УДК 004.056.5

М.Ю. Кривов`язюк
О.П. Войтович

ПІДХІД РИЗИК-ОРІЄНОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація.

У роботі представлено розробку ризик-орієнтованого підходу проведення аудиту інформаційної безпеки, спрямованого на підвищення об'єктивності та ефективності контролю в банківських установах. Підхід базується на вимогах Національного банку України та міжнародних стандартах ISO/IEC 27001, ISO/IEC 27005, COBIT 2019 і NIST SP 800-30, поєднуючи динамічну оцінку ризиків, технічні тестування, аналіз інцидентів та залучення експертів з IT та ІБ. Особлива увага приділяється ролі ризик-координаторів, які забезпечують ефективну взаємодію між аудиторами та технічними командами. Підхід підвищує достовірність результатів аудиту, зменшує залежність від формальної документації та узгоджує процес аудиту з сучасними загрозами.

Ключові слова: *ризик-орієнтований аудит, інформаційна безпека, банківський сектор, ISO/IEC 27001, COBIT 2019, управління ризиками, кібербезпека.*

Abstract.

This paper presents the development of a risk-oriented information security audit method aimed at improving the objectivity and efficiency of control within banking institutions. The approach is based on the requirements of the National Bank of Ukraine and international standards ISO/IEC 27001, ISO/IEC 27005, COBIT 2019, and NIST SP 800-30, integrating dynamic risk assessment, technical testing, incident analysis, and the involvement of IT and IS experts. Special attention is given to the role of risk coordinators, who ensure effective communication between auditors and technical teams. The method enhances the reliability of audit results, reduces dependence on formal documentation, an aligns the audit process with the modern cybersecurity landscape.

Keywords: *risk-oriented audit, information security, banking sector, ISO/IEC 27001, COBIT 2019, risk management, cybersecurity.*

Вступ

У сучасних умовах фінансово-кредитні установи стикаються зі зростаючими кіберзагрозами, що можуть призвести до фінансових втрат і витоку конфіденційної інформації. Традиційні підходи до проведення аудиту не враховують специфічні ризики систем та не дозволяють ефективно пріоритизувати перевірки [1-4]. Також у зв'язку з рухом України в бік Євросоюзу, де сформована культура кібераудиту, нормативні вимоги, підтримані жорсткими штрафами, поєднуються з галузевими стандартами і прозорими аудитами задля підвищення кіберстійкості, постає задача фокусування на критичних процесах, підвищення точності оцінювання ризиків та інтегрування автоматизованих інструментів для аналізу даних [3]. Актуальною залишається задача стандартизувати процедури аудиту відповідно до міжнародних вимог, ефективного управління ризиками та прийняття обґрунтованих управлінських рішень, що підвищує кіберстійкість фінансових установ [4-5].

Основна частина

Аудит інформаційної безпеки ґрунтується на вимогах Національного банку України [6-8], міжнародних стандартах ISO/IEC 27001, ISO/IEC 27005, COBIT, NIST SP 800-30 та на практичних підходах до оцінювання ефективності кіберзахисту. Запропонований ризик-орієнтований аудит інформаційної безпеки (кібераудит) полягає у тому, що оцінювання стану ІБ здійснюється не за формальними чек-листами, а залежно від рівня ризиків конкретних інформаційних систем, процесів та активів фінансово-кредитної установи. Основна увага приділяється тим зонам, які несуть найбільшу загрозу для безперервності бізнесу, конфіденційності даних та фінансової стабільності.

Спершу аудитори отримують доступ до звітів першої та другої лінії захисту, а також до даних SIEM та інших систем моніторингу інцидентів. Це створює основу для аналізу фактичних подій та визначення актуальних загроз. На основі зібраної інформації аудитори здійснюють аналіз ризиків, формують карту ризиків і визначають пріоритети аудиторських процедур. Програма аудиту вибудовується відповідно до цих пріоритетів, що дозволяє сфокусувати ресурси на найбільш критичних процесах. У процесі реалізації аудиту відбувається взаємодія з персоналом, який працює з відповідними

системами. Для підвищення точності оцінювання залучається ризик-координатор – фахівець ІТ/ІБ підрозділу, який володіє експертизою щодо архітектури систем і допомагає організувати комунікацію та доступ до даних. Ключовим елементом підходу є підтвердження висновків аудиту шляхом практичних тестувань: аналіз логів, перевірка налаштувань, вибірки з БД, функціональні тестування контролів. Це мінімізує ризик маніпуляції даними та забезпечує об'єктивність. Для ефективного аналізу цих даних аудиторам потрібні спеціалізовані інструменти [9].

Підсумкові висновки та рекомендації також проходять уточнення з ризик-координаторами, що дозволяє зробити їх більш точними, реалістичними та релевантними до фактичного середовища.

Такий підхід формує основу для ризик-орієнтованого аудиту, оскільки дозволяє ідентифікувати найбільш критичні ділянки контролів і процесів. Аналіз сирих даних дає змогу оцінити ймовірність та потенційний вплив ризиків, що дозволяє пріоритизувати перевірки за ступенем значущості. Впровадження цих заходів допомагає аудиторським підрозділам фокусувати ресурси на високоризикових областях і забезпечує більш ефективне управління ризиками в банківській ІТ-інфраструктурі. У результаті ризик-орієнтований аудит трансформує традиційну періодичну перевірку в безперервний, адаптивний, технічно обґрунтований механізм контролю, який забезпечує точнішу оцінку ефективності існуючих заходів, підвищує прозорість та стійкість інформаційної системи банку, а також дозволяє своєчасно й результативно реагувати на нові загрози, зменшуючи ймовірність реалізації критичних ризиків.

Висновок

Запропонований ризик-орієнтований підхід до проведення аудиту інформаційної безпеки дозволяє трансформувати традиційну періодичну перевірку у безперервний, адаптивний процес, який враховує актуальні ризики та реальні інциденти. Використання технічних інструментів, тестів та залучення ризик-координаторів і експертів ІТ/ІБ підвищує об'єктивність і достовірність аудиторських висновків. Інтеграція аудиту з моніторингом та управлінням ризиками забезпечує своєчасне виявлення критичних загроз, підвищує ефективність контролів і зміцнює систему кіберзахисту банківської установи. Такий підхід відповідає вимогам регулятора, міжнародним стандартам і створює підґрунтя для подальшого підвищення зрілості інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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
2. TZI. Аудит безпеки інформаційних систем. URL: https://tzi.com.ua/audbezib.html
3. Войтович, О. П., Пилявець, І. Ю., Радченко, Є. В. (2025). Використання штучного інтелекту в аудиті інформаційної безпеки. Матеріали науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи», https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/view/22704
4. IBM. (2024). X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence
5. KR-Labs. Аудит інформаційної безпеки. URL: https://kr-labs.com.ua/service/cybersecurity/audyt-informatsijnoyi-bezpeky/
6. Національний банк України. Постанова № 4 від 16.01.2021 "Про затвердження порядку проведення інспекційних перевірок у сфері інформаційної кібербезпеки банків".
7. Національний банк України. Постанова № 43 від 19.05.2021 "Про затвердження Положення про захист інформації в платіжних системах".
8. Національний банк України. Постанова № 95 від 28.09.2020 "Про організацію заходів із забезпечення інформаційної безпеки в банках України".

Кривов`язюк Максим Юрійович – студент групи 1БС-24м, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, e-mail: kryvovyazykmaks@gmail.com.

Kryvovyazyk M. Y. – student 1BS-24m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kryvovyazykmaks@gmail.com

Науковий керівник: Войтович Олеся Петрівна – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.olesya@vntu.edu.ua

Supervisor: Voytovych Olesya P. – Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical e-mail voytovych.olesya@vntu.edu.ua