Огляд методології проведення аудитів з кібербезпеки на відповідність стандартам

Максим Делембовський[1], Максим Маркевич[2], Борис Корнійчук[3]

[1 2 3] Київський національний університет будівництва і архітектури
пр-т Повітрофлотський, 31, Київ, Україна, 03680
[1] delembovskyi.mm@knuba.edu.ua, https://orcid.org/0000-0002-6543-0701,
[2] markevych_mo@knuba.edu.ua,
[3] korniichuk.bv@knuba.edu.ua, https://orcid.org/0000-0003-3881-1581

Received 13.05.2024, accepted 20.05.2024
https://doi.org/10.32347/uwt.2024.14.1206

Анотація. Це дослідження зосереджується на аналізі проведення аудитів кібербезпеки, яке надає узагальнене бачення даного процесу.

Основна увага приділена аналізу етапів проведення аудитів кібербезпеки та методам збору інформації. Основна увага приділена розробці та імплементації сенсорних систем, здатних витримувати високий тиск та корозію у підводному середовищі, а також забезпечувати точні та надійні дані.

В роботі охоплено теоретичні аспекти проведення аудитів, включаючи визначення цілей, обсягу та типу аудиту, його планування, збір доказів та оцінку відповідності стандартам кібербезпеки.

Дане дослідження вказує важливість коригувальних дій зі сторони організації після проведеного аудиту, оскільки без цього етапу даний процес майже повністю позбавлений сенсу.

Ключові слова: кібербезпека, стандарт кібербезпеки, аудит, перевірка на відповідність, захист даних, рівень захисту, ризик, процес проведення аудиту.

ВСТУП

В роботі представлено інформацію про аудит кібербезпеки та надає читачеві базові знання щодо даного процесу.

Сучасна індустрія інформаційних технологій (далі - ІТ) стрімко розвивається, і разом із цим зростає потреба у захисті ІТ ресурсів від зловмисників, а також, перевірок надійності такого захисту. Аудит кібербезпеки допомагає організаціям виявити вразливості систем та/або процесів, кількісно та якісно оцінити ризики та розробити роудмап для зменшення впливу цих ризиків, або їх усунення, зменшити ризики фінансових втрат та підвищити довіру клієнтів.

Аудити з кібербезпеки поділяються на аудит мережевої безпеки, аудит тестування на проникнення, аудит відповідності та загальний аудит. Крім того, аудити можуть бути внутрішніми та зовнішніми.

МЕТА ТА МЕТОДИ ДОСЛІДЖЕННЯ

Головною метою цього дослідження є опис процесу проведення аудитів кібербезпеки, а саме аналіз етапів аудиту, методів та інструментів для проведення аудитів.

Під час цього дослідження використовувався метод аналізу даних, у тому числі відкритих даних, який дозволяє використання

статистичних та аналітичних методів для обробки інформації.

Отже, незважаючи на те, що в даному дослідженні використовується лише один метод дослідження процесу проведення аудитів, можна стверджувати, що це дослідження повноцінне, оскільки охоплює кожен етап проведення аудитів.

ЕТАП ПЛАНУВАННЯ АУДИТУ

На етапі планування аудиту Організація повинна визначити для себе обсяг, цілі аудиту, стандарт, відповідно до якого буде проводитись аудит та тип аудиту (внутрішній/зовнішній).

Обсяг аудиту містить перелік інформаційних активів, які будуть перевірятись (інформаційні системи, відділи).

Цілі аудиту передбачають кінцевий результат, який хоче отримати Організація після його проведення. Це може бути визначений рівень захисту Організації, перевірка та сертифікація на відповідність конкретному стандарту, або виявлення та оцінка ризиків.

Залежно від цілей, змінюється і тип аудиту. Якщо аудит внутрішній – формується команда із відповідальних співробітників для створення плану аудиту. При залученні третіх сторін для проведення зовнішнього аудиту Організація повинна укласти договір про нерозголошення задля забезпечення мінімізації можливості витоку даних та надати третій стороні всю потрібну документацію для ознайомлення.

Після чого фінальним кроком даного етапу є створення плану аудиту, який повинен описувати кожен етап аудиту та містити інформацію про графік робіт, методи збору інформації та критерії оцінки (Рис. 1).

ЕТАП ЗБОРУ ІНФОРМАЦІЇ

На етапі збору інформації проводяться інтерв'ю з відповідальними співробітниками відділів Організації для покриття питань, які не були розкриті в документах взагалі, або розкриті не в повній мірі та для підтвердження, що співробітники Організації керуються документацією на практиці.

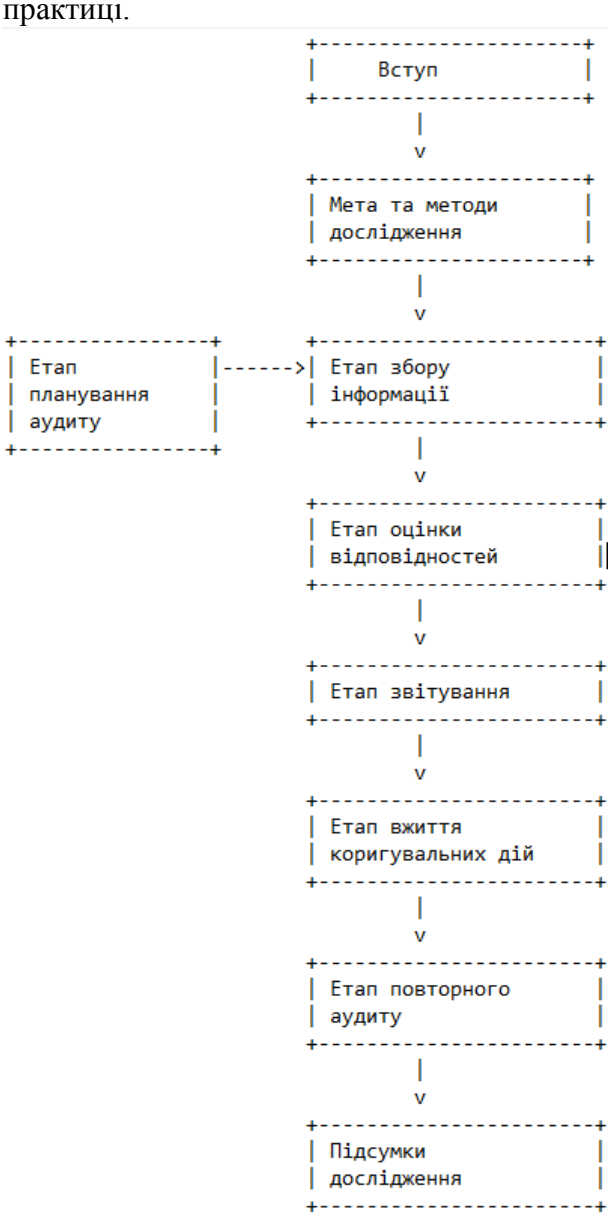

Рис. 1. Етапи аудиту кібербезпеки

Fig. 1. Stages of cyber security audit

Окрім інтерв’ю проводиться сканування систем на вразливості за допомогою спеціалізованого програмного забезпечення, тестування на проникнення та перевірка конфігурацій систем на відповідність вимогам стандарту.

ЕТАП ОЦІНКИ ВІДПОВІДНОСТЕЙ

Етап оцінки відповідностей є ключовим з точки зору аудитора, оскільки протягом цього етапу зібрана інформація з інтерв’ю, політики, процедури та результати

сканувань систем Організації порівнюються з вимогами та рекомендаціями стандартів. Водночас, цей етап є найбільш проблемним, оскільки кожен аудитор може оцінювати рівень захисту по-різному, оскільки це суб'єктивний параметр.

Крім того, даний етап може включати оцінку ризиків.

ЕТАП ЗВІТУВАННЯ

На етапі звітування відповідальні співробітники повинні підготувати звіт щодо проведеного аудиту, який повинен містити оцінку відповідності стандарту, опис виявлених розбіжностей, вразливостей, ризиків та рекомендацій щодо їх мінімізації, або усунення.

Структура звіту повинна бути лаконічною та зрозумілою для керівництва.

Звіт повинен бути наданий керівництву для ознайомлення. Після чого, при виникненні запитань від керівництва, аудитор повинен відповісти на них.

ЕТАП ВЖИТТЯ КОРИГУВАЛЬНИХ ДІЙ

Етап вжиття коригувальних дій здебільшого стосується лише організації замовника і є для неї ключовим, оскільки проведення аудиту без реагування на ідентифіковані вразливості та ризики є марно витраченими ресурсами. Протягом даного етапу відповідальні співробітники організації визначають критичність виявлених вразливостей та ризиків, поступово мінімізуючи їх вплив.

Проте до даного етапу також можуть залучатись і аудитори.

ЕТАП ПОВТОРНОГО АУДИТУ

Протягом етапу повторного аудиту перевіряються впроваджені зміни та здійснюється переоцінка відповідності стандартам кібербезпеки.

ПІДСУМКИ ДОСЛІДЖЕННЯ

Результати дослідження показали, що ефективність аудиту залежить від ретельності планування, кваліфікації аудиторів, використання різних методів для збору інформації та кількості впроваджених в організації заходів захисту (чим якісніший захист в організації, тим більш ефективним є результат аудиту).

Аналізуючи порядок проведення аудитів кібербезпеки, можна стверджувати, що це дуже важливий процес, незважаючи на його довготривалість та ресурсозатратність, оскільки після аудиту організація отримує детальний опис поточного стану кібербезпеки та напрями для розвитку. визначити основні напрямки їх використання та/або застосування. Найбільш доцільна це є моніторинг морського середовища, але навіть окрім моніторингу є ще багато різних напрямки використання, які будуть також затребувані в технології сенсорних мереж (Рис. 2).

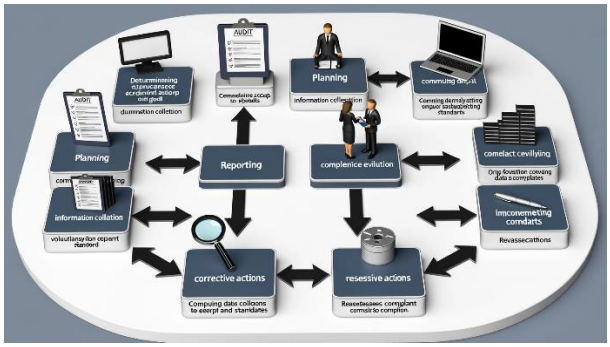

Рис. 2. Процес аудиту кібербезпеки

Fig. 2. Cyber security audit process

ВИСНОВОК

Аудит відповідності стандартам кіберрбезпеки є важливим процесом для організацій для підвищення рівню захищеності від загроз.

Ефективне проведення аудиту залежить від багатьох факторів, проте не матиме ніякого сенсу за умови відсутності заходів захисту в організації до початку проведення аудиту, а також, за відсутності коригувальних дій зі сторони організації після його проведення.

Задля забезпечення належного рівню кіберзахисту організація повинна постійно покращувати засоби захисту, проводити тренінги для персоналу та періодично проводити аудити кібербезпеки.

Це дослідження допомагає зрозуміти важливість аудиту кібербезпеки та пропонує основні напрямки для його впровадження та покращення, забезпечуючи захист інформаційних активів та підвищення довіри клієнтів.

ЛІТЕРАТУРА

1. **Рой Я. В., Мазур Н. П., & Складанний П. М.** (2018). Аудит інформаційної безпеки– основа ефективного захисту підприємства. Науково-технічний журнал" Кібербезпека: освіта, наука, техніка", (1), 86-93.
2. **Мельниченко О. В.** (2013). Аудит інформаційної безпеки банку при роботі з електронними грошима. Проблеми економіки, (4), 341-347.
3. **Огнева А. М.** (2009). Аудит інформаційних систем і технологій. Вісник Хмельницького національного університету, (6), 229-232.
4. **Kryvoruchko O., Desiatko A., & Synichuk O.** (2020). Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки. Управління розвитком складних систем, (43), 67-75.
5. **Войцьо О. М.** (2022). Аудит інформаційної безпеки ТОВ “СЕ Борднетце-Україна” 1” (Bachelor's thesis, ТНТУ).
6. **Пліс Г. В., Котух Є. В., Халімов Г. З., & Кучма О. М.** (2021). Аудит інформаційної безпеки як необхідна складова управління в державних установах. Державне будівництво, 1(30).
7. **Подола Х. А., & Сарахман О. М.** (2023) Аудит інформаційної безпеки компанії. Інновінг сучасних трендів в менеджменті безпеки, 4.
8. **Гавриленко А. С.** (2019). Аудит інформаційної безпеки в комп’ютерних мережах на базі Mikrotik.
9. **Тімченко А. В.** (2022). Методика аудиту інформаційної безпеки на стійкість до атак соціальної інженерії.
10. **Танянський А. Ю.** (2019). Аудит інформаційної безпеки в комп'ютерній системі підприемств.

REFERENCES

1. **Roy Y. V., Mazur N. P., & Skladanniy P. M.** (2018). Information security audit is the basis of effective enterprise protection. Scientific and technical journal "Cyber security: education, science, technology", (1), 86-93.
2. **Melnychenko O. V.** (2013). Audit of the bank's information security when working with electronic money. Problems of economics, (4), 341-347.
3. **Ogneva A. M.** (2009). Audit of information systems and technologies. Bulletin of the Khmelnytskyi National University, (6), 229-232.
4. **Kryvoruchko O., Desiatko A., & Synichuk, O.** (2020). Modeling of the information system for conducting an independent audit of information security. Management of the development of complex systems, (43), 67-75.
5. **Voitso O. M.** (2022). Information security audit of "SE Bordnetze-Ukraine" LLC 1" (Bachelor's thesis, TNTU).
6. **Plis G. V., Kotukh E. V., Halimov G. Z., & Kuchma O. M.** (2021). Information security audit as a necessary component of management in state institutions. State construction, 1(30).
7. **Podola H. A., & Sarakhman O. M.** (2023) Company information security audit. Innovating modern trends in security management, 4.
8. **Havrylenko A. S.** (2019). Audit of information security in computer networks based on Mikrotik.
9. **Timchenko A. V.** (2022). Information security audit methodology for resistance to social engineering attacks.
10. **Tanyansky A. Yu.** (2019). Audit of information security in the computer system of enterprises.

Review of methodology for conducting cybersecurity audits for compliance with standards

Maksym Delembovskyi, Maksym Markevych, Borys Korniichuk

Abstract. This study focuses on the analysis of conducting cybersecurity audits, providing a generalized view of this process. The main attention is given to analyzing the stages of conducting cybersecurity audits and methods of information collection. Special emphasis is placed on the development and implementation of sensor systems capable of withstanding high pressure and corrosion in underwater environments, as well as providing accurate and reliable data.

The work covers theoretical aspects of conducting audits, including defining objectives, scope, and type of audit, planning, evidence collection, and evaluating compliance with cybersecurity standards.

This research highlights the importance of corrective actions by the organization after the audit, as without this step, the process is almost entirely meaningless.

Keywords: cybersecurity, cybersecurity standard, audit, compliance check, data protection, protection level, risk, audit process.