	1. Політика управління знімними носіями інформації. 2. Реєстр знімних носіїв інформації.		Невідповідність	0%	

7.11	Підтримка служб	БЕЗ ЗМІН: 1. Чи є система безперебійного живлення або резервний генератор? 2. Чи були вони протестовані у відповідні терміни?	1. Переконатися, що обладнання, яке підтримує служби, налаштоване, експлуатується та обслуговується відповідно до специфікацій виробника. 2. Забезпечити регулярне оцінювання відповідності інженерних мереж потребам зростання бізнесу та взаємодії з іншими допоміжними інженерними мережами. 3. Забезпечити регулярну перевірку та тестування обладнання, що підтримує інженерні мережі, для забезпечення їх належного функціонування. 4. За необхідності, впровадити системи сигналізації для виявлення несправностей інженерних мереж. 5. За необхідності, забезпечити інженерні комунікації декількома каналами з різноманітною фізичною маршрутизацією. 6. У разі підключення до мережі переконатися, що обладнання, яке підтримує комунальні послуги, знаходиться в окремій мережі від засобів обробки інформації. 7. Переконатися, що обладнання, яке підтримує роботу утиліт, підключено до Інтернету лише за необхідності і лише у безпечний спосіб. 8. Забезпечити аварійне освітлення та зв'язок. Розмістіть аварійні вимикачі та клапани належним чином. Запишіть і зробіть доступними контактні дані на випадок надзвичайних ситуацій.	1. Внутрішні інструкції з обслуговування допоміжних систем. 2. Система безперебійного живлення, генератор.		Невідповідність	0%	
7.12	Безпека кабелів	Було: 11.2.3 1. Чи була проведена оцінка ризиків щодо розташування силових та телекомунікаційних кабелів? 2. Чи розміщені вони таким чином, щоб захистити від перешкод, перехоплення або пошкодження? Стало: 1. Чи була проведена оцінка ризиків щодо розташування силових кабелів, кабелів передачі даних та допоміжних інформаційних послуг? 2. Чи розміщені вони таким чином, щоб захистити їх від перешкод, перехоплення або пошкодження?	1. Забезпечити, щоб лінії електропостачання та телекомунікації до об'єктів обробки інформації були підземними, де це можливо, або були забезпечені адекватним альтернативним захистом. 2. Відокремити силові кабелі від комунікаційних, щоб запобігти виникненню перешкод. 3. Для чутливих або критично важливих систем забезпечити а) встановлення броньованих кабелепроводів та замкнених приміщень або боксів, а також сигналізації в точках перевірки та завершення роботи; б) використання електромагнітного екранування для захисту кабелів в) періодичні технічні перевірки та фізичні огляди для виявлення несанкціонованих пристроїв, підключених до кабелів; г) контрольований доступ до комутаційних панелей та кабельних приміщень (наприклад, за допомогою механічних ключів або PIN-кодів) д) використання волоконно-оптичних кабелів; 4. Переконайтися, що кабелі мають маркування на кожному кінці з достатньою інформацією про джерело та пункт призначення, щоб забезпечити фізичну ідентифікацію та перевірку кабелю.	1. Політика фізичної та екологічної безпеки (Вимоги до забезпечення безпеки кабелювання).		Невідповідність	0%	

			5. Отримати консультацію фахівця щодо управління ризиками, які виникають внаслідок інцидентів або несправностей кабелів.					
7.13	Технічне обслуговування обладнання	БЕЗ ЗМІН: Чи існує суворий графік технічного обслуговування обладнання?	1. Переконайтися, що обладнання обслуговується відповідно до рекомендованої постачальником періодичності та специфікацій. - чи потрібно взагалі? 2. Впровадити та контролювати програму технічного обслуговування для всього обладнання. 3. Переконатися, що тільки уповноважений персонал виконує ремонт і технічне обслуговування обладнання. 4. Забезпечити ведення обліку всіх підозрюваних або фактичних несправностей, а також усіх профілактичних та коригувальних робіт. 5. Впровадити відповідні заходи контролю, коли обладнання заплановано для технічного обслуговування, включаючи нагляд за технічним персоналом на місці та контроль доступу для дистанційного обслуговування. 6. Впровадити процес нагляду за технічним персоналом під час проведення технічного обслуговування на місці. 7. Забезпечити, щоб процес технічного обслуговування обладнання відповідав усім вимогам до технічного обслуговування, встановленим страховою компанією. 8. Забезпечити перевірку обладнання після технічного обслуговування, щоб переконатися, що воно не було пошкоджене і функціонує належним чином. 9. Вживати заходів для безпечної утилізації або повторного використання обладнання, якщо визначено, що воно підлягає утилізації.	1.Документована програма технічного обслуговування обладнання. 2.Політика фізичної та екологічної безпеки (Вимоги до забезпечення безпеки обладнання).		Невідповідність	0%	
7.14	Безпечна утилізація або повторне використання обладнання	БЕЗ ЗМІН: 1. Чи існує політика щодо повторного використання інформаційних активів? 2. Якщо дані видаляються, чи перевіряється це належним чином перед повторним використанням/утилізацією?	1. Перед утилізацією або повторним використанням перевірити, чи містяться носії інформації в обладнанні. 2. Переконатися, що існує процес фізичного знищення носіїв інформації, що містять конфіденційну інформацію або інформацію, захищену авторським правом, або знищення, видалення чи перезапису інформації з використанням методів, які унеможливлюють відновлення первинної інформації. 3. Переконатися, що існує процес видалення етикеток та маркування, що ідентифікують організацію або вказують на класифікацію, власника, систему чи мережу, перед утилізацією, включаючи перепродаж або пожертвування на благодійність. 4. Розглянути можливість демонтажу засобів контролю безпеки, таких як системи контролю доступу або обладнання для спостереження, в кінці оренди або при виїзді з приміщення, виходячи з різних факторів, включаючи договори оренди, ризики	1. Правила роботи з медіа-матеріалами.		Невідповідність	0%	

			та можливість повторного використання засобів контролю. 5. Запровадити процедуру оцінки ризиків щодо пошкодженого обладнання, яке містить носії інформації, щоб визначити, чи потрібно їх фізично знищувати, а не відправляти на ремонт або викидати. 6. Впровадити повне шифрування диска для зменшення ризику розголошення конфіденційної інформації при утилізації або передислокації обладнання. 7. Перевірити інструменти перезапису, щоб переконатися, що вони сумісні з технологією носіїв інформації.					
8	**Technological controls**							
8.1	Кінцеві пристрої користувача	Було: 6.2.1, 11.2.8 1. Чи існує політика щодо мобільних пристроїв? 2. Чи затверджена ця політика керівництвом? 3. Чи документує політика додаткові ризики, пов'язані з використанням мобільних пристроїв (наприклад, крадіжка активів, використання відкритих бездротових точок доступу тощо)? 1. Чи має організація політику щодо захисту обладнання, яке залишається без нагляду? 2. Чи існують технічні засоби контролю для захисту обладнання, яке ненавмисно залишили без нагляду? Стало: 1. Чи існує політика щодо безпечної конфігурації та поводження з кінцевими пристроями користувачів, орієнтована на конкретну тему? 2. Чи затверджена ця політика керівництвом? 3. Чи всі користувачі ознайомлені з цією політикою? 4. Чи має організація політику на випадок крадіжки або втрати кінцевих пристроїв користувачів? 5. Чи існує політика щодо персональних	1. Впровадити політику безпечної конфігурації та поводження з кінцевими пристроями користувачів. 2. Переконатися, що ця політика включає наступне: a) тип інформації та рівень класифікації, яку користувацькі кінцеві пристрої можуть обробляти, зберігати, зберігати або підтримувати b) реєстрація кінцевих пристроїв користувачів c) вимоги до фізичного захисту r) обмеження на встановлення програмного забезпечення (наприклад, дистанційно контрольованого системними адміністраторами); e) вимоги до програмного забезпечення кінцевих пристроїв користувачів (включаючи версії програмного забезпечення) та до застосування оновлень (наприклад, активне автоматичне оновлення); f) правила підключення до інформаційних служб, публічних мереж або будь-яких інших мереж за межами приміщення (наприклад, вимога щодо використання персонального брандмауера); g) контроль доступу; h) шифрування пристроїв зберігання даних; i) захист від шкідливого програмного забезпечення; j) віддалене відключення, видалення або блокування; k) резервне копіювання; l) використання веб-сервісів та веб-додатків; m) аналітика поведінки кінцевого користувача; n) використання знімних пристроїв, включаючи знімні пристрої пам'яті, та можливість відключення фізичних портів (наприклад, USB-портів) o) використання можливостей розділення, якщо це підтримується кінцевим пристроєм користувача, які можуть безпечно відокремити інформацію організації та інші пов'язані з нею активи (наприклад, програмне забезпечення) від іншої інформації та інших пов'язаних з нею активів на пристрої.	1.Політика управління мобільними пристроями (Політика щодо безпечної конфігурації та обробки пристроїв кінцевих користувачів). 2.Система управління мобільними пристроями (СУМП).		Невідповідність	0%	

		пристроїв? 6. Чи існують задокументовані процедури для бездротового підключення кінцевих пристроїв? 7. ???	3. Довести цю політику до відома всього відповідного персоналу. 4. Передбачити додаткові технічні засоби захисту на пристрої, якщо певна інформація є настільки чутливою, що доступ до неї можна отримати лише через кінцеві пристрої користувачів, але не зберігати її на таких пристроях. 5. Проінформувати всіх користувачів про вимоги безпеки та процедури захисту кінцевих пристроїв користувачів, а також про їхні обов'язки щодо впровадження таких заходів безпеки. Проінструктуйте їх про наступне: а) виходити з активних сеансів і завершувати роботу служб, якщо вони більше не потрібні; б) захищати кінцеві пристрої користувачів від несанкціонованого використання за допомогою фізичного контролю (наприклад, блокування ключем або спеціальними замками) та логічного контролю (наприклад, доступ за паролем), коли вони не використовуються; не залишати без нагляду пристрої, на яких зберігається важлива, конфіденційна або критична бізнес-інформація; с) з особливою обережністю використовуйте пристрої в громадських місцях, відкритих офісах, місцях проведення зустрічей та інших незахищених місцях (наприклад, уникайте читання конфіденційної інформації, якщо люди можуть читати зі зворотного боку, використовуйте фільтри екрану конфіденційності); г) фізично захищати кінцеві пристрої користувачів від крадіжок (наприклад, в автомобілях та інших видах транспорту, готельних номерах, конференц-центрах та місцях проведення зустрічей). 6. Встановити конкретну процедуру для випадків крадіжки або втрати кінцевих пристроїв користувачів з урахуванням правових, законодавчих, нормативних, договірних (зокрема страхових) та інших вимог безпеки організації. 7. Якщо використання особистих пристроїв дозволено, впровадити додаткові засоби контролю, такі як а) розмежування особистого та службового використання пристроїв, включаючи використання програмного забезпечення для підтримки такого розмежування та захисту службових даних на приватних пристроях; б) надання доступу до ділової інформації лише після того, як користувачі визнали свої обов'язки (фізичний захист, оновлення програмного забезпечення тощо), відмовилися від права власності на ділові дані, дозволили віддалене стирання даних організацією у випадку крадіжки чи втрати пристрою або коли вони більше не мають права користуватися послугою. У таких випадках слід					

			враховувати законодавство про захист персональних даних; в) політики та процедури для запобігання суперечкам щодо прав на інтелектуальну власність, розроблену на обладнанні, що перебуває у приватній власності, з урахуванням конкретної теми; г) доступ до обладнання, що перебуває у приватній власності (для перевірки безпеки машини або під час розслідування), якому може перешкоджати законодавство; е) ліцензійні угоди на програмне забезпечення, за якими організації можуть нести відповідальність за ліцензування клієнтського програмного забезпечення на кінцевих пристроях користувачів, що перебувають у приватній власності персоналу або зовнішніх користувачів. 8. Встановити процедури для налаштування бездротових з'єднань на пристроях та використання бездротових або дротових з'єднань з відповідною пропускною здатністю згідно з відповідними політиками для конкретної тематики.					
8.2	Привілейовані права доступу	Чи є облікові записи з привілейованим доступом окремо керованими та контрольованими?	1. Розробити процес авторизації для розподілу привілейованих прав доступу відповідно до політики управління доступом. 2. Цей процес авторизації повинен включати наступне: a) визначення користувачів, які потребують привілейованих прав доступу для кожної системи або процесу (наприклад, операційні системи, системи управління базами даних та додатки) b) надання привілейованих прав доступу користувачам за необхідності та на індивідуальній основі відповідно до політики контролю доступу для конкретної теми (тобто лише особам, які мають необхідну компетенцію для здійснення діяльності, що вимагає привілейованого доступу, та на основі мінімальних вимог до їхніх функціональних ролей); c) ведення процесу авторизації (тобто визначення того, хто може затверджувати права привілейованого доступу, або не надавати права привілейованого доступу до завершення процесу авторизації) та обліку всіх наданих привілеїв; г) визначення та впровадження вимог щодо закінчення терміну дії привілейованих прав доступу; е) вжиття заходів для забезпечення того, щоб користувачі знали про свої права привілейованого доступу та про те, коли вони перебувають у режимі привілейованого доступу. Можливі заходи включають використання спеціальних ідентифікаторів користувачів, налаштувань користувацького інтерфейсу або навіть спеціального обладнання; f) вимоги до автентифікації для привілейованих прав доступу можуть бути вищими, ніж для звичайних прав доступу. Перед виконанням роботи з привілейованими правами доступу може	1. Політика управління доступом. 2. Система управління доступом (централізована). **Додатково**: *3. Інструмент управління привілейованим доступом.*		Невідповідність	0%	

			знадобитися повторна автентифікація або підвищення рівня автентифікації; g) регулярно, а також після будь-яких організаційних змін, перевіряти користувачів, які працюють з привілейованими правами доступу, щоб переконатися, що їхні обов'язки, ролі, відповідальність та компетенція все ще дають їм право працювати з привілейованими правами доступу; h) встановлення спеціальних правил для уникнення використання загальних ідентифікаторів користувачів для адміністрування (наприклад, "root"), залежно від можливостей конфігурації системи. Управління та захист автентифікаційної інформації таких ідентифікаторів; i) надання тимчасового привілейованого доступу лише на часовий проміжок, необхідний для реалізації затверджених змін або дій (наприклад, для технічного обслуговування або деяких критичних змін), замість постійного надання привілейованих прав доступу. Цю процедуру часто називають процедурою "розбитого скла" і часто автоматизують за допомогою технологій управління привілейованим доступом; j) реєструвати всі випадки привілейованого доступу до систем для цілей аудиту; k) не надавати спільні або пов'язані ідентичності з привілейованими правами доступу кільком особам, призначаючи кожній особі окрему ідентичність, яка дозволяє призначати конкретні привілейовані права доступу. Ідентифікатори можуть бути згруповані (наприклад, шляхом визначення групи адміністраторів), щоб спростити управління привілейованими правами доступу; l) використання ідентифікаторів з привілейованими правами доступу лише для виконання адміністративних завдань, а не для повсякденних загальних завдань [наприклад, перевірка електронної пошти, доступ до Інтернету (користувачі повинні мати окремий звичайний мережевий ідентифікатор для цих дій)].					
8.3	Обмеження доступу до інформації	Було: 9.2.4 Чи обмежено доступ до інформації та функцій прикладної системи відповідно до політики управління доступом? Стало: Чи обмежено доступ до інформації та інших пов'язаних з нею активів	1. Забезпечити обмеження доступу до інформації та інших пов'язаних з нею активів відповідно до встановленої політики. 2. Впровадити та керувати методами та процесами динамічного управління доступом до конфіденційної інформації. 3. Встановити правила управління динамічним доступом на основі конкретних випадків використання, враховуючи а) надання дозволів на доступ на основі ідентифікації особи, пристрою, місцезнаходження або програми; б) використання схеми класифікації для того, щоб визначити, яку інформацію потрібно захищати за допомогою методів управління	1. Політика управління доступом. 2. Система управління доступом (централізована).		Невідповідність	0%	

		відповідно до тематичної політики управління доступом?	динамічним доступом. 4. Впровадити операційні процеси, процеси моніторингу та звітності, а також підтримуючу технічну інфраструктуру. 5. Впровадити системи динамічного управління доступом, які вимагають автентифікації, обмежують доступ, використовують шифрування, визначають дозволи на друк та реєструють доступ до інформації та її використання.					
8.4	Доступ до вихідного коду	Було: 9.4.5 Чи захищено доступ до вихідного коду системи контролю доступу? Стало: 1. Чи існує політика, що регулює доступ на читання та запис до вихідного коду, інструментів розробки та програмних бібліотек? 2. Чи існує процес управління доступом до вихідного коду та пов'язаних з ним елементів і засобів розробки?	1. Встановити процедури контролю та управління доступом до вихідного коду, інструментів розробки та програмних бібліотек. 2. Впровадити централізовану систему зберігання, бажано систему управління вихідним кодом, для контролю доступу до вихідного коду. 3. Забезпечити впровадження процесів для a) управління доступом до вихідного коду програм та бібліотек вихідного коду програм відповідно до встановлених процедур; b) надання доступу на читання та запис вихідного коду на основі бізнес-потреб та управління ризиками зміни або неправомірного використання відповідно до встановлених процедур; c) оновлення вихідного коду та пов'язаних з ним елементів і надання доступу до вихідного коду відповідно до процедур контролю змін (див. 8.32) та виконання його лише після отримання відповідного дозволу; d) не надавати розробникам прямий доступ до сховища вихідного коду, а лише через інструменти розробника, які контролюють дії та дозволи на доступ до вихідного коду; e) зберігання лістингів програм у захищеному середовищі, де доступ до читання та запису має бути належним чином керованим та призначеним; f) ведення журналу аудиту всіх доступів та всіх змін до вихідного коду. 4. Якщо вихідний код призначено для публікації, впровадити додаткові засоби контролю для забезпечення його цілісності, такі як цифрові підписи.	1. Політика управління доступом. 2. Система управління доступом (централізована).		Невідповідність	0%	
8.5	Захищена автентифікація	Було: 9.4.2 Якщо цього вимагає політика контролю доступу, чи контролюється доступ за допомогою захищеної процедури входу в систему? Стало: Чи впроваджені безпечні технології та	1. Впровадити безпечні технології та процедури автентифікації, засновані на обмеженнях доступу до інформації та політиці управління доступом. 2. Обирати відповідний метод автентифікації, який підтверджує заявлену ідентичність користувача, програмного забезпечення, повідомлень та інших об'єктів. 3. Впровадити багатофакторну автентифікацію для доступу до критично важливих інформаційних систем. 4. Впровадити біометричну автентифікацію, яка повинна	1. Політика управління доступом. 2. Система управління доступом (централізована). 3. Система		Невідповідність	0%	

		процедури автентифікації, що базуються на обмеженнях доступу до інформації та тематичній політиці управління доступом?	супроводжуватися принаймні одним альтернативним методом автентифікації. 5. Впровадити безпечні процедури та технології входу в систему, враховуючи наступне: a) не відображати конфіденційну інформацію про систему або програму до успішного завершення процесу входу в систему, щоб уникнути надання неавторизованому користувачеві будь-якої непотрібної допомоги; б) відображення загального повідомлення, яке попереджає про те, що доступ до системи, додатку або сервісу повинен бути дозволений лише авторизованим користувачам; c) не надавати підказки під час процедури входу в систему, які могли б допомогти неавторизованому користувачеві (наприклад, у разі виникнення помилки система не повинна вказувати, яка частина даних є правильною, а яка - неправильною); г) перевірка інформації для входу в систему тільки після завершення введення всіх вхідних даних; e) захист від спроб грубого підбору імен користувачів та паролів [наприклад, використання повністю автоматизованого публічного тесту Тьюринга для розрізнення комп'ютерів і людей (CAPTCHA), вимога скидання паролю після заздалегідь визначеної кількості невдалих спроб або блокування користувача після максимальної кількості помилок]; f) ведення журналу невдалих та успішних спроб; g) генерування події безпеки при виявленні потенційної спроби або успішного порушення контролю входу в систему (наприклад, надсилання сповіщення користувачеві та системним адміністраторам організації при досягненні певної кількості спроб неправильного введення пароля); з) відображення або надсилання окремим каналом наступної інформації про завершення успішного входу в систему 1) дату та час попереднього успішного входу в систему 2) відомості про всі невдалі спроби входу з моменту останнього успішного входу; i) не відображати пароль відкритим текстом під час його введення; у деяких випадках може знадобитися деактивувати цю функцію, щоб полегшити вхід користувача в систему (наприклад, з міркувань доступності або щоб уникнути блокування користувачів через повторні помилки); j) не передавати паролі відкритим текстом через мережу, щоб уникнути їх перехоплення мережевою програмою-"сніффером"; k) завершення неактивних сеансів після певного періоду бездіяльності, особливо в місцях підвищеного ризику, таких як	керування ідентичністю			

			громадські або зовнішні зони, що не підпадають під систему управління безпекою організації, або на кінцевих пристроях користувачів; l) обмеження тривалості з'єднання для забезпечення додаткової безпеки для додатків з високим рівнем ризику та зменшення можливостей для несанкціонованого доступу.					
8.6	Управління потужністю	БЕЗ ЗМІН: Чи існує процес управління потужністю?	1. Визначити потреби в ресурсах для обробки інформації, людських ресурсах, офісах та інших об'єктах з урахуванням бізнес-критичності відповідних систем і процесів. 2. Застосовувати налаштування та моніторинг систем для забезпечення та, за необхідності, підвищення доступності та ефективності систем. 3. Провести стрес-тести систем та послуг для підтвердження наявності достатньої пропускної здатності системи для задоволення пікових вимог до продуктивності. 4. Впровадити засоби контролю для своєчасного виявлення проблем. 5. Прогнозувати майбутні потреби у потужностях з урахуванням нових бізнес- і системних вимог, а також поточних і прогнозованих тенденцій у сфері обробки інформації в організації. 6. Моніторинг використання ключових системних ресурсів та виявлення потенційних ресурсних обмежень і залежностей від ключового персоналу. 7. Розглянути можливість найму нового персоналу, отримання нових приміщень або площ, придбання більш потужних систем обробки, пам'яті та сховищ, а також використання хмарних обчислень для збільшення потужностей. 8. Розглянути можливість видалення застарілих даних, утилізації паперових записів, виведення з експлуатації додатків, систем, баз даних або середовищ, оптимізації пакетних процесів і розкладів, оптимізації коду додатків або запитів до баз даних, а також заборони або обмеження пропускної здатності для ресурсоємних послуг, щоб зменшити попит на ресурси організації. 9. Впровадити задокументований план управління потужностями для критично важливих систем.	1. Задокументовані вимоги до потужностей. 2. Задокументований план управління потужностями.		Невідповідність	0%	
8.7	Захист від шкідливого програмного забезпечення	БЕЗ ЗМІН: 1. Чи впроваджені процеси для виявлення шкідливого програмного забезпечення? 2. Чи впроваджені процеси для запобігання поширенню шкідливого програмного забезпечення? 3. Чи має організація процес та	1. Впровадити правила та засоби контролю, які запобігають або виявляють використання несанкціонованого програмного забезпечення (наприклад, список дозволених програм). 2. Впровадити засоби контролю, які запобігають або виявляють використання відомих або підозрюваних шкідливих веб-сайтів (наприклад, блокування). 3. Зменшити вразливості, які можуть бути використані шкідливим програмним забезпеченням (наприклад, за допомогою	1. Політика захисту від шкідливого програмного забезпечення. 2. Політика управління вразливостями.		Невідповідність	0%	

		можливості для відновлення після зараження шкідливим програмним забезпеченням.	управління технічними вразливостями). 4. Запровадити процес проведення регулярної автоматизованої перевірки програмного забезпечення та вмісту даних систем, особливо для систем, що підтримують критичні бізнес-процеси; розслідувати наявність будь-яких несанкціонованих файлів або несанкціонованих змін. 5. Встановити заходи захисту від ризиків, пов'язаних з отриманням файлів і програмного забезпечення із зовнішніх мереж або через них, або на будь-яких інших носіях. 6. Встановити програмне забезпечення для виявлення та усунення шкідливого програмного забезпечення для сканування комп'ютерів та електронних носіїв інформації, а також розробити план його регулярного оновлення, що включає в себе 1) перевірку будь-яких даних, отриманих через мережі або з будь-яких електронних носіїв, на наявність шкідливого програмного забезпечення перед використанням; 2) перевірку на наявність шкідливого програмного забезпечення вкладень електронної пошти та миттєвих повідомлень, а також завантажених файлів перед їх використанням. Здійснювати цю перевірку в різних місцях (наприклад, на поштових серверах, настільних комп'ютерах) та при вході в мережу організації; 3) сканування веб-сторінок на наявність шкідливого програмного забезпечення під час доступу до них; 7. Визначити розміщення та конфігурацію засобів виявлення та усунення шкідливого програмного забезпечення на основі результатів оцінки ризиків та з урахуванням принципів глибокого захисту і методів ухилення зловмисників. 8. Подбати про захист від впровадження шкідливого програмного забезпечення під час технічного обслуговування та аварійних процедур. 9. Впровадити процедуру надання дозволу на тимчасове або постійне відключення деяких або всіх заходів захисту від зловмисного програмного забезпечення, включаючи повноваження щодо затвердження винятків, задокументоване обґрунтування та дату перегляду. 10. Підготувати відповідні плани безперервності бізнесу для відновлення після атак зловмисного програмного забезпечення, включаючи всі необхідні заходи з резервного копіювання та відновлення даних і програмного забезпечення. 11. Ізолювати середовища, де можуть виникнути катастрофічні наслідки. 12. Визначити процедури та обов'язки щодо захисту систем від шкідливого програмного забезпечення, включаючи навчання їх	3. Система захисту від шкідливого програмного забезпечення.			

			використанню, звітності та відновленню після атак шкідливого програмного забезпечення. 13. Забезпечити обізнаність або навчання всіх користувачів щодо того, як ідентифікувати та потенційно зменшити ризик отримання, відправлення або встановлення електронних листів, файлів або програм, заражених шкідливим програмним забезпеченням. 14. Впровадити процедури для регулярного збору інформації про нове шкідливе програмне забезпечення, наприклад, підписатися на списки розсилки або переглядати відповідні веб-сайти. 15. Переконатися, що інформація про шкідливе програмне забезпечення, наприклад, попереджувальні бюлетені, надходить з кваліфікованих та авторитетних джерел, є точною та інформативною.					
8.8	Управління технічними вразливостями	Було: 12.6.1, 18.2.3 1. Чи має організація доступ до актуальної та своєчасної інформації про технічні вразливості? 2. Чи існує процес оцінки ризиків та реагування на будь-які нові вразливості в міру їх виявлення? Чи проводить організація регулярні перевірки технічних вимог до своїх інформаційних систем? Стало: 1. Чи має організація доступ до актуальної та своєчасної інформації про технічні вразливості? 2. Чи існує процес оцінки ризиків та реагування на будь-які нові вразливості в міру їх виявлення?	1. Розробити та підтримувати актуальну інвентаризацію всіх програмних та апаратних засобів в організації, яка повинна містити такі дані, як постачальник програмного забезпечення, назва програмного забезпечення, номери версій, поточний стан розгортання (наприклад, яке програмне забезпечення встановлено на яких системах) та особа (особи) в організації, відповідальна (відповідальні) за програмне забезпечення. 2. Визначити та встановити ролі та обов'язки, пов'язані з управлінням технічними вразливостями, включаючи моніторинг вразливостей, оцінку ризиків вразливостей, оновлення, відстеження активів та будь-які необхідні обов'язки з координації. 3. Визначити ресурси для отримання інформації про технічні вразливості для всього програмного забезпечення та технологій, перелічених в інвентаризації активів. Встановити процедуру оновлення переліку інформаційних ресурсів на основі змін в інвентаризації або при виявленні інших нових або корисних ресурсів. 4. Запровадити процедуру роботи з постачальниками, яка гарантуватиме, що вони повідомлятимуть, оброблятимуть та розкриватимуть вразливості, включивши відповідні вимоги до контрактів. 5. Запровадити використання інструментів сканування вразливостей, придатних для технологій, що використовуються. 6. Розробити та впровадити план проведення запланованих, задокументованих та повторюваних тестів на проникнення або оцінок вразливостей компетентними та уповноваженими особами для підтримки виявлення вразливостей. 7. Впровадити процес відстеження використання сторонніх бібліотек та вихідного коду для виявлення вразливостей та включити його в практику безпечного кодування.	1. Задокументована інвентаризація всіх програмних та апаратних активів в організації. (Інвентаризація активів) 2. Політика управління вразливостями. 3. Система управління вразливостями.		Невідповідність	0%	

			8. Розробити процедури та можливості для виявлення вразливостей у продуктах, послугах та будь-яких зовнішніх компонентах, що використовуються, а також для отримання звітів про вразливості з внутрішніх та зовнішніх джерел. 9. Створити публічну контактну особу та запровадити процедури повідомлення про вразливості, включаючи онлайн-форми та форуми для розвідки загроз або обміну інформацією. Розгляньте можливість впровадження програми винагороди за виправлення помилок. 10. Налагодити процес обміну інформацією з компетентними галузевими органами або іншими зацікавленими сторонами. 11. Запровадити процес оцінки технічних вразливостей, який має включати наступні дії: а) аналіз та перевірка звітів для визначення необхідних заходів реагування та усунення недоліків б) після виявлення потенційної технічної вразливості визначити пов'язані з нею ризики та заходи, які необхідно вжити. Такі дії можуть включати оновлення вразливих систем або застосування інших засобів контролю. 12. Впровадити процес управління оновленням програмного забезпечення, щоб забезпечити встановлення найновіших затверджених патчів та оновлень для всього авторизованого програмного забезпечення. 13. Визначити графік для вжиття відповідних та своєчасних заходів у відповідь на виявлення потенційних технічних вразливостей. 14. Забезпечити, щоб дії здійснювалися відповідно до засобів контролю, пов'язаних з управлінням змінами або з дотриманням процедур реагування на інциденти інформаційної безпеки. 15. Забезпечити отримання оновлень тільки з законних джерел, які можуть бути внутрішніми або зовнішніми по відношенню до організації. 16. Впровадити процес тестування та оцінки оновлень перед їх встановленням, щоб переконатися, що вони ефективні та не призводять до побічних ефектів, які не можна терпіти. 17. Запровадити процес першочергового реагування на системи з високим рівнем ризику. 18. Розробити заходи з виправлення ситуації (як правило, оновлення програмного забезпечення або патчі) та протестувати їх, щоб підтвердити, що виправлення або пом'якшення наслідків є ефективними. 19. Створити механізм перевірки достовірності виправлення ситуації. 20. Якщо оновлення недоступні або неможливі, розглянути					

			можливість впровадження інших засобів контролю, таких як застосування будь-якого обхідного шляху, запропонованого постачальником програмного забезпечення або іншими відповідними джерелами; вимкнення послуг або можливостей, пов'язаних з вразливістю; адаптація або додавання засобів контролю доступу на кордонах мережі; посилення моніторингу для виявлення фактичних атак; підвищення обізнаності про вразливість серед відповідних зацікавлених сторін. 21. Створити та вести детальний журнал аудиту для всіх кроків, здійснених в рамках управління технічними вразливостями. 22. Запровадити процес регулярного моніторингу та оцінки процесу управління технічними вразливостями для забезпечення його ефективності та результативності. 23. Створити механізм координації між процесом управління технічними вразливостями та діяльністю з управління інцидентами, щоб полегшити передачу даних про вразливості до функції реагування на інциденти та забезпечити технічні процедури, які необхідно виконати у разі виникнення інциденту. 23. У разі використання хмарних сервісів забезпечити, щоб обов'язки постачальника хмарних послуг щодо управління технічними вразливостями були чітко визначені в договорі про надання послуг, а також щоб існував процес звітування про його дії, пов'язані з технічними вразливостями. 24. Інтегрувати процес управління технічними вразливостями з існуючими процесами та процедурами управління змінами. 25. Враховувати ризики, пов'язані з виправленнями або оновленнями програмного забезпечення, що може передбачати відтермінування оновлень для оцінки пов'язаних з ними ризиків на основі досвіду, отриманого від інших користувачів, або забезпечення автоматизованого процесу оновлення, коли ці оновлення встановлюються на відповідні системи або продукти без необхідності втручання з боку клієнта або користувача.					
8.9	Управління конфігурацією	1. Чи визначені та впроваджені процеси та інструменти для забезпечення дотримання конфігурацій, в тому числі конфігурацій безпеки, апаратного, програмного забезпечення, послуг та мереж? 2. ???	1. Визначити та задокументуйте конфігурації всього обладнання, програмного забезпечення, послуг та мереж в організації. Це включає конфігурації безпеки, а також конфігурації, пов'язані з функціональністю. 2. Визначити та впровадити інструменти та процеси для забезпечення дотримання цих конфігурацій у всіх системах та протягом усього терміну їх експлуатації. 3. Визначити ролі та обов'язки для управління цими конфігураціями та забезпечення їхньої актуальності. Визначити процедури для управління всіма змінами конфігурації. 4. Розробити стандартні шаблони для безпечної конфігурації	1. Базові конфігурації або задокументовані конфігурації для всього апаратного та програмного забезпечення, послуг та мереж усередині організації.		Невідповідність	0%	

			обладнання, програмного забезпечення, послуг та мереж. Ці шаблони повинні а) використовувати загальнодоступні рекомендації, такі як попередньо визначені шаблони від постачальників та незалежних організацій, що займаються питаннями безпеки; б) враховувати рівень захисту, необхідний для визначення достатнього рівня безпеки с) підтримувати політику інформаційної безпеки організації, тематичні політики, стандарти та інші вимоги безпеки; г) враховувати доцільність і застосовність конфігурацій безпеки в контексті організації. 5. Для створення стандартних шаблонів безпечної конфігурації обладнання, програмного забезпечення, послуг та мереж слід враховувати наступне: а) мінімізація кількості ідентифікаторів з привілейованими правами доступу або правами адміністратора; б) вимкнення непотрібних, невикористовуваних або небезпечних ідентифікаторів; в) відключення або обмеження непотрібних функцій та сервісів г) обмеження доступу до потужних службових програм та налаштувань параметрів хосту; е) синхронізація годинника f) зміна інформації автентифікації за замовчуванням, наданої виробником, наприклад, паролів за замовчуванням, одразу після встановлення та перегляд інших важливих параметрів безпеки за замовчуванням; g) виклик засобів тайм-ауту, які автоматично вимикають комп'ютерні пристрої після заздалегідь визначеного періоду бездіяльності; h) перевірка дотримання ліцензійних вимог. 6. Встановити процес періодичного перегляду та оновлення таких шаблонів, особливо у відповідь на нові загрози або вразливості, або впровадження нових версій програмного чи апаратного забезпечення. 7. Запровадити облік встановлених конфігурацій усіх апаратних засобів, програмного забезпечення, послуг та мереж, а також ведення журналу всіх змін у цих конфігураціях. 8. Створити механізми, такі як бази даних конфігурацій або шаблони конфігурацій для безпечного зберігання цих записів. 9. Забезпечити дотримання формального процесу управління змінами для всіх змін у конфігураціях. 10. Впровадити процес моніторингу всіх конфігурацій за допомогою комплексного набору інструментів управління	2. Задокументовані стандартні шаблони для безпечної конфігурації апаратного та програмного забезпечення, послуг та мереж. 3.Програмне забезпечення перевірки конфігурацій або журнал для встановлених конфігурацій всього апаратного та програмного забезпечення, послуг та мереж, і запис усіх змін до цих конфігурацій.				

			системою. Ці інструменти можуть включати утиліти для обслуговування, віддалену підтримку, інструменти управління підприємством, програмне забезпечення для резервного копіювання та відновлення тощо. 11. Запровадити процес регулярного перегляду конфігурацій для перевірки параметрів конфігурації, оцінки надійності паролів та оцінки виконаних дій. 12. За необхідності, інтегрувати управління конфігураціями з процесами управління активами та відповідними інструментами. 13. При створенні безпечних шаблонів конфігурацій забезпечити їх відповідний захист від несанкціонованого доступу, якщо вони містять конфіденційну інформацію.					
8.10	Видалення інформації	1. Чи існує процедура, яка документує, коли, як і де слід видаляти інформацію? 2. Чи включені вимоги щодо видалення інформації в угоди з третіми сторонами?	1. Розробити процедуру видалення інформації, яка визначає а) вибір методу видалення (наприклад, електронний перезапис або криптографічне стирання) відповідно до бізнес-вимог та з урахуванням відповідних законів і нормативних актів б) фіксування результатів видалення як доказів; в) при використанні постачальників послуг з видалення інформації, отримання від них доказів видалення інформації. 2. У разі залучення третіх осіб до зберігання інформації організації, вимоги щодо видалення інформації мають бути включені до договорів з третіми особами для забезпечення їх виконання під час та після припинення надання таких послуг. 3. Впровадити безпечні методи видалення інформації, коли чутлива інформація більше не потрібна: а) ... - чи потрібно їх описувати взагалі? чи достатньо п.1? 4. Автоматизувати процеси видалення відповідно до тематичних політик, якщо вони доступні та застосовні. 5. Створити запис про видалення інформації.	1. Процедура видалення інформації. 2. Запис про видалення інформації. 3. Система безпечного видалення інформації.		Невідповідність	0%	
8.11	Маскування даних	Чи встановлені методи маскування даних відповідно до тематичної політики організації щодо доступу контролю доступу та іншими пов'язаними політиками, а також бізнес-вимогами?	1. Встановити відповідні методи маскування даних. Це може включати а) методи псевдонімізації або анонімізації, які приховують ОВІ, маскують справжню особу розпорядників ОВІ(PII) або іншу конфіденційну інформацію та розривають зв'язок між ОВІ та особою розпорядника ОВІ або зв'язок між іншою конфіденційною інформацією; б) додаткові методи маскування даних, такі як шифрування, обнулення або видалення символів, зміна чисел і дат, підстановка та заміна значень їхнім хешем. 2. Переконатися, що дані були належним чином псевдонімізовані або анонімізовані при використанні методів псевдонімізації або анонімізації. 3. Під час застосування методів маскування даних враховувати	1. Політика маскування даних або вимоги до маскування даних.		Невідповідність	0%	

			наступне: а) не можна надавати всім користувачам доступ до всіх даних, тому слід розробляти запити та маски таким чином, щоб показувати користувачеві лише мінімально необхідні дані; б) існують випадки, коли деякі дані не повинні бути видимими для користувача для деяких записів з набору даних; у цьому випадку розробляється та впроваджується механізм затемнення даних (наприклад, якщо пацієнт не хоче, щоб персонал лікарні бачив усі його записи, навіть у випадку надзвичайної ситуації, то персоналу лікарні надаються частково затемнені дані, а доступ до даних може бути наданий лише персоналу з певними ролями, якщо вони містять корисну інформацію для відповідного лікування); с) при завуальовуванні даних надавати суб'єкту ОВІ можливість вимагати, щоб користувачі не могли бачити, чи були дані завуальовані (завуальовування завуальовування; це використовується в медичних установах, наприклад, якщо пацієнт не хоче, щоб персонал бачив, що конфіденційна інформація, така як вагітності чи результати кров'яних тестів, була завуальована); г) будь-які законодавчі або регуляторні вимоги (наприклад, вимога маскування інформації про платіжні картки під час обробки або зберігання). 4. Використовувати маскування даних, псевдонімізацію або анонімізацію, враховуйте наступне: а) рівень надійності маскування, псевдонімізації або анонімізації даних відповідно до використання оброблюваних даних; б) контроль доступу до оброблених даних; с) угоди або обмеження на використання оброблених даних; г) заборону зіставлення оброблених даних з іншою інформацією з метою ідентифікації розпорядника PII; е) відстеження надання та отримання оброблених даних.					
8.12	Запобігання витоку даних	Чи визначені та застосовуються заходи щодо запобігання витоку даних?	1. Розробити та впровадити процес ідентифікації та класифікації конфіденційної інформації (наприклад, персональні дані, моделі ціноутворення, дизайн продукції), яка потребує захисту від витоку даних. 2. Скласти та регулярно переглядати перелік потенційних каналів витоку даних, які можуть включати електронну пошту, передачу файлів, мобільні пристрої та портативні носії інформації. 3. Впровадити процедури для запобігання витоку даних, такі як карантин електронних листів, що містять конфіденційну інформацію. 4. Розгорнути та налаштувати інструменти запобігання витоку даних для того, щоб а) виявлення та моніторингу конфіденційної інформації, що	1.Політика запобігання витоку даних. 2.Система запобігання витоку даних (СЗВД).		Невідповідність	0%	

			піддається ризику несанкціонованого розголошення (наприклад, у неструктурованих даних у системі користувача) б) виявляти розголошення конфіденційної інформації (наприклад, коли інформація завантажується на ненадійні сторонні хмарні сервіси або надсилається електронною поштою) в) блокувати дії користувача або мережеві передачі, які розкривають конфіденційну інформацію (наприклад, запобігання копіюванню записів бази даних в електронну таблицю). 5. Оцінити та прийняти рішення щодо необхідності обмеження можливостей користувачів копіювати, вставляти або завантажувати дані за межами організації. За потреби, запровадьте необхідні обмеження, використовуючи такі технології, як інструменти запобігання витоку даних або налаштувавши існуючі інструменти, які дозволяють користувачам переглядати та маніпулювати даними, що зберігаються віддалено, але запобігають копіюванню та вставці даних поза межами контролю організації. 6. Запровадити процес, за яким власник даних затверджує експорт даних та притягує користувачів до відповідальності за їхні дії. 7. Вирішити проблему потенційного витоку за допомогою скріншотів або фотографій екрану через умови використання, навчання та аудит. 8. Впровадити заходи шифрування, контролю доступу та фізичного захисту для резервних копій даних, щоб запобігти витоку конфіденційної інформації. 9. Розробити стратегії захисту від розвідувальних дій супротивника, спрямованих на отримання конфіденційної або секретної інформації, в тому числі з використанням таких методів, як підміна достовірної інформації неправдивою, зворотна соціальна інженерія або використання "медових пасток". 10. Перед розгортанням засобів запобігання витоку даних враховувати законодавчі та регуляторні вимоги, пов'язані з конфіденційністю, захистом даних, працевлаштуванням, перехопленням даних та телекомунікаціями. 11. Підтримати зусилля із запобігання витоку даних за допомогою стандартних засобів контролю безпеки, таких як контроль доступу та політики безпечного документообігу.					
8.13	Резервне копіювання даних	Було: 12.3.1 1. Чи існує узгоджена політика резервного копіювання? 2. Чи відповідає політика резервного копіювання організації відповідним	1. Розробити та підтримувати політику резервного копіювання, яка відповідає вимогам організації щодо збереження даних та інформаційної безпеки. 2. Забезпечити належні засоби резервного копіювання для відновлення важливої інформації, програмного забезпечення та систем після інциденту або втрати носія інформації.	1.Політика резервного копіювання. 2.Розклад та реєстр резервного		Невідповідність	0%	

		законодавчим нормам? 3. Чи створюються резервні копії відповідно до політики? 4. Чи тестуються резервні копії? Стало: 1. Чи існує спеціальна політика, що регулює резервне копіювання інформації, програмного забезпечення та систем? 2. Чи створюються резервні копії відповідно до політики? 3. Чи перевіряються резервні копії? 4. ?	3. Розробити та впровадити план резервного копіювання інформації, програмного забезпечення та систем відповідно до політики резервного копіювання. 4. Переконайтися, що план резервного копіювання враховує наступне: a) створення точних і повних записів про резервні копії та задокументовані процедури відновлення; b) відображення бізнес-вимог організації (наприклад, мета точки відновлення), вимог безпеки відповідної інформації та критичності інформації для безперервної роботи організації в обсязі (наприклад, повне або диференційоване резервне копіювання) та частоті резервного копіювання; c) зберігання резервних копій у безпечному та захищеному віддаленому місці, на достатній відстані, щоб уникнути будь-якої шкоди від катастрофи на основному місці; d) забезпечення належного рівня фізичного та екологічного захисту резервних копій відповідно до стандартів, що застосовуються на головному майданчику; e) регулярне тестування носіїв резервних копій, щоб переконатися, що на них можна покластися для екстреного використання в разі потреби. Перевірка здатності відновлювати резервні копії даних на тестовій системі, не перезаписуючи оригінальні носії, у випадку, якщо процес резервного копіювання або відновлення завершиться невдачею і призведе до непоправного пошкодження або втрати даних; f) захист резервних копій за допомогою шифрування відповідно до виявлених ризиків (наприклад, у ситуаціях, коли важлива конфіденційність); g) подбати про те, щоб ненавмисна втрата даних була виявлена до того, як буде зроблена резервна копія. 5. Впровадити операційні процедури для моніторингу виконання резервного копіювання та реагування на збої у виконанні запланованих резервних копій для забезпечення повноти резервного копіювання відповідно до політики резервного копіювання. 6. Впровадити процес регулярного тестування заходів з резервного копіювання для окремих систем та сервісів, щоб переконатися, що вони відповідають цілям плану реагування на інциденти та плану забезпечення безперервності бізнесу. Це повинно включати тестування процедур відновлення та перевірку часу відновлення, передбаченого планом забезпечення безперервності діяльності. 7. Переконатися, що у випадку критично важливих систем та	копіювання. 3.Система резервного копіювання.			

			послуг заходи з резервного копіювання охоплюють всі необхідні системи, інформацію, додатки та дані для повного відновлення системи у випадку катастрофи. 8. У разі використання хмарних сервісів забезпечити створення резервних копій інформації, додатків і систем організації в хмарному середовищі. Оцініть вимоги до резервного копіювання та їх виконання при використанні сервісу резервного копіювання інформації хмарного сервісу. - організаційна активність? 9. Визначити термін зберігання важливої бізнес-інформації з урахуванням будь-яких вимог до зберігання архівних копій. Впровадити процедури видалення інформації з носіїв резервних копій після закінчення терміну зберігання інформації відповідно до законодавства та нормативних актів.					
8.14	Резервування засобів обробки інформації	БЕЗ ЗМІН: Чи мають засоби обробки інформації достатнє резервування, щоб відповідати вимогам доступності організації?	1. Визначити вимоги організації до доступності бізнес-послуг та інформаційних систем. 2. Розробити та впровадити системну архітектуру з відповідними рівнями резервування для забезпечення цих вимог. 3. Спланувати та впровадити процедури активації резервних компонентів та засобів обробки даних. Ці процедури повинні визначати, чи завжди активуються резервні компоненти та засоби обробки даних, чи у випадку надзвичайних ситуацій вони активуються автоматично або вручну. 4. Забезпечити, щоб резервні компоненти та засоби обробки інформації підтримували той самий рівень безпеки, що й основні. 5. Впровадити механізми оповіщення для сповіщення організації про будь-які збої в засобах обробки інформації, що дозволить виконати заплановані процедури та підтримувати доступність під час ремонту або заміни засобів обробки інформації. 6. Враховувати наступні фактори при впровадженні резервних систем: а) укладання контрактів з двома або більше постачальниками мережевого обладнання та засобів обробки критично важливої інформації, наприклад, інтернет-провайдерами; б) використання резервних мереж; в) використання двох географічно відокремлених центрів обробки даних з дзеркальними системами г) використання фізично надлишкових джерел або блоків живлення е) використання декількох паралельних екземплярів програмних компонентів з автоматичним балансуванням навантаження між ними (між екземплярами в одному дата-центрі або в різних дата-центрах) f) наявність дубльованих компонентів у системах (наприклад,	1.Політика резервного копіювання. 2.Розклад та реєстр резервного копіювання. 3.Система резервного копіювання. 4. План управління потужностями.		Невідповідність	0%	

			процесор, жорсткі диски, пам'ять) або в мережах (наприклад, брандмауери, маршрутизатори, комутатори). 7. Тестувати резервні інформаційні системи, бажано у виробничому режимі, щоб переконатися, що перемикання з одного компонента на інший працює належним чином. 8. Визначити потенційні ризики для цілісності або конфіденційності інформації та інформаційних систем, що виникають внаслідок впровадження резервування. Ці ризики слід враховувати при проектуванні інформаційних систем. 9. У разі використання публічних хмарних обчислень розглянути можливість впровадження декількох робочих версій засобів обробки інформації в окремих фізичних локаціях з автоматичним відмовостійкістю та балансуванням навантаження між ними.					
8.15	Логування	Було: 12.4.1, 12.4.2, 12.4.3 Чи ведуться та регулярно переглядаються відповідні журнали подій? Чи захищені засоби реєстрації від фальсифікації та несанкціонованого доступу? Чи ведуться, захищаються та регулярно переглядаються журнали системного адміністратора / системного адміністратора? Стало: 1. Чи існує політика ведення журналів? 2. Чи ведуться та регулярно переглядаються відповідні журнали подій? 3. Чи захищені засоби реєстрації від несанкціонованого втручання та несанкціонованого доступу? 4. Чи регулярно проводиться аналіз журналів?	1. Створити політику ведення журналів, яка визначатиме, для чого створюються журнали, які дані збираються та реєструються, а також як захищати та обробляти дані журналів. 2. Заносити до журналу для кожної події, де це можливо, такі деталі, як a) ідентифікатори користувачів б) дії системи c) дати, час і деталі відповідних подій (наприклад, вхід і вихід з системи) d) ідентифікатор пристрою, ідентифікатор системи та місцезнаходження; д) мережеві адреси та протоколи. 3. Розглянути можливість реєстрації таких подій, як а) успішні та відхилені спроби доступу до системи; б) успішні та відхилені спроби доступу до даних та інших ресурсів; в) зміни конфігурації системи; г) використання привілеїв; е) використання службових програм і додатків; f) файли, до яких здійснювався доступ, і тип доступу, включаючи видалення важливих файлів даних; g) тривоги, що надходять від системи контролю доступу; h) активація та деактивація систем безпеки, таких як антивірусні системи та системи виявлення вторгнень; i) створення, зміна або видалення ідентифікаційних даних; j) транзакції, що виконуються користувачами в додатках. У деяких випадках додатки є послугою або продуктом, що надається або експлуатується третьою стороною. 4. Переконатися, що всі системи мають синхронізовані джерела часу, оскільки це дозволяє корелювати журнали між системами для аналізу, оповіщення та розслідування інциденту.	1.Політика ведення журналів та моніторингу. 2.Централізована система ведення журналів (SIEM-система) - система управління подіями та інформаційною безпекою.		Невідповідність	0%	

			5. Переконатися, що користувачі, в тому числі з привілейованими правами доступу, не мають права видаляти або деактивувати журнали власної діяльності. 6. Впровадити засоби контролю для захисту від несанкціонованої зміни інформації в журналах та проблем з роботою засобів реєстрації, в тому числі а) зміни типів повідомлень, що реєструються; б) редагування або видалення файлів журналів в) відмова від запису подій або перезапис минулих записаних подій, якщо обсяг носія, на якому зберігається файл журналу, перевищено. 7. Впроваджувати такі методи, як криптографічне хешування, запис у файл, доступний лише для додавання та читання, або запис у файл публічної прозорості для захисту журналів. 8. Архівувати певні журнали аудиту відповідно до вимог зберігання даних або вимог щодо збору та збереження доказів. 9. Деідентифікувати журнали, де це можливо, використовуючи методи маскування даних під час надсилання журналів системи або додатків постачальнику для налагодження або усунення помилок. 10. Впровадити належні заходи захисту конфіденційності для журналів подій, які містять конфіденційні дані та інформацію, що ідентифікує особу. 11. Налагодити процес регулярного аналізу журналів подій, враховуючи наступне: а) необхідні навички експертів, які виконують аналіз; б) визначення процедури аналізу журналу с) необхідні атрибути кожної події, пов'язаної з безпекою; г) винятки, виявлені за допомогою використання заздалегідь визначених правил [наприклад, управління інформацією та подіями забезпечення безпеки (SIEM) або правил брандмауера, а також систем виявлення вторгнень (IDS) або сигнатур шкідливого програмного забезпечення (ШПЗ)]; е) відомі моделі поведінки та стандартний мережевий трафік у порівнянні з аномальною активністю та поведінкою [аналіз поведінки користувачів та організацій (UEBA)]; f) результати аналізу тенденцій або шаблонів (наприклад, в результаті використання аналітики даних, методів великих даних і спеціалізованих інструментів аналізу) g) наявні розвідувальні дані про загрози. 12. Встановити конкретні заходи з моніторингу для виявлення та аналізу аномальної поведінки, такі як а) перегляд успішних і неуспішних спроб доступу до захищених				

			ресурсів [наприклад, серверів системи доменних імен (DNS), веб-порталів і файлообмінників]; б) перевірка журналів DNS для виявлення вихідних мережевих з'єднань зі зловмисними серверами, наприклад, пов'язаними з командними та контрольними серверами бот-мереж; в) вивчення звітів про використання від постачальників послуг (наприклад, рахунків або звітів про надання послуг) на предмет незвичної активності в системах та мережах (наприклад, шляхом перегляду шаблонів активності); d) включення журналів подій фізичного моніторингу, таких як вхід та вихід, для забезпечення більш точного виявлення та аналізу інцидентів; е) кореляція журналів для забезпечення ефективного та високоточного аналізу. 13. Впровадити процедуру ідентифікації підозрюваних та фактичних інцидентів інформаційної безпеки для подальшого розслідування (наприклад, в рамках процесу управління інцидентами інформаційної безпеки). 14. Розглянути можливість використання відповідних службових програм або інструментів аудиту для виявлення важливих подій для моніторингу інформаційної безпеки. 15. Використовувати інструмент SIEM або еквівалентний сервіс для зберігання, кореляції, нормалізації та аналізу інформації з журналів, а також для генерування сповіщень. Ретельно налаштовуйте SIEM, щоб оптимізувати їх переваги. - організаційна активність?					
8.16	Моніторингова діяльність	1. Чи існує процес моніторингу аномальної поведінки мереж, систем та додатків?	1. Створити систему моніторингу мереж, систем та додатків на предмет аномальної поведінки. 2. Визначити обсяг та рівень моніторингу відповідно до вимог бізнесу та інформаційної безпеки, беручи до уваги відповідні закони та нормативні акти. Зберігати записи моніторингу протягом визначених періодів зберігання. 3. Включити в систему моніторингу такі аспекти, як а) вихідний та вхідний мережевий, системний трафік та трафік додатків б) доступ до систем, серверів, мережевого обладнання, системи моніторингу, критично важливих додатків тощо в) файли конфігурації системи та мережі критичного або адміністративного рівня г) журнали інструментів безпеки [наприклад, антивірус, IDS, система запобігання вторгненням (IPS), веб-фільтри, брандмауери, запобігання витоку даних]; е) журнали подій, що стосуються системної та мережевої	1.Політика ведення журналів та моніторингу. 2.Централізована система ведення журналів (SIEM-система) - система управління подіями та інформаційною безпекою.		Невідповідність	0%	

			активності; f) перевірка того, що код, який виконується, має дозвіл на запуск в системі і що він не був змінений (наприклад, шляхом перекомпіляції для додавання додаткового небажаного коду) g) використання ресурсів (наприклад, процесор, жорсткі диски, пам'ять, пропускна здатність) та їх продуктивність. 4. Встановити базову лінію нормальної поведінки та здійснювати моніторинг щодо цієї базової лінії для виявлення аномалій, беручи до уваги а) аналіз використання систем у звичайні та пікові періоди; б) звичайний час доступу, місце доступу, частоту доступу для кожного користувача або групи користувачів. 5. Налаштувати систему моніторингу на встановлену базову лінію для виявлення аномальної поведінки, включаючи а) незаплановане завершення процесів або додатків; б) активність, зазвичай пов'язану зі шкідливим програмним забезпеченням або трафіком, що походить з відомих шкідливих IP-адрес або мережевих доменів (наприклад, пов'язаних з командними і керуючими серверами бот-мереж); в) відомі характеристики атаки (наприклад, відмова в обслуговуванні та переповнення буфера) г) незвична поведінка системи (наприклад, реєстрація натискань клавіш, впровадження процесів та відхилення у використанні стандартних протоколів) е) вузькі місця та перевантаження (наприклад, мережеві черги, рівні затримок та мережевий джиттер) f) несанкціонований доступ (фактичний або спроба) до систем або інформації g) несанкціоноване сканування бізнес-додатків, систем та мереж h) успішні та невдалі спроби доступу до захищених ресурсів (наприклад, DNS-серверів, веб-порталів та файлових систем) і) незвична поведінка користувачів і систем по відношенню до очікуваної поведінки. 6. Впровадити безперервний моніторинг за допомогою спеціального інструменту в режимі реального часу або через певні проміжки часу, залежно від потреб та можливостей організації. Переконайтеся, що інструмент може обробляти великі обсяги даних, адаптуватися до постійно мінливого ландшафту загроз, надавати сповіщення в реальному часі та бути здатним розпізнавати певні сигнатури і дані, а також моделі поведінки мережі або додатків. 7. Налаштувати програмне забезпечення для автоматизованого моніторингу, щоб генерувати сповіщення на основі попередньо				

			визначених порогових значень. Переконайтеся, що система оповіщення налаштована і навчена на базовому рівні організації, щоб мінімізувати помилкові спрацьовування. 8. Навчити персонал правильно інтерпретувати потенційні інциденти. 9. Повідомити про аномальні події відповідним сторонам для покращення аудиту, оцінки безпеки, сканування вразливостей та моніторингу. 10. Впровадити резервні системи та процеси для отримання та реагування на тривожні сповіщення. 11. Запровадити процедури для швидкого реагування на позитивні показники системи моніторингу, а також для виявлення та усунення помилкових спрацьовувань. 12. Посилити моніторинг безпеки шляхом а) використання систем розвідки загроз (див. 5.7) б) використання можливостей машинного навчання та штучного інтелекту с) використання блок-листів або списків дозволів г) проведення низки оцінок технічної безпеки (наприклад, оцінювання вразливостей, тестування на проникнення, моделювання кібератак та навчань з кіберреагування) та використання результатів цих оцінок для визначення базових показників або прийнятної поведінки е) використання систем моніторингу продуктивності для встановлення та виявлення аномальної поведінки; f) використання журналів у поєднанні з системами моніторингу. 13. Запровадити процес моніторингу аномальних комунікацій для виявлення бот-мереж.					
8.17	Синхронізація часу	Чи всі пристрої систем обробки інформації в організації синхронізовані з затвердженими джерелами часу?	1. Задокументувати та впровадити зовнішні та внутрішні вимоги до представлення часу, надійної синхронізації та точності. Ці вимоги можуть бути зумовлені юридичними, законодавчими, нормативними, договірними, стандартними вимогами та потребами внутрішнього моніторингу. 2. Визначити стандартний контрольний час, який має використовуватися в усіх системах організації, включно з системами управління будівлею, системами входу та виходу, а також іншими, які можуть допомогти в розслідуванні. 3. Використати годинник, прив'язаний до радіо часу, що транслюється національним атомним годинником або глобальною системою позиціонування (GPS), як еталонний годинник для систем реєстрації, щоб забезпечити точні часові позначки. 4. Використати такі протоколи, як протокол мережевого часу (NTP) або протокол точного часу (PTP), щоб синхронізувати всі мережеві	1.Документовані зовнішні та внутрішні вимоги щодо представлення часу, надійної синхронізації та точності. 2.Сервер NTP (Network Time Protocol) - сервер синхронізації часу в мережі.		Невідповідність	0%	

			системи з еталонним годинником. 5. Розглянути можливість використання двох зовнішніх джерел часу одночасно, щоб підвищити надійність зовнішніх годинників та керувати будь-якими відхиленнями. 6. Слідкувати за годинником кожного сервісу та фіксуйте різницю, щоб зменшити ризики, пов'язані з розбіжностями при використанні декількох хмарних сервісів або при використанні як хмарних, так і локальних сервісів. 7. Розуміти та доносити до персоналу важливість точного налаштування комп'ютерного годинника. Підкреслити, що точність журналів подій має важливе значення для розслідувань, юридичних та дисциплінарних справ, і що неточні журнали аудиту можуть перешкоджати розслідуванню та підривати достовірність доказів.					
0	Використання привілейованих службових програм	Чи обмежуються та контролюються привілейовані службові програми?	1. Обмежити використання службових програм, які можуть перевизначати засоби керування системою та додатками, до мінімальної кількості довірених, авторизованих користувачів. 2. Використати процедури ідентифікації, аутентифікації та авторизації для службових програм, що забезпечують унікальну ідентифікацію особи, яка використовує службову програму. 3. Визначити та задокументувати рівні авторизації для використання службових програм. 4. Запровадити процедури авторизації для спеціального використання утилітарних програм. 5. Заборонити доступ до службових програм користувачам, які мають доступ до додатків у системах, де потрібен розподіл обов'язків. 6. Видалити або вимкнути усі непотрібні службові програми. 7. Логічно відокремити службові програми від прикладного програмного забезпечення. Де це можливо, відокремити мережеві комунікації для цих програм від трафіку додатків. 8. Обмежити доступність службових програм лише за необхідності, наприклад, під час санкціонованих змін. 9. Реєструвати всі випадки використання службових програм, щоб зберегти інформацію про те, хто і коли їх використовував.	1.Задокументовані рівні авторизації для використання службових програм. 2.Задокументований журнал усіх використань службових програм.		Невідповідність	0%	
8.19	Встановлення програмного забезпечення на операці	Було: 12.5.1, 12.6.2 Чи існує процес контролю за встановленням програмного забезпечення до операційних систем? Чи існують процеси для обмеження того, як користувачі встановлюють програмне забезпечення?	1. Встановити процедури та заходи для безпечного управління встановленням програмного забезпечення в операційних системах, враховуючи наступне: а) виконання оновлень операційного програмного забезпечення лише навченими адміністраторами за відповідним дозволом керівництва; б) забезпечення того, щоб на операційні системи встановлювався лише затверджений виконуваний код, а не код для розробки чи	1. Стандартний список програмного забезпечення. 2. Чорний список програмного забезпечення. 3. Встановлення		Невідповідність	0%	

	йні системи	Стало: 1. Чи існує процес контролю за встановленням програмного забезпечення в операційні системи? 2. Чи існують чіткі правила щодо того, які типи програмного забезпечення користувачі можуть встановлювати?	компілятори; c) встановлювати та оновлювати програмне забезпечення лише після всебічного та успішного тестування; d) оновлення всіх відповідних бібліотек вихідних текстів програм; e) використання системи контролю конфігурації для збереження контролю над усім операційним програмним забезпеченням, а також над системною документацією; f) визначення стратегії відкату перед впровадженням змін; g) ведення журналу аудиту всіх оновлень операційного програмного забезпечення; h) архівування старих версій програмного забезпечення разом з усією необхідною інформацією та параметрами, процедурами, деталями конфігурації та допоміжним програмним забезпеченням як резервний захід і до тих пір, поки програмне забезпечення необхідне для зчитування або обробки заархівованих даних. 2. Моніторинг та контроль програмного забезпечення та пакетів, що постачаються ззовні, з метою уникнення несанкціонованих змін, які можуть призвести до вразливостей у системі безпеки. 3. Підтримувати програмне забезпечення, що постачається постачальником, та програмне забезпечення з відкритим кодом на рівні, що підтримується постачальником або останньою відповідною версією, враховуючи ризики, пов'язані з використанням непідтримуваного або необслуговуваного програмного забезпечення. 4. Встановити контроль над фізичним або логічним доступом постачальників, коли вони беруть участь у встановленні або оновленні програмного забезпечення. Відстежуйте їхню діяльність та надавайте доступ лише у разі необхідності та за наявності відповідного дозволу. 5. Визначити та забезпечте дотримання суворих правил щодо того, яке програмне забезпечення можуть встановлювати користувачі. 6. Застосовувати принцип найменших привілеїв до встановлення програмного забезпечення в операційних системах. Визначити, які типи встановлення програмного забезпечення дозволені, а які заборонені. Надавайте ці привілеї на основі ролей користувачів.	програмного забезпечення				
8.20	Мережева безпека	БЕЗ ЗМІН: Чи існує процес управління мережею?	1. Впровадити засоби контролю для забезпечення безпеки інформації в мережі та захисту підключених послуг від несанкціонованого доступу, враховуючи наступні моменти: а) тип та рівень секретності інформації, яку може підтримувати мережа; б) встановлення відповідальності та процедур для управління мережевим обладнанням та пристроями; c) підтримання в актуальному стані документації, включаючи	1.Політика безпеки мережі. 2.Системи виявлення та запобігання вторгнень у мережу (IDS і IPS).		Невідповідність	0%	

			схеми мережі та конфігураційні файли пристроїв (наприклад, маршрутизаторів, комутаторів); d) відокремлення операційної відповідальності за мережі від операцій з ІКТ-системами, де це доречно; e) встановлення засобів контролю для захисту конфіденційності та цілісності даних, що передаються через загальнодоступні мережі, мережі третіх сторін або через бездротові мережі, а також для захисту підключених систем і додатків. Також можуть знадобитися додаткові засоби контролю для підтримки доступності мережевих сервісів та комп'ютерів, підключених до мережі; f) належне ведення журналів та моніторинг, що дозволяє реєструвати та виявляти дії, які можуть вплинути на інформаційну безпеку або мають відношення до неї (див. пункти 8.16 та 8.15) g) тісна координація діяльності з управління мережею як для оптимізації обслуговування організації, так і для забезпечення послідовного застосування засобів контролю в інфраструктурі обробки інформації; h) системи автентифікації в мережі; i) обмеження та фільтрація підключення систем до мережі (наприклад, за допомогою брандмауерів) j) виявлення, обмеження та аутентифікація підключення обладнання та пристроїв до мережі; k) посилення захисту мережевих пристроїв; l) відокремлення каналів мережевого адміністрування від іншого мережевого трафіку m) тимчасова ізоляція критично важливих підмереж (наприклад, за допомогою розвідних мостів), якщо мережа піддається атаці; n) відключення вразливих мережевих протоколів. 2. Застосовувати відповідні засоби контролю безпеки до використання віртуалізованих мереж, включаючи програмно-визначені мережі (SDN, SD-WAN). Віртуалізовані мережі можуть дозволити логічне розділення комунікації, що відбувається через фізичні мережі, що підвищує безпеку, особливо для систем і додатків, які використовують розподілені обчислення.	3.Брандмауери. 4.Сегментація мережі. 5.Топологія мережі.				
8.21	Безпека мережевих служб	Було: 13.1.2. 1. Чи застосовує організація підхід до управління ризиками, який ідентифікує всі мережеві послуги та угоди про надання послуг? 2. Чи передбачено забезпечення безпеки в угодах та контрактах з постачальниками послуг (внутрішніми	1. Визначити заходи безпеки, включаючи засоби захисту, рівні обслуговування та вимоги до послуг, необхідні для конкретних мережевих послуг, та забезпечити їх впровадження внутрішніми або зовнішніми постачальниками мережевих послуг. 2. Оцінити здатність постачальника мережевих послуг безпечно управляти узгодженими послугами та здійснювати регулярний моніторинг. Укладіть угоду про право на аудит між вашою організацією та провайдером. 3. Розглянути атестації третьої сторони, надані провайдерами	1.Політика безпеки мережі. 2.Системи виявлення та запобігання вторгнень у мережу (IDS і IPS). 3.Угода про		Невідповідність	0%	

		та зовнішніми). 3. Чи є обов'язковими SLA, пов'язані з безпекою? Стало : 1. Чи застосовує організація підхід до управління ризиками, який ідентифікує всі мережеві послуги. 2. Чи передбачено безпеку в угодах та контрактах з постачальниками послуг (внутрішніми та аутсорсинговими). 3. Чи є обов'язковими SLA, пов'язані з безпекою?	послуг, щоб переконатися, що вони дотримуються належних заходів безпеки. 4. Сформулювати та впровадьте правила користування мережами та мережевими послугами, які охоплюватимуть а) мережі та мережеві послуги, до яких дозволено доступ; б) вимоги до автентифікації для доступу до різних мережевих послуг с) процедури авторизації для визначення того, кому дозволено доступ до яких мереж і мережевих послуг г) управління мережею та технологічні засоби контролю і процедури захисту доступу до мережевих з'єднань і мережевих сервісів; е) засоби, що використовуються для доступу до мереж та мережевих послуг [наприклад, використання віртуальної приватної мережі (VPN) або бездротової мережі]; f) час, місцезнаходження та інші атрибути користувача під час доступу; g) моніторинг використання мережевих послуг. 5. Розглянути наступні особливості безпеки мережевих сервісів: а) технології, що застосовуються для забезпечення безпеки мережевих сервісів, такі як аутентифікація, шифрування та контроль мережевих з'єднань; б) технічні параметри, необхідні для безпечного з'єднання з мережевими службами відповідно до правил безпеки та мережевого з'єднання; с) кешування (наприклад, у мережі доставки контенту) та його параметри, які дозволяють користувачам обирати використання кешування відповідно до вимог продуктивності, доступності та конфіденційності; г) процедури використання мережевих послуг для обмеження доступу до мережевих послуг або додатків, де це необхідно.	рівень обслуговування(SLA) та контракти із постачальниками мережевих послуг.				
8.22	Розмеж ування мереж	БЕЗ ЗМІН: Чи забезпечує мережева топологія розмежування мереж для різних завдань?	1. Розділити великі мережі на окремі мережеві домени та ізолюйте їх від публічної мережі (Інтернету). Домени можуть бути визначені за рівнями довіри, критичності та чутливості, або узгоджені з організаційними підрозділами. Сегрегація може бути здійснена як за допомогою фізично різних мереж, так і за допомогою різних логічних мереж. 2. Чітко визначити периметр кожного домену. Якщо доступ між мережевими доменами дозволений, контролюйте його на периметрі за допомогою шлюзів, таких як брандмауери або фільтруючі маршрутизатори. 3. Провести оцінку вимог безпеки для кожного домену. Критерії поділу мережі на домени та дозволений доступ через шлюзи	1.Політика безпеки мережі. 2.Системи виявлення та запобігання вторгнень у мережу (IDS і IPS). 3.Брандмауери. 4.Сегментація мережі.		Невідповід ність	0%	

			мають ґрунтуватися на результатах цієї оцінки. 4. Забезпечити, щоб оцінка проводилася відповідно до політики контролю доступу, вимог до доступу, цінності та класифікації оброблюваної інформації, а також враховувала відносну вартість та вплив на продуктивність від впровадження відповідної технології шлюзу. 5. Розглянути бездротові мережі окремо через їх погано визначений мережевий периметр. Розглянути можливість регулювання радіопокриття для відокремлення бездротових мереж. 6. У чутливих середовищах розглянути весь бездротовий доступ як зовнішні з'єднання, відокремивши цей доступ від внутрішніх мереж, доки він не пройде через мережевий шлюз відповідно до мережевих засобів контролю, перш ніж надавати доступ до внутрішніх систем. 7. Забезпечити окрему мережу бездротового доступу для гостей, якщо персонал використовує лише контрольовані користувацькі кінцеві пристрої, що відповідають політиці організації. Переконайтеся, що WiFi для гостей має щонайменше такі ж обмеження, як і WiFi для персоналу, щоб утримати персонал від використання гостьового WiFi.	5.Топологія мережі.				
8.23	Веб-фільтрація	Чи існує процес контролю доступу до зовнішніх веб-сайтів?	1. Впровадити технології веб-фільтрації для блокування доступу до певних типів веб-сайтів, які, як відомо або підозрюється, містять шкідливе програмне забезпечення, фішинговий контент або незаконну інформацію. 2. Визначити типи веб-сайтів, до яких працівники повинні мати доступ, а до яких - ні. Розгляньте можливість блокування доступу до наступних типів веб-сайтів: а) веб-сайти, які мають функцію завантаження інформації, якщо це не дозволено з поважних ділових причин; б) відомі або підозрювані шкідливі веб-сайти (наприклад, ті, що поширюють шкідливе програмне забезпечення або фішинговий контент) с) командні та контрольні сервери; г) шкідливі веб-сайти, отримані з розвідки загроз; д) веб-сайти, що поширюють незаконний контент. 3. Встановити правила безпечного та належного використання онлайн-ресурсів. Ці правила повинні визначати будь-які обмеження на доступ до певних веб-сайтів або веб-додатків і регулярно оновлюватися. 4. Провести навчання для працівників щодо безпечного та належного використання онлайн-ресурсів, у тому числі перегляду веб-сторінок. Таке навчання має включати огляд правил	1. Чорний список веб-ресурсів. 2. Налаштування веб-фільтрації за допомогою інструменту безпеки кінцевих точок або програмного забезпечення для веб-фільтрації.		Невідповідність	0%	

			організації, процес висловлення занепокоєння щодо безпеки, а також процедуру винятків для доступу до обмежених веб-ресурсів з поважних ділових причин. 5. Навчити працівників не ігнорувати попередження браузера про те, що веб-сайт не є безпечним, навіть якщо браузер дозволяє користувачеві продовжити роботу.					
8.24	Застосування криптографії	Було: 10.1.1., 10.1.2 Чи існує політика щодо використання криптографічних засобів контролю? Чи існує політика, що регулює весь життєвий цикл криптографічних ключів? Стало: 1. Чи визначені правила для ефективного використання криптографії? 2. Чи встановлені процеси управління криптографічними ключами?	1. Розробити та впровадити політику щодо використання криптографії. Ця політика повинна визначати принципи захисту інформації та керувати використанням криптографічних методів, щоб уникнути неналежного або некоректного використання. 2. Визначити необхідний рівень захисту та класифікацію інформації і, відповідно, встановити тип, стійкість та якість необхідних криптографічних алгоритмів. 3. Впровадити криптографічний захист інформації на кінцевих пристроях мобільних користувачів або носіях інформації, а також інформації, що передається мережами. 4. Створити систему управління ключами, яка включає методи генерації та захисту криптографічних ключів, а також відновлення зашифрованої інформації у разі втрати, компрометації або пошкодження ключів. 5. Визначити ролі та обов'язки щодо впровадження правил криптографії та управління ключами (включаючи генерацію ключів). 6. Прийняти криптографічні алгоритми, стійкість шифрів, криптографічні рішення та практики використання, які схвалені або необхідні для використання в організації. 7. Розглянути вплив використання зашифрованої інформації на засоби контролю, які покладаються на перевірку контенту, наприклад, на виявлення шкідливого програмного забезпечення або фільтрацію контенту. 8. Оцінити та дотримуватися міжнародних правил та обмежень, які можуть застосовуватися до використання криптографічних методів, а також питань, пов'язаних з транскордонним потоком зашифрованої інформації. 9. Забезпечити, щоб угоди про рівень обслуговування або контракти із зовнішніми постачальниками криптографічних послуг (наприклад, із центром сертифікації) охоплювали питання відповідальності, надійності послуг та часу реагування на надання послуг. 10. Створити систему управління ключами, яка повинна базуватися на узгодженому наборі стандартів, процедур та безпечних методів для	1. Політика управління криптографічними ключами або політика шифрування.		Невідповідність	0%	

			а) генерації ключів для різних криптографічних систем та різних додатків б) видачі та отримання сертифікатів відкритих ключів c) розповсюдження ключів серед відповідних суб'єктів, включаючи способи активації ключів після їх отримання г) зберігання ключів, у тому числі способи отримання доступу до ключів авторизованими користувачами e) зміна або оновлення ключів, включаючи правила щодо того, коли змінювати ключі та як це робити; f) поводження зі скомпрометованими ключами; g) відкликання ключів, у тому числі як вилучати або деактивувати ключі [наприклад, коли ключі були скомпрометовані або коли користувач залишає організацію (у цьому випадку ключі також повинні бути заархівовані)]; h) відновлення втрачених або пошкоджених ключів; i) резервне копіювання або архівування ключів; j) знищення ключів; k) реєстрація та аудит дій, пов'язаних з управлінням ключами; l) встановлення дат активації та деактивації ключів таким чином, щоб ключі можна було використовувати лише протягом періоду часу, визначеного правилами організації щодо управління ключами; m) обробка юридичних запитів на доступ до криптографічних ключів (наприклад, зашифровану інформацію можуть вимагати надати в незашифрованому вигляді як доказ у судовій справі). 11. Забезпечити захист усіх криптографічних ключів від модифікації та втрати, захист секретних та особистих ключів від несанкціонованого використання та розголошення, а також фізичний захист обладнання, що використовується для генерації, зберігання та архівування ключів.					
8.25	Безпечний життєвий цикл розробки	Було: 14.2.1 1. Чи розробляє організація програмне забезпечення або системи? 2. Якщо так, то чи існують політики, що вимагають впровадження та оцінки засобів контролю безпеки? Стало: 1. Чи існують правила безпечної розробки програмного забезпечення та систем?	1. Встановити правила безпечної розробки програмного забезпечення та систем, враховуючи наступне: а) розмежування середовищ розробки, тестування та виробництва; б) настанови щодо безпеки в життєвому циклі розробки програмного забезпечення: 1) безпека в методології розробки програмного забезпечення; 2) керівні принципи безпечного кодування для кожної використовуваної мови програмування в) вимоги безпеки на етапі специфікації та проектування; г) контрольні точки безпеки в проєктах; е) системне тестування та тестування безпеки, таке як регресійне тестування, сканування коду та тести на проникнення;	1.Політика безпечної розробки. 2.Програмне забезпечення для статичного та динамічного аналізу безпеки додатків. 3.Аналіз композиції програмного забезпечення.		Невідповідність	0%	

			f) безпечні репозиторії для вихідного коду та конфігурації; g) безпека в управлінні версіями; h) необхідні знання та навчання з безпеки додатків; i) спроможність розробників запобігати, знаходити та виправляти вразливості; к) ліцензійні вимоги та альтернативи для забезпечення економічно ефективних рішень та уникнення проблем з ліцензуванням у майбутньому. 2. Якщо розробка передається на аутсорсинг, переконайтися, що постачальник дотримується правил організації щодо безпечної розробки.					
8.26	Вимоги до безпеки додатків	Було: 14.1.2., 14.1.3 Чи програми, які передають інформацію через публічні мережі, належним чином захищають інформацію від шахрайських дій, суперечок за контрактом, несанкціонованого розкриття та несанкціонованої модифікації? Чи існують засоби контролю для запобігання неповної передачі, неправильної маршрутизації, несанкціонованої зміни повідомлень, несанкціонованого розкриття, несанкціонованого дублювання повідомлень або атак на повторне відтворення? Стало: 1. Чи чітко визначені вимоги до інформаційної безпеки при розробці або придбанні додатків? 2. Чи затверджені ці вимоги керівництвом? 3. Чи є ці вимоги предметом процесу управління, який включає оцінку ризиків?	1. Провести оцінку ризиків, щоб визначити та конкретизувати вимоги до безпеки додатків. 2. Вимоги до безпеки додатків повинні включати, залежно від обставин a) рівень довіри до ідентичності суб'єктів (наприклад, через автентифікацію); b) визначення типу інформації та рівня секретності, що має оброблятися додатком c) необхідність розмежування доступу та рівнів доступу до даних і функцій у додатку г) стійкість до зловмисних атак або ненавмисних збоїв [наприклад, захист від переповнення буфера або ін'єкцій мови структурованих запитів (SQL)]; e) правові, законодавчі та регуляторні вимоги в юрисдикції, де транзакція генерується, обробляється, завершується або зберігається; f) потреба в конфіденційності, пов'язана з усіма залученими сторонами; g) вимоги щодо захисту будь-якої конфіденційної інформації; h) захист даних під час обробки, передачі та зберігання; i) необхідність надійного шифрування комунікацій між усіма залученими сторонами; j) вхідний контроль, включаючи перевірку цілісності та валідацію вхідних даних; k) автоматизовані засоби контролю (наприклад, ліміти дозволів або подвійні дозволи) l) вихідний контроль, який також враховує, хто може отримати доступ до вихідних даних та їх авторизацію; m) обмеження щодо вмісту полів "вільного тексту", оскільки це може призвести до неконтрольованого зберігання конфіденційних даних (наприклад, персональних даних); n) вимоги, що випливають з бізнес-процесів, такі як реєстрація та	1. Політика безпечної розробки.		Невідповідність	0%	

			моніторинг транзакцій, вимоги щодо неспростування; o) вимоги, передбачені іншими засобами контролю безпеки (наприклад, інтерфейси для реєстрації та моніторингу або системи виявлення витоку даних); p) обробка повідомлень про помилки. 3. Для додатків, що пропонують транзакційні послуги між організацією та партнером, при визначенні вимог до інформаційної безпеки слід враховувати наступне a) рівень довіри, необхідний кожній стороні до заявленої ідентичності одна одної; б) рівень довіри, необхідний для забезпечення цілісності інформації, якою обмінюються або обробляють, та механізми виявлення відсутності цілісності (наприклад, циклічна перевірка на надмірність, хешування, цифрові підписи) в) процеси авторизації, пов'язані з тим, хто може затверджувати зміст, випускати або підписувати ключові транзакційні документи; г) конфіденційність, цілісність, докази відправлення та отримання ключових документів і неможливість відмови від них (наприклад, контракти, пов'язані з тендерними та контрактними процесами); e) конфіденційність та цілісність будь-яких транзакцій (наприклад, замовлень, адрес доставки та підтвердження квитанцій); f) вимоги щодо того, як довго зберігати конфіденційність транзакції; g) страхування та інші договірні вимоги. 4. Для додатків, що передбачають електронне замовлення та оплату, враховувати вимоги щодо збереження конфіденційності та цілісності інформації про замовлення, перевірки платіжної інформації, запобігання втраті або дублюванню інформації про транзакцію та зберігання деталей транзакції.					
8.27	Безпечна системна архітектура та інженерні принципи	БЕЗ ЗМІН: Чи має організація задокументовані принципи щодо того, як мають бути розроблені системи для забезпечення безпеки?	1. Встановити та задокументувати безпечні інженерні принципи інжинірингу інформаційних систем. 2. Переконатися, що безпека врахована на всіх рівнях архітектури (бізнес, дані, додатки та технології). 3. Впровадити процес аналізу нових технологій на предмет ризиків для безпеки та перевірки дизайну на відповідність відомим моделям атак. 4. Впровадити принципи "нульової довіри", наприклад, припустити, що інформаційні системи організації вже зламані, і, таким чином, не покладатися виключно на захист мережевого периметру. Застосовувати підхід "ніколи не довіряй і завжди перевіряй" для доступу до інформаційних систем. 5. Якщо розробка передається на аутсорсинг, переконатися, що встановлені принципи інженерії безпеки застосовуються в	1. Політика безпечної розробки. 2. Договори/угоди між організацією та постачальниками послуг аутсорсингу.		Невідповідність	0%	

			контрактах та інших обов'язкових угодах між організацією та постачальником. Переконатися, що практики інженерії безпеки постачальників відповідають потребам організації. 6. Впровадити план регулярного перегляду принципів інженерії безпеки та встановлених інженерних процедур.					
8.28	Безпечне кодування	Чи існують загальноорганізаційні принципи безпечного кодування?	1. Визначити загальноорганізаційні процеси безпечного кодування та встановіть безпечну базову лінію. Поширити ці процеси на сторонні та відкриті програмні компоненти. 2. Відстежувати реальні загрози, а також актуальні поради та інформацію про вразливості програмного забезпечення. 3. Застосовувати принципи безпечного кодування до діяльності з розробки як всередині організації, так і для продуктів та послуг, які організація надає іншим. 4. Впроваджувати практики безпечного кодування, специфічні для мов та методів програмування, що використовуються. Використовувати структуровані методи програмування та забороняти використання небезпечних методів проектування (наприклад, жорстко закодовані паролі). 5. Налагодити процес тестування під час та після розробки, а також статичне тестування безпеки додатків (SAST) для виявлення вразливостей програмного забезпечення. До того, як програмне забезпечення буде введено в експлуатацію, оцініть поверхню атаки та проведіть аналіз поширених помилок програмування, переконавшись, що вони були усунені. 6. Впровадити процес регулярного перегляду та підтримки коду після введення його в експлуатацію або у випадку використання зовнішніх інструментів та бібліотек, або коли програмний пакет потребує модифікації.	1. Політика безпечної розробки. 2. Договори/угоди між організацією та постачальниками послуг аутсорсингу.		Невідповідність	0%	
8.29	Тестування безпеки під час розробки та приймання	Було: 14.2.8, 14.2.9 Чи розробляються системи або додатки, які тестуються на безпеку як частина процесу розробки? Чи існує встановлений процес прийняття нових систем/додатків або їх оновлень у промислову експлуатацію? Існує: 1. Чи проводиться тестування безпеки систем або додатків, що розробляються, як частина життєвого циклу розробки? 2. Чи існує встановлений процес	1. Встановити процеси для проведення тестування безпеки протягом усього життєвого циклу розробки. Ці процеси повинні бути невід'ємною частиною загальної стратегії тестування систем або компонентів. 2. Розробити набір вимог до тестування. 3. Розробити комплексний план тестування, який включає графік заходів і тестів, вхідні дані та очікувані результати за різних умов, критерії оцінки та критерії прийняття рішень щодо подальших дій. 4. Впровадити автоматизовані інструменти, такі як інструменти аналізу коду або сканери вразливостей, для виявлення та перевірки усунення дефектів, пов'язаних з безпекою. 5. Проводити внутрішнє та незалежне приймальне тестування. 6. Для аутсорсингових розробок та придбаних компонентів укладайте контракти, які враховують виявлені вимоги до безпеки. Продукти та послуги слід оцінювати за цими критеріями перед	1.Політика безпечної розробки. 2.Програмне забезпечення для статичного та динамічного аналізу безпеки додатків. 3.Аналіз композиції програмного забезпечення.		Невідповідність	0%	

		прийняття нових систем/додатків або їх оновлень у промислову експлуатацію?	придбанням. 7. Розглянути можливість створення декількох тестових середовищ для різних видів тестування, таких як функціональне тестування та тестування продуктивності. Ці середовища можуть бути віртуальними та індивідуально налаштованими для імітації різних операційних середовищ. 8. Розглянути необхідність тестування та моніторингу тестових середовищ, інструментів та технологій для забезпечення ефективного тестування. Ті ж самі міркування стосуються моніторингу систем моніторингу, розгорнутих у середовищі розробки, тестування та виробництва.					
8.30	Аутсорсингова розробка	БЕЗ ЗМІН: 1. Якщо розробка була передана на аутсорсинг, чи здійснюється нагляд та перевірка? 2. Чи підлягає зовнішній код перевірці безпеки перед розгортанням?	1. Чітко сформулювати та узгодити вимоги та очікування щодо аутсорсингової розробки системи. Це включає в себе визначення очікувань щодо безпечного дизайну, кодування та тестування. 2. Налагодити процес постійного моніторингу та аналізу виконання робіт, що передаються на аутсорсинг, щоб переконатися, що вони відповідають очікуванням організації.	1.Договори/угоди між організацією та постачальниками послуг аутсорсингу.		Невідповідність	0%	
8.31	Розділення середовищ розробки, тестування та виробництва	БУЛО: 12.1.4, 14.2.6 Чи забезпечує організація розділення середовищ розробки, тестування та експлуатації? 1. Чи створено безпечне середовище розробки? 2. Чи всі проекти використовують безпечне середовище розробки належним чином протягом життєвого циклу розробки системи? Стало: 1. Чи забезпечує організація розділення середовищ розробки, тестування та виробництва? 2. ???	1. Визначити процедури щодо розділення середовищ розробки, тестування та виробництва. Переконайтеся, що вони включають правила та протоколи авторизації для розгортання програмного забезпечення. 2. Переконайтися, що середовища розробки, тестування та виробництва належним чином розділені. Вони можуть бути в окремих фізичних або віртуальних просторах. 3. Визначити, задокументуйте та впровадьте правила та авторизацію для розгортання програмного забезпечення від стадії розробки до стадії виробництва. 4. Визначити та задокументувати протоколи для тестування змін у виробничих системах та додатках у тестовому або постановочному середовищі перед тим, як застосовувати їх у виробничих системах. 5. Визначити, які інструменти розробки, такі як компілятори та редактори, необхідні у виробничому середовищі. Впровадити обмеження для запобігання доступу до цих інструментів, коли вони не потрібні. 6. Створити і задокументувати протоколи поводження з конфіденційною інформацією. Це включає правила, що забороняють копіювання такої інформації в середовища тестування та розробки, якщо вони не мають еквівалентних засобів контролю безпеки. 7. Встановити та підтримувати заходи безпеки для середовищ тестування та розробки, включаючи регулярне виправлення та оновлення інструментів, безпечну конфігурацію системи, контрольований доступ, моніторинг змін, моніторинг безпечного	1.Політика безпечної розробки.		Невідповідність	0%	

			середовища та регулярне резервне копіювання. 8. Впровадити систему розподілу обов'язків, щоб одна особа не могла вносити зміни як у середовище розробки, так і у виробниче середовище без попередньої перевірки та затвердження. 9. У виняткових випадках, коли зміни в обох середовищах можуть бути необхідними, розробити детальні протоколи реєстрації та моніторингу в реальному часі для швидкого виявлення несанкціонованих змін та реагування на них.					
8.32	Керування змінами	Було: 12.1.2, 14.2.2., 14.2.3, 14.2.4 Чи існує контрольований процес управління змінами? Чи існує формальний процес контролю змін? Чи існує процес, що забезпечує проведення технічного огляду при зміні операційних платформ? Чи існує політика, яка визначає, коли і як можна змінювати або модифікувати програмні пакети? Стало: 1. Чи існують контрольовані процедури управління змінами? 2. Чи задокументовані контрольовані процедури управління змінами?	1. Розробити та задокументувати процедури управління змінами. 2. Забезпечити ретельне документування всіх процедур управління змінами з чітким поясненням того, як вони підтримують конфіденційність, цілісність та доступність інформації протягом усього життєвого циклу розробки системи. 3. Інтегрувати процедури контролю змін для інфраструктури ІКТ та програмного забезпеченням , де це можливо. 4. Переконатися, що процедури контролю за змінами включають a) планування та оцінку потенційного впливу змін з урахуванням усіх залежностей; б) затвердження змін c) інформування про зміни відповідних зацікавлених сторін d) тестування та прийняття тестів змін (див. 8.29) e) впровадження змін, включаючи плани розгортання; f) міркування щодо надзвичайних ситуацій та непередбачуваних обставин, включаючи резервні процедури; g) ведення записів змін, які включають все вищезазначене; h) забезпечення внесення змін до експлуатаційної документації (див. 5.37) та користувацьких процедур за необхідності для підтримання їх у належному стані; i) забезпечення внесення змін до планів забезпечення безперервності ІКТ та процедур реагування і відновлення (див. 5.30) за необхідності для підтримання їх у належному стані.	1.Політика управління змінами. 2.Програмне забезпечення для управління змінами.		Невідповідність	0%	
8.33	Інформація про тестування	Було: 14.2.3 1. Чи існує процес відбору даних для тестування? 2. Чи захищені тестові дані належним чином? Належним чином: 1. Чи існує процес відбору тестової інформації? 2. Чи належним чином захищена тестова інформація?	1. Визначити процес вибору тестової інформації, який забезпечить надійні результати тестування, захищаючи при цьому конфіденційність операційної інформації. Переконайтеся, що цей процес чітко запобігає копіюванню конфіденційної інформації, наприклад, інформації, що ідентифікує особу, в середовище розробки та тестування. 2. Переконатися, що до тестових середовищ застосовуються ті самі процедури контролю доступу, що й до робочих середовищ. 3. Впровадити процес отримання окремого дозволу кожного разу, коли операційні дані копіюються в тестове середовище. 4. Впровадити систему реєстрації для моніторингу та запису копіювання та використання оперативної інформації в тестових	1.Політика безпечної розробки.		Невідповідність	0%	

			середовищах, забезпечуючи чіткий аудиторський слід. 5. Застосовувати заходи для захисту конфіденційної інформації, якщо вона використовується для тестування, наприклад, видалення або маскування даних. 6. Розробити та впровадити процес належного видалення операційних даних з тестового середовища одразу після завершення тестування. 7. Створити безпечні системи зберігання тестової інформації, щоб запобігти її підробці та забезпечити її використання лише для цілей тестування.					
8.34	Захист інформаційних систем під час аудиторського тестування	БЕЗ ЗМІН: 1. Чи підлягають аудиту системи ІС? 2. Чи забезпечує процес аудиту мінімізацію перебоїв у роботі?	1. Запровадити формальний процес узгодження аудиторських запитів на доступ до систем та даних з відповідним керівництвом організації. 2. Запровадити процес узгодження та контролю обсягу технічних аудиторських тестів. 3. Впровадити процес, який гарантує, що аудиторські тести обмежуються доступом до програмного забезпечення та даних лише в режимі читання. У ситуаціях, коли доступ тільки для читання недоступний, розробити інструкції для проведення тестів досвідченим адміністратором з необхідними правами доступу. 4. Встановити політику перевірки та підтвердження вимог безпеки пристроїв, що використовуються для доступу до систем (наприклад, перевірка актуальності антивірусу, наявність виправлень тощо), перш ніж надавати доступ. 5. Розробити процедуру, яка обмежує доступ до ізольованих копій системних файлів, дозволяє їх видалення після завершення аудиту та забезпечує відповідний захист, якщо ці файли необхідно зберігати відповідно до вимог аудиторської документації. 6. Розробити процедуру для визначення та узгодження спеціальних або додаткових заходів з обробки даних, таких як запуск інструментів аудиту. 7. Створити настанови для забезпечення того, щоб аудиторські тести, які можуть вплинути на доступність системи, проводилися в неробочий час, щоб мінімізувати збої в роботі. 8. Впровадити систему моніторингу та реєстрації всіх доступів для цілей аудиту та тестування.	1.Процедура внутрішнього аудиту. 2.Звіти з пентестів.		Невідповідність	0%	

ДОДАТОК Г. ШАБЛОН ДЛЯ ОЦІНКИ РИЗИКІВ

ID Ризику	Актив/Процес	Опис Ризику	Власник Ризику	Імовірність	Вплив	Рівень Ризику	Варіант Обробки Ризику	Відповідний ISO 27001 Контроль	Номер відповідного контролю ISO 27001	Відповідний ISO 27001 Домен	Контроль	Статус	Залишкова імовірність	Залишковий вплив	Залишковий рівень ризику

ДОДАТОК Д. ШАБЛОН ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика Інформаційної Безпеки [Назва_організації]

Дата затвердження: дд.мм.рррр

МЕТА ПОЛІТИКИ

Дана Політика має на меті сформулювати обґрунтування та заходи щодо захисту конфіденційної інформації, забезпечити відповідність застосовним правовим і нормативним вимогам і забезпечити досягнення бізнес-цілей організації. В умовах дедалі більшої цифровізації ця Політика направлена на зміцнення стійкості Компанії проти потенційних загроз і сприяє розвитку культури безпеки.

Впроваджуючи цю політику, Компанія може зменшити ризики, зміцнити довіру зацікавлених сторін, підвищити операційну ефективність і, зрештою, отримати конкурентну перевагу на ринку.

1. Вступні положення

1.1. Політика інформаційної безпеки («Політика») поширюється на [Назва компанії] («Компанія») та її директорів, посадових осіб, штатних і зовнішніх працівників, підрядників і консультантів. Очікується, що персонал буде діяти, щоб зміцнити репутацію Компанії через чесність, порядність і надійність.

1.2. Політика поширюється на всі країни, де Компанія працює або веде бізнес. Однак, якщо закони цих країн вимагають вищих стандартів, пріоритет матиме місцевий стандарт.

1.3. Ця Політика поширюється на всі відносини з будь-якими контрагентами, такими як потенційні та існуючі клієнти та сторонні постачальники послуг, з якими Компанія може мати справу.

1.4. Якщо Політика не стосується конкретного питання, необхідно звернутися до [назва відділу], відповідального за нагляд за дотриманням кібербезпеки та інформаційної безпеки, щоб забезпечити дотримання всіх відповідних норм і вказівок.

1.5. Цю Політику було схвалено на засіданні Ради директорів [Дата]. Рада затверджує будь-які наступні зміни на своїх засіданнях.

1.6. Компанія переглядає та переглядає Політику не рідше одного разу на рік. Компанія може переглядати Політику частіше на свій розсуд.

1.7. Переглянуту Політику буде представлено Раді директорів для затвердження на щорічних зборах.

2. Корпоративне управління

2.1. Інформаційна безпека вимагає як функції управління інформаційними ризиками, так і функції безпеки інформаційних технологій.

2.2. Компанія призначає менеджера з безпеки відповідальним за обидві функції, гарантуючи, що:

2.2.1. міркування, пов’язані з ризиками інформаційних активів та окремих інформаційних систем, включаючи рішення щодо авторизації, розглядаються з огляду на загальні стратегічні цілі та завдання виконання його основних місій та бізнес-функцій;

2.2.2. управління інформаційними активами та ризиками безпеки, пов’язаними з інформаційною системою, є послідовним, відображає толерантність до ризику та розглядається разом з іншими ризиками для забезпечення успіху місії/бізнесу.

2.3. Менеджер із безпеки несе повну відповідальність за моніторинг і забезпечення дотримання Політики. Менеджер із безпеки несе відповідальність за розробку та виконання дій із зменшення наслідків у разі виникнення проблем.

2.4. Політика компанії передбачає захист інформації від втрати:

2.4.1. конфіденційності – інформація буде доступна лише уповноваженим особам;

2.4.2. цілісності – збережеться точність і повнота інформації;

2.4.3. доступність – інформація буде доступна для авторизованих користувачів і процесів, коли це буде потрібно.

3. Ролі і обов’язки

3.1. **Бізнес-команда відповідає за наступне:**

3.1.1. Оцінку та затвердження ризиків від імені Компанії;

3.1.2. Визначення цілей та обов'язків, пов'язаних з інформаційною безпекою, та включення їх у відповідні процедури;

3.1.3. Демонстрація відповідальності за безпеку шляхом надання чітких вказівок та виділення відповідних ресурсів;

3.1.4. Сприяння підвищенню обізнаності про найкращі методики інформаційної безпеки серед працівників та підрядників;;

3.1.5. Впровадження процесу ідентифікації, обробки, використання, передачі та знищення інформаційних активів відповідно до класифікації та категоризації;

3.1.6. Визначення власників інформації, зберігаючи за собою кінцеву відповідальність за конфіденційність, цілісність та доступність даних;

3.1.7. Реагування на інциденти, пов'язані з безпекою;

3.1.8. Дотримання вимог щодо розкриття інформації у випадку порушення конфіденційності приватної інформації;

3.1.9. Дотримання конкретних законодавчих та нормативних зобов'язань щодо інформаційної безпеки;

3.1.10. Доведення вимог політики та пов'язаних з нею стандартів, включаючи наслідки їх недотримання, до відома працівників та третіх осіб, а також включення питань дотримання вимог у контрактах з третіми особами.

3.2. **Керівник відділу безпеки несе відповідальність за:**

3.2.1. Підтримання обізнаності з бізнес-функціями та вимогами;

3.2.2. Підтримання належного рівня поточних знань та навичок у сфері інформаційної безпеки;

3.2.3. Забезпечення однакового застосування політик та інструкцій з інформаційної безпеки;
3.2.4. Оцінювання дотримання політик інформаційної безпеки та нормативно-правових вимог, пов'язаних з інформаційною безпекою;
3.2.5. Аналіз та розуміння ризиків інформаційної безпеки та відповідних методів управління ними;
3.2.6. Забезпечення врахування міркувань архітектури безпеки;
3.2.7. Надання рекомендацій з питань безпеки під час закупівлі продуктів та послуг;
3.2.8. Піднімати питання безпеки, які не вирішуються належним чином, дотримуючись відповідних процедур звітності та ескалації;
3.2.9. Розповсюдження інформації про загрози серед відповідних зацікавлених сторін;
3.2.10. Участь у реагуванні на потенційні інциденти безпеки;
3.2.11. Впровадження процесу визначення класифікації та категоризації інформації на основі рекомендованих галузевих практик;
3.2.12. Участь у розробці політик та стандартів, що відображають потреби Компанії; та
3.2.13. Сприяння підвищенню обізнаності з питань інформаційної безпеки в межах всієї Компанії.

3.3. **Юридичний відділ відповідає за:**
3.3.1. Моніторинг та забезпечення дотримання цієї Політики;
3.3.2. Розробку та реалізацію заходів щодо пом'якшення наслідків у разі виникнення проблем.
3.3.3. Інформування про законодавчі та регуляторні вимоги та їх виконання.

3.4. **Технічний відділ (Системний адміністратор безпеки, DevOps інженери) відповідають за наступне:**
3.4.1. Забезпечення безпеки шляхом надання чітких вказівок та врахування засобів контролю безпеки в інфраструктурі обробки даних та обчислювальних мережах, які підтримують власників інформації;
3.4.2. Надання ресурсів, необхідних для підтримки рівня контролю інформаційної безпеки, що відповідає цій Політиці;
3.4.3. Ідентифікація та впровадження всіх процесів, політик та засобів контролю відповідно до вимог безпеки, визначених бізнесом та цією Політикою;
3.4.4. Впровадження належного контролю за інформацією, якою володіють на основі грифів секретності;
3.4.5. Забезпечення навчання відповідного технічного персоналу щодо безпечних методів роботи (наприклад, безпечне кодування, безпечна конфігурація);
3.4.6. Сприяння участі працівників служби інформаційної безпеки та технічного персоналу в захисті інформаційних активів, а також у визначенні, виборі та

впровадженні належних та економічно ефективних засобів і процедур контролю та забезпечення безпеки; та

3.4.7. Впровадження планів безперервності бізнесу та аварійного відновлення.

3.5. **Працівники несуть відповідальність за наступне:**

3.5.1. Розуміння базових засобів контролю інформаційної безпеки, необхідних для захисту конфіденційності, цілісності та доступності довіреної інформації;

3.5.2. Захищати інформацію та ресурси від несанкціонованого використання або розголошення;

3.5.3. Захист особистої, приватної та конфіденційної інформації від несанкціонованого використання або розголошення;

3.5.4. Повідомляти про підозри щодо інцидентів або слабких місць у системі інформаційної безпеки відповідному керівнику та Адміністратору системної безпеки.

3.6. Розподіл обов'язків та сфер відповідальності повинен бути впроваджений там, де це доречно, щоб зменшити ризик випадкового або навмисного неправомірного використання системи.

3.6.1. Якщо розподіл обов'язків не є технічно можливим, необхідно впровадити інші компенсаційні засоби контролю, такі як моніторинг діяльності, аудиторські записи та нагляд з боку керівництва.

3.6.2. Аудит та затвердження засобів контролю безпеки завжди повинні залишатися незалежними та відокремленими від реалізації засобів контролю безпеки.

4. Управління ризиками

4.1. Усі системи та процеси, які сприяють бізнес операціям, повинні належним чином управлятися з точки зору інформаційних ризиків і повинні проходити оцінку інформаційних ризиків принаймні раз на рік відповідно до Політики управління ризиками.

4.2. Оцінку ризиків інформаційної безпеки необхідно проводити для нових ініціатив, впровадження нових технологій, значних змін операційного середовища або при виявленні критичних вразливостей.

4.3. Результати оцінки ризиків, а також рішення, прийняті на основі цих результатів, повинні реєструватися та зберігатися.

5. Класифікація інформації

5.1. У наступній таблиці наведено стислий опис рівнів класифікації інформації, прийнятих у Компанії.

5.2. Інформація може змінювати ступінь секретності протягом свого існування або у зв'язку з її обсягом.

Класифікаційний рівень	Приклади
Публічний	● Статут компанії та інша інформація, що міститься в офіційних відкритих джерелах. ● інформація у всіх встановлених формах державної звітності. ● інформація про сплату податків та інших обов'язкових платежів. ● маркетингові матеріали, брошури та реклама, що широко розповсюджуються. ● інформація, що знаходиться у відкритому доступі, зокрема на загальнодоступному веб-сайті. ● номери телефонів та адреси офісів Товариства. ● оголошення про вакансії. ● матеріали для ЗМІ, прес-релізи, презентації.
Внутрішній / Тільки для внутрішнього використання	● внутрішні розсилки. ● внутрішні оголошення про вакансії. ● навчальні матеріали. ● внутрішні політики та процедури, робочі інструкції, керівництва, посібники для користувачів тощо ● внутрішні номери телефонів та каталоги електронної пошти. ● загальна стратегія компанії. ● опис бізнес-процесів. ● методології розвитку. ● загальні плани розвитку компанії. ● персональні дані працівників Компанії та підрядників, які надали згоду на обробку цих даних.
Конфіденційний	● інформація, розкрита клієнтами Товариства або оброблена від імені клієнтів Товариства, якщо тільки відповідний клієнт письмово не заявив про протилежне. ● договори, протоколи зустрічей, попередні домовленості, будь-які односторонні, двосторонні або багатосторонні акти, як підписані, так і підготовлені, які стосуються Компанії, її працівників та підрядників. ● комерційна таємниця, плани щодо продуктів або послуг, списки постачальників. ● розміри та форми оплати праці, премії, винагороди за виконані роботи та надані послуги, інші матеріальні та

	грошові компенсації працівникам та підрядникам Товариства. ● дати та форми отримання Товариством будь-яких сум та будь-яких платежів. ● звіти, що містять фінансові показники. ● маркетингові стратегії та плани. ● розмір бюджету, заплановані витрати, прогнози продажів, бізнес-плани та результати діяльності, що стосуються минулої, теперішньої або майбутньої господарської діяльності Товариства, а також його дочірніх, залежних та афілійованих товариств. ● звіти та пропозиції, плани організаційних змін. ● будь-яка інформація, пов'язана з виробництвом: розміри, потужність, кількість і тип обладнання, інструментів, деталей; технологія виробництва, технологічні карти, виробничий процес, описи, специфікації, технічні завдання, нормування робіт тощо ● технічні завдання, специфікації, зразки, схеми, звіти, дані, ноу-хау, незавершене виробництво, проекти, креслення, фотографії, засоби розробки, специфікації, комп'ютерні програми, вихідний код, об'єктний код, блок-схеми, бази даних та будь-яка інша технічна документація, створена Компанією, а також інтелектуальна власність та інші результати розробки ● логіни та паролі, коди доступу до будь-якого компоненту інфраструктури або облікового запису користувача, який адмініструється або фінансується Компанією. ● інформація про топологію, пропускну здатність локальних мереж, Інтернету та провайдерів Компанії. ● інформацію про заходи безпеки та контроль в межах Компанії. ● інформація про події та інциденти у сфері інформаційної безпеки. ● інформація про проведені аудити та тестування інформаційних систем Товариства, їх результати та виявлені вразливості. ● зміст зустрічей, питання, що розглядалися на них, результати зустрічей з працівниками та підрядниками Товариства. ● персональні дані, включаючи (i) персональні дані працівників та підрядників Товариства; (ii) персональні дані

	клієнтів Товариства та (iii) інші персональні дані, які перебувають у володінні або розпорядженні Товариства.

6. Управління активами

6.1. Компанія повинна забезпечити ідентифікацію активів, пов'язаних з інформацією та засобами обробки інформації (далі - інформаційні активи), а також складання та ведення інвентаризації цих активів.

6.2. Інвентаризація повинна включати інформацію про наступні активи компанії:

6.2.1. інформаційні системи та сервіси

6.2.2. апаратні активи

6.2.3. інфраструктурні активи

6.2.4. інші активи, які компанія вважає важливими

6.3. Для всіх активів повинні бути визначені власники, які несуть відповідальність за утримання та захист своїх активів відповідно до Політики управління активами.

6.4. **Всі інформаційні активи** повинні бути класифіковані відповідно до прийнятої в компанії схеми класифікації. Кожному активу повинен бути присвоєний класифікаційний гриф, що відображає найвищий рівень чутливості інформації, яка зберігається або обробляється відповідним активом. Класифікація вказує на відповідні вимоги до поводження з ними.

7. Управління доступом

7.1. Доступ до всієї інформації повинен контролюватися і визначатися вимогами Компанії, включаючи цю Політику. Доступ буде надано або організовано для користувачів відповідно до їхньої ролі та класифікації інформації лише на тому рівні, який дозволить їм виконувати свої обов'язки.

7.2. Для доступу до всіх інформаційних систем та послуг підтримується офіційний процес реєстрації та скасування реєстрації користувачів. Це включає обов'язкові методи автентифікації, що базуються на чутливості інформації, до якої надається доступ, та включають в себе розгляд багатьох факторів, за необхідності.

7.3. Для користувачів з підвищеними привілеями повинні бути впроваджені спеціальні засоби контролю, щоб зменшити ризик недбалого або навмисного зловживання системою. Розподіл обов'язків повинен бути реалізований там, де це практично можливо.

7.4. Доступ до систем повинен надаватися за допомогою індивідуально призначених унікальних ідентифікаторів або ідентифікаторів користувачів, за винятком випадків, зазначених у Політиці управління доступом.

7.5. З кожним ідентифікатором користувача повинен бути пов'язаний маркер автентифікації (наприклад, пароль, ключ-брелок, біометрія) для перевірки ідентичності особи або системи, що запитує доступ.

7.6. Повинні застосовуватися автоматизовані методи та засоби контролю для блокування сеансу і вимагати автентифікації або повторної автентифікації після періоду бездіяльності в системах, які вимагають автентифікації. Під час блокування сеансу на екрані повинна відображатися загальнодоступна інформація (наприклад, заставка, порожній екран, годинник).

7.7. Повинні використовуватися автоматизовані методи та засоби контролю для завершення сеансу при виконанні певних умов, визначених у Політиці розмежування доступу.

7.8. Токени, що використовуються для аутентифікації особи або процесу, повинні розглядатися як конфіденційні і захищатися відповідним чином.

7.9. Токени не повинні зберігатися на папері, в електронних файлах, на портативних пристроях або в браузерах, якщо тільки вони не зберігаються надійно і не схвалені Компанією (наприклад, у сховищі паролів).

7.10. Власники інформації несуть відповідальність за визначення доступу до захищених ресурсів у межах свого домену та відповідних привілеїв доступу (наприклад, читання, оновлення).

7.11. Привілеї доступу повинні надаватися відповідно до посадових обов'язків користувача, обмежуючись мінімумом, необхідним для виконання поставлених завдань (тобто, найменшим привілеєм).

7.12. Користувачі привілейованих облікових записів повинні використовувати окремий непривілейований обліковий запис для звичайних ділових операцій (наприклад, доступ до Інтернету, електронна пошта).

7.13. Усі віддалені з'єднання повинні здійснюватися через керовані точки входу та перевірятися Компанією.

7.14. Дозвіл на віддалену роботу має бути наданий керівництвом, а методи, що забезпечують належний захист даних у віддаленому середовищі, мають бути доведені до відома особи до надання їй віддаленого доступу.

8. Шифрування

8.1. З метою зменшення ризику розкриття або несанкціонованого доступу до конфіденційної інформації Компанії шляхом перехоплення, втрати або крадіжки інформації чи обладнання, Компанія, її працівники та підрядники повинні розгорнути відповідні засоби криптографічного захисту разом з процедурами управління відповідними ключами шифрування відповідно до Політики шифрування.

8.2. Для шифрування інформації в стані спокою та під час передачі слід використовувати загальноприйняті міжнародні стійкі криптографічні стандарти та алгоритми.

8.3. Внутрішня та конфіденційна інформація Товариства повинна переважно створюватися та зберігатися в авторизованих інформаційних системах, що перебувають в управлінні Товариства.

8.4. Однак, коли така інформація передається за межі авторизованої системи, вона повинна бути зашифрована під час передачі. Шифрування під час передачі може включати шифрування файлу, надісланого електронною поштою, шифрування портативного жорсткого диска, який використовується для передачі інформації, або використання зашифрованих протоколів передачі, таких як TLS.

8.5. Там, де це вважається обґрунтованим, і актив Компанії здатний шифрувати дані на пристрої, необхідно застосовувати шифрування на пристрої. Для оцінки ризиків, пов'язаних з використанням активу, і прийняття рішення про застосування криптографічного захисту може бути проведена оцінка ризиків.

9. Безпека систем

9.1. Системи, включаючи сервери, платформи, мережі, засоби зв'язку, бази даних і програмне забезпечення, повинні відповідати наступним вимогам:

9.1.1. На окрему особу або групу осіб повинна бути покладена відповідальність за обслуговування та адміністрування будь-якої системи, розгорнутої від імені Компанії, з централізованим веденням списку призначених осіб або груп.

9.1.2. Міркування безпеки повинні бути задокументовані при створенні або модифікації системи.

9.1.3. Усі системи повинні розроблятися, підтримуватися та виводитися з експлуатації відповідно до життєвого циклу розробки безпечної системи (SSDLC).

9.1.4. Кожна система повинна мати засоби контролю відповідно до класифікації будь-яких даних, що зберігаються або передаються через систему.

9.1.5. Усі системні годинники повинні синхронізуватися з централізованим джерелом еталонного часу, встановленим на UTC

9.1.6. Повинні бути створені середовища та плани тестування для перевірки функціональності системи перед розгортанням у виробництві.

9.1.7. Для розробки, тестування, забезпечення якості та виробництва повинні підтримуватися окремі середовища, як логічні, так і фізичні, включаючи окремі ідентифікатори середовищ.

9.1.8. Необхідно розробити, впровадити та забезпечити виконання формальних процедур контролю змін для всіх систем, включаючи будь-які зміни, що впливають на виробниче середовище та/або виробничі дані.

9.2. Бази даних та програмне забезпечення (зокрема розроблене власними силами або сторонніми організаціями, а також комерційне готове програмне забезпечення (COTS)):

9.2.1. Усе програмне забезпечення повинно включати безпечні методи кодування перед розгортанням у виробництві.

9.2.2. Дані тестування повинні бути захищені та контрольовані протягом усього процесу тестування відповідно до їхньої класифікації.

9.2.3. Виробничі дані можуть бути використані для тестування тільки за умови схвалення власником інформації, застосування відповідних заходів безпеки до тестового середовища або маскування конфіденційних даних чи заміни їх фіктивною інформацією.

9.2.4. Програмне забезпечення та інструменти для розробки не повинні підтримуватися на експлуатаційних системах, якщо це технічно можливо.

9.2.5. Вихідний код не повинен зберігатися на експлуатаційній системі, на якій працює додаток або програмне забезпечення, якщо це технічно можливо.

9.2.6. Скрипти, які не потрібні для роботи та обслуговування, повинні бути видалені з експлуатаційних систем.

9.2.7. Привілейований доступ розробників до експлуатаційних систем повинен бути обмежений.

9.2.8. Повинні бути задокументовані та впроваджені процеси міграції для перенесення програмного забезпечення з середовища розробки у експлуатаційне середовище.

9.3. Мережеві системи:

9.3.1. З'єднання між системами повинні бути дозволені вищим виконавчим керівництвом та захищені відповідними засобами контролю.

9.3.2. Необхідно підтримувати мережеву архітектуру з багаторівневою сегментацією мережі між різними типами систем та сегментами.

9.3.3. Управління мережею повинно здійснюватися із захищеної, виділеної мережі.

9.3.4. Для всіх користувачів, що підключаються до внутрішніх систем, необхідна аутентифікація.

9.3.5. Мережева автентифікація необхідна для всіх пристроїв, що підключаються до внутрішніх мереж.

9.3.6. Тільки уповноважені особи або структурні підрозділи можуть перехоплювати або контролювати мережевий трафік.

9.3.7. Перед ініціюванням або значною зміною будь-якої мережевої технології або проекту, включаючи бездротову технологію, необхідно провести оцінку ризиків.

10. Фізична безпека

10.1. Приміщення для обробки інформації повинні бути розміщені в безпечних зонах, фізично захищених від несанкціонованого доступу, пошкодження та втручання за допомогою визначених периметрів безпеки.

10.2. Інформаційно-технологічне обладнання повинно бути фізично захищене від загроз безпеці та небезпек, пов'язаних з навколишнім середовищем. Також можуть знадобитися спеціальні засоби контролю для захисту допоміжної інфраструктури та об'єктів, таких як електропостачання та кабельна інфраструктура.

10.3. Повинні існувати багаторівневі внутрішні та зовнішні засоби контролю безпеки для стримування або запобігання несанкціонованому доступу та захисту активів. Це стосується тих, які є критично важливими або вразливими до раптових або прихованих атак.

10.4. Періодична оцінка ризиків повинна проводитися для засобів обробки та зберігання інформації, щоб визначити, чи працюють існуючі засоби контролю належним чином і чи потрібні додаткові заходи фізичного захисту. Ці заходи повинні бути впроваджені для зменшення ризиків.

10.5. Все інформаційно-технологічне обладнання та носії інформації повинні бути захищені для запобігання порушенню конфіденційності, цілісності або доступності відповідно до ступеня секретності інформації, що міститься в них.

10.6. Відвідувачі приміщень для обробки та зберігання інформації, включаючи обслуговуючий персонал, завжди повинні супроводжуватися.

11. Управління вразливостями

11.1. Товариство зобов'язане вживати належних заходів для усунення ризиків, пов'язаних з технічною вразливістю інформаційних систем, що використовуються в Товаристві.

11.2. Власники активів несуть відповідальність за отримання інформації про технічні вразливості, що впливають на їхні активи, та своєчасне усунення виявлених технічних вразливостей.

11.3. Інформація про технічні вразливості, що впливають на активи Товариства, може бути отримана наступними каналами:

- 11.3.1. звіти та повідомлення від систем моніторингу безпеки
- 11.3.2. результати сканування вразливостей
- 11.3.3. результати тестування на проникнення
- 11.3.4. звіти та повідомлення від користувачів
- 11.3.5. звіти та повідомлення від постачальників
- 11.3.6. звіти та повідомлення від груп та спільнот з інформаційної безпеки
- 11.3.7. звіти та повідомлення від платформ розвідки загроз та баз даних вразливостей

11.4. Для усунення виявлених вразливостей повинні бути вжиті відповідні заходи, такі як виправлення або оновлення системи.

11.5. Будь-яке сканування вразливостей/тестування на проникнення повинно проводитися особами, уповноваженими менеджером з безпеки та бізнес-групою. Про будь-які такі тести необхідно заздалегідь повідомляти Менеджера з безпеки та Бізнес-команду. Будь-які інші спроби виконати таке сканування вразливостей/тестування на проникнення будуть вважатися спробою несанкціонованого доступу.

11.6. Будь-яка особа, уповноважена виконувати сканування вразливостей/тестування на проникнення, повинна мати формальний процес, визначений, протестований і постійно дотримуватися його, щоб звести до мінімуму можливість збоїв.

12. Безпека операційних процесів

12.1. Компанія забезпечує коректну та безпечну роботу систем обробки інформації. Це включає в себе наступне:
- 12.1.1. задокументовані операційні процедури;
- 12.1.2. використання формального управління змінами та потужностями;
- 12.1.3. засоби захисту від шкідливого програмного забезпечення;
- 12.1.4. визначене використання журналювання;
- 12.1.5. управління вразливостями.

12.2. Системи та фізичні об'єкти, на яких вони розміщені, повинні мати задокументовані інструкції з експлуатації, процеси управління та офіційні процедури управління інцидентами, що стосуються інформаційної безпеки, з розмежуванням ролей та відповідальності осіб, які їх експлуатують або використовують.

12.3. Конфігурації систем повинні відповідати затвердженим стандартам конфігурації.

12.4. Необхідно здійснювати завчасне планування та підготовку для забезпечення достатньої потужності та доступності ресурсів. Пропускна спроможність системи повинна постійно контролюватися.

12.5. Засоби контролю, такі як антивірус та веб-фільтрація, повинні бути впроваджені в усіх системах, де це технічно можливо, для запобігання та виявлення шкідливого коду або інших загроз.

12.6. Повинні бути впроваджені засоби контролю для відключення автоматичного виконання контенту зі змінних носіїв.

12.7. Повинні бути впроваджені засоби контролю, що обмежують зберігання інформації лише авторизованими місцями.

12.8. Повинні бути встановлені засоби контролю, що дозволяють запускати в системі тільки затверджене програмне забезпечення та запобігають виконанню всього іншого програмного забезпечення.

12.9. Всі системи повинні підтримуватися на рівні, що підтримується постачальником, для забезпечення точності та цілісності.

12.10. Виправлення безпеки повинні своєчасно переглядатися, оцінюватися та застосовуватися. Цей процес повинен бути автоматизований, якщо це технічно можливо.

12.11. Системи, що не підтримуються або не піддаються виправленню, повинні бути видалені.

12.12. Системи та додатки повинні контролюватися та аналізуватися для виявлення відхилень від вимог контролю доступу, викладених у цій Політиці та Політиці реєстрації та моніторингу, а також для реєстрації подій з метою отримання доказів та реконструкції даних.

12.13. Журнали аудиту, що фіксують винятки та події, пов'язані з безпекою, повинні створюватися, захищатися та зберігатися відповідно до графіків та вимог щодо зберігання записів.

12.14. Системи моніторингу, такі як системи виявлення/запобігання вторгненням, повинні бути розгорнуті в стратегічних місцях для моніторингу вхідного, вихідного та внутрішнього мережевого трафіку.

12.15. Системи моніторингу повинні бути налаштовані таким чином, щоб сповіщати персонал, який реагує на інциденти, про ознаки компрометації або потенційної компрометації.

12.16. Необхідно розробити та регулярно тестувати плани на випадок непередбачених обставин (наприклад, плани безперервності бізнесу, плани аварійного відновлення). Як мінімум, ці плани повинні включати наступне:

12.16.1. Оцінку критичності систем, що використовуються для обробки інформації.

12.16.2. Цілі часу відновлення (RTO)/цілі точки відновлення (RPO) для всіх критичних систем.

12.17. Резервні копії інформації, програмного забезпечення та системних образів Компанії повинні створюватися регулярно, відповідно до визначених вимог Компанії.

12.18. Резервне копіювання та відновлення повинні регулярно тестуватися, і для цих функцій повинен застосовуватися розподіл обов'язків.

12.19. Повинні бути встановлені процедури для підтримки інформаційної безпеки під час несприятливих подій. Якщо певні засоби контролю неможливо підтримувати, необхідно впровадити компенсаційні засоби контролю.

13. Безпека комунікації

13.1. Компанія буде підтримувати контроль мережевої безпеки для забезпечення захисту інформації в своїх мережах. Компанія також надасть інструменти та інструкції для забезпечення безпеки передачі інформації в своїх мережах та із зовнішніми організаціями. Це відповідає вимогам щодо класифікації та поводження з такою інформацією.

14. Придбання, розробка, і підтримка систем

14.1. Вимоги інформаційної безпеки повинні бути визначені під час розробки бізнес-вимог до нових інформаційних систем або змін до існуючих інформаційних систем.

14.2. Заходи контролю для зменшення будь-яких виявлених ризиків повинні бути впроваджені там, де це доречно.

14.3. Розробка систем повинна підлягати контролю змін та розділенню тестового, розробницького та експлуатаційного середовищ.

15. Аспекти інформаційної безпеки у процесах забезпечення безперервності бізнесу

15.1. У Товаристві впроваджені заходи для захисту критично важливих бізнес-процесів від наслідків серйозних збоїв інформаційних систем або катастроф. Це має забезпечити їх своєчасне відновлення відповідно до задокументованих бізнес-потреб. Це включає відповідні процедури резервного копіювання та вбудовану відмовостійкість.

15.2. Плани безперервності діяльності повинні підтримуватися та тестуватися на підтримку цієї Політики..

15.3. Необхідно проводити аналіз впливу на бізнес з детальним описом наслідків:

15.3.1. стихійних лих;

15.3.2. збоїв у системі безпеки;

15.3.3. втрати послуг;

15.3.4. відсутності доступності послуг.

Затверджено на
засіданні Ради директорів
дд.мм.рррр

ДОДАТОК Е. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Kurii, Y. Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32. *Особистий внесок аспіранта: проведено аналіз та представлено порівняльну характеристику стандартів аудиту з кібербезпеки ISO 27001 та NIST SP 800-53.*

2. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 6–20.doi: https://doi.org/10.15587/1729-4061.2023.273363. *Особистий внесок аспіранта: проведено аналіз недавніх кібератак на критичну інфраструктуру.*

3. Kurii, Y. ., & Opirskyy, I. (2023). ISO 27001: АНАЛІЗ ЗМІН ТА ОСОБЛИВОСТІ ВІДПОВІДНОСТІ НОВІЙ ВЕРСІЇ СТАНДАРТУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655. *Особистий внесок аспіранта: проведено огляд нової редакції стандарту ISO 27001:2022 та ключових змін у структурі та описі контролів безпеки, а також розроблено рекомендації для досягнення відповідності вимогам оновленої версії стандарту.*

4. Євгеній Курій, Віталій Сусукайло, Іван Опірський (2023). РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001. Ukrainian Information Security Research Journal. 25(3):132-139. DOI: https://doi.org/10.18372/2410-7840.25.17938. *Особистий внесок аспіранта: розроблено метод оцінки системи управління інформаційною безпекою об’єкта*

критичної інфраструктури на відповідність вимогам стандарту ISO 27001, що ґрунтується на використанні детального контрольного списка.

5. Vakhula O., Kurii Y., Opirskyy I., Susukailo V. (2024) Security-as-code concept for fulfilling ISO/IEC 27001:2022 requirements // Paper presented at the CEUR Workshop Proceedings, vol. 3654, . 59–72. *Особистий внесок аспіранта: проведено огляд і аналіз нових вимог стандарту ISO 27001:2022 і, зокрема, контролю A.8.9 - Управління налаштуваннями.*

6. Курій Є. О., Опірський І. Р. (2024) Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS // Кібербезпека: освіта, наука, техніка. – Т. 3, № 23. – С. 145–155. DOI: https://doi.org/10.28925/2663-4023.2024.23.145155. *Особистий внесок аспіранта: проведено дослідження та аналіз останньої версії стандарту PCI DSS v.4.0., зокрема, її основних змін та вдосконалень у порівнянні з попередньою версією PCI DSS v.3.2.1.*

Наукові публікації у збірниках матеріалів та тез конференцій:

7. Yevhenii KURII, Ivan OPIRSKYY, Leonid BORTNIK ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD // Materials of IXth International Scientific and Technical Conference INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY, May 25–26, 2023. - Lviv, Ukraine, pp 15-17, ISBN 978-966-941-829-6. *Особистий внесок аспіранта: проведено аналіз оновленої редакції стандарту ISO 27001:2022 та розроблено рекомендації для досягнення відповідності вимогам оновленої версії.*

8. Курій Є. О., Опірський І. Р. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОСНОВНИХ ФРЕЙМВОРКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск

85): матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 15-16 лютого 2024 р.). – 2024. – С. 34–36. *Особистий внесок аспіранта: проведено порівняльну характеристику провідних стандартів аудиту з кібербезпеки..*

9. Курій Є. О., Опірський І. Р. АНАЛІЗ ПЕРЕВАГ І НЕДОЛІКІВ ПЕРЕХРЕСНОГО ВПРОВАДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ // Materials of the V International Research and Practical Internet Conference «Development Strategies for Modern Education and Science», – 2024. – 2024. – С. 16–17. *Особистий внесок аспіранта: проведено аналіз переваг і недоліків застосування методології перехресного впровадження стандартів аудиту з кібербезпеки для підвищення захищеності об'єктів критичної інфраструктури.*