УДК 004.056.5

Войтович О.П.
Волинець В.В.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРАУДИТ: КОНЦЕПЦІЯ ТА СТАНДАРТИ ЗАХИСТУ ПІДПРИЄМСТВА

Вінницький національний технічний університет

Анотація
У тезах розглядається поняття аудиту інформаційної безпеки та його технічної складової - кібераудиту, а також стандарти, на яких базується оцінка захищеності підприємств. Аудит безпеки трактується як комплексний механізм оцінювання ефективності заходів захисту, де кібераудит виступає інструментом виявлення технічних вразливостей і контролю відповідності цифрових активів вимогам стандартів і регуляторних норм. Проаналізовано міжнародні стандарти та фреймворки (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework, COBIT, а також NIS2, PCI DSS, GDPR), їх роль у підвищенні стійкості організацій та формуванні програм комплексного аудиту. Окреслено перехід від періодичних перевірок до безперервного та адаптивного кібераудиту, використання автоматизації та штучного інтелекту для аналізу даних і виявлення аномалій. Наголошено на важливості постійного удосконалення методик аудиту в умовах динамічного середовища загроз.

Ключові слова: *аудит інформаційної безпеки; кібераудит; стандарти кібербезпеки; ISO/IEC 27001; NIST CSF; COBIT*

Abstract
These theses examine the concept of information security audit and its component - cyber audit, as well as the main standards that underpin enterprise security assessment. Security audit is treated as a core mechanism for evaluating the effectiveness of security measures, while cyber audit serves as a tool for identifying technical vulnerabilities and ensuring digital compliance with relevant standards and regulatory requirements. The work analyzes international standards and frameworks (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework, COBIT, as well as NIS2, PCI DSS, GDPR), their role in strengthening organizational resilience and shaping audit programs. It outlines the shift from periodic, checklist-based inspections towards continuous and adaptive cyber auditing supported by automation and artificial intelligence. The importance of ongoing improvement of audit methodologies in a dynamic threat environment is emphasized.

Keywords: *information security audit; cyber audit; security standards; ISO/IEC 27001; NIST CSF; COBIT.*

Вступ

Сучасні підприємства дедалі більше залежать від інформаційних систем, хмарних сервісів та цифрових каналів взаємодії з клієнтами й партнерами. Це підвищує їхню вразливість до кібератак, витоків даних і порушення критично важливих процесів. У таких умовах аудит інформаційної безпеки, що включає кібераудит як технічну компоненту, є важливою складовою управління захистом підприємства.

Аудит інформаційної безпеки – це систематична перевірка стану захисту всіх активів організації (інформаційних, фізичних, кадрових), яка дає змогу оцінити ефективність заходів безпеки та відповідність політик вимогам стандартів [1]. У свою чергу, кібераудит (Cybersecurity Audit) вимагає чіткої технічної дефініції. Згідно з визначенням міжнародної асоціації ISACA, кібераудит - це технічна оцінка систем і контролів, що діють для забезпечення безпеки кібердіяльності, метою якої є підтвердження того, що технологічні активи захищені, а регуляторні вимоги виконуються ефективно та результативно. Він фокусується на перевірці цифрового середовища, дозволяючи виявити технічні вразливості та перевірити дієвість технічних контролів у кіберпросторі [2].

Необхідність розмежування та інтеграції цих видів аудиту зумовлена зростанням кількості та складності кібератак, а також посиленням регуляторних вимог щодо захисту об’єктів критичної інфраструктури та персональних даних. Для багатьох організацій формалізована програма аудиту стала умовою доступу до ринків. У цьому контексті кібераудит

забезпечує глибокий аналіз технічних контролів (активний аудит), що є фундаментом для ширшого оцінювання зрілості процесів управління інформаційною безпекою.

Результати дослідження

Сучасна практика аудиту спирається на комплекс міжнародних стандартів, які чітко структуруються за рівнями управління та технічної реалізації. Центральне місце в системі аудиту інформаційної безпеки посідає ISO/IEC 27001, що встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Стандарт орієнтує підприємства на ризик-орієнтований підхід до захисту всіх активів і цикл безперервного удосконалення. ISO/IEC 27002 доповнює його детальним описом контролів, які слугують критеріями для перевірки, охоплюючи як організаційні, так і технічні аспекти [3].

Натомість, ключовим орієнтиром для кібераудиту є NIST Cybersecurity Framework, що описує цикл кіберзахисту через п’ять базових функцій: ідентифікація, захист, виявлення, реагування та відновлення. Цей фреймворк дозволяє детально перевірити технічну здатність організації протистояти кіберзагрозам, а його категорії зіставляються з вимогами ISO/IEC 27001. Оновлена версія NIST CSF 2.0 посилила акцент на управлінні (Govern), що сприяє кращій інтеграції технічного кібераудиту в загальну систему менеджменту [4].

Варто також враховувати глобальну специфіку вимог. Підходи до аудиту суттєво варіюються в різних регіонів світу: від жорсткого централізованого регулювання в ЄС (GDPR, NIS2) до ринково-орієнтованих моделей у США та специфічних вимог державного контролю в Азії. Це створює виклики для міжнародних компаній і вимагає адаптації процедур кібераудиту до локальних нормативних ландшафтів, щоб уникнути «втоми від відповідності» та забезпечити реальну кіберстійкість [5].

Фреймворк COBIT зосереджується на управлінні IT та узгодженні IT-процесів зі стратегічними цілями, надаючи структуру для аудиту управління технологіями, що є сполучною ланкою між бізнес-цілями та кібербезпекою. Паралельно застосовуються регуляторні стандарти. Директива NIS2 в ЄС та відповідне законодавство України вимагають від операторів об’єктів критичної інфраструктури впроваджувати технічні заходи кібербезпеки, виконання яких є предметом саме кібераудиту. Стандарт PCI DSS регламентує захист платіжних даних і вимагає регулярного сканування вразливостей, що є типовим прикладом технічного аудиту [3].

Практика показує, що зрілі організації використовують ISO/IEC 27001 як загальний каркас СУІБ, а NIST CSF - як модель для побудови технічного профілю кібербезпеки. У підсумку формується ієрархічна програма аудиту: аудит інформаційної безпеки оцінює організаційну відповідність і процеси, а кібераудит - надійність технічних бар'єрів та стійкість до атак [6].

Класичний процес аудиту включає етапи планування, збору доказів, аналізу й оцінювання. На етапі збору доказів розмежування стає очевидним: для аудиту ІБ проводяться інтерв’ю з персоналом та аналіз документації, тоді як для кібераудиту здійснюється активний моніторинг, огляд конфігурацій, тестування технічних контролів, систем керування доступом, журналювання подій і засобів виявлення вторгнень.

Разова або рідкісна перевірка вже не відповідає динаміці сучасного середовища загроз. Нові вразливості з’являються майже щодня. У відповідь формується підхід безперервного кібераудиту, що є технічним підґрунтям для актуалізації стану інформаційної безпеки. Такий підхід передбачає автоматизований збір і кореляцію даних із журналів подій, систем моніторингу, платформ керування вразливостями.

Важливим чинником розвитку саме кібераудиту є застосування штучного інтелекту. Інтеграція технологій ШІ в аудиторські процеси дозволяє не лише автоматизувати рутинні завдання перевірки, але й значно підвищити точність виявлення аномалій у великих масивах даних, що є критичним для предиктивного аналізу ризиків. Алгоритми допомагають класифікувати події й пріоритизувати інциденти за рівнем ризику, що зменшує навантаження на аудиторів та підвищує точність виявлення потенційно небезпечних ситуацій. На цій основі

формуються адаптивні моделі аудиту, у яких результати технічного аналізу використовуються для оперативного коригування планів перевірок СУІБ [7].

Організаційно кібераудит розглядається в контексті моделі трьох ліній захисту. Перша лінія відповідає за щоденне виконання контролів, друга забезпечує моніторинг, а третя (внутрішній аудит) здійснює незалежну оцінку, спираючись на дані кібераудиту як на доказову базу.

Висновок

Аудит інформаційної безпеки є центральним елементом системи захисту підприємства, що забезпечує комплексну оцінку управління ризиками, тоді як кібераудит виступає його невід'ємною технологічною складовою, орієнтованою на цифровий простір. Міжнародні стандарти, зокрема ISO/IEC 27001 (рівень управління) та NIST Cybersecurity Framework (рівень кіберзахисту), разом із вимогами NIS2, PCI DSS, GDPR формують методологічну основу цієї дворівневої системи оцінювання. Сучасні тенденції демонструють перехід від епізодичних перевірок до адаптивного й безперервного кібераудиту, який поєднує стандартизовані підходи з автоматизацією, аналітикою та використанням штучного інтелекту. Такий інтегрований підхід дозволяє підприємствам не лише відповідати вимогам стандартів, але й реально протистояти сучасним кіберзагрозам у динамічному цифровому середовищі.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548
2. Chimwanda, E. (2022, April 8). *Essentials for an effective cybersecurity audit*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit
3. National Institute of Standards and Technology. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29
4. Riaz, K. (2025). *ISO 27001 and cybersecurity: A synergistic approach for resilient information governance*. SSRN. https://doi.org/10.2139/ssrn.5228894
5. Войтович, О., & Волинець, В. (2025). Особливості законодавства щодо аудиту кібербезпеки в різних регіонах світу. *Measuring and Computing Devices in Technological Processes*, (3), 23–29. https://doi.org/10.31891/2219-9365-2025-83-3
6. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, *144*, 103964. https://doi.org/10.1016/j.cose.2024.103964
7. Войтович, О. П., Пилявець, І. Ю., & Радченко, Є. В. (2025). Використання штучного інтелекту в аудиті інформаційної безпеки. В *Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2025)»*. Вінницький національний технічний університет. https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/view/22704

Волинець Віталій Володимирович — аспірант групи 125-24а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: volynets1026@gmail.com

Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.vk.vntu.edu.ua

Volynets Vitalii V. — Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: volynets1026@gmail.com

Voytovych Olesya P. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail voytovych.vk.vntu.edu.ua