https://doi.org/10.31891/2219-9365-2025-84-14
УДК 004.023

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
КОЛБА Сергій
Хмельницький національний університет
https://orcid.org/0009-0004-9354-6025
e-mail: revoment365@ukr.net
СИРОТЕНКО Дмитро
Хмельницький національний університет
https://orcid.org/0009-0004-4054-0498
e-mail: syrotenko.dm27@gmail.com
РИКУН Костянтин
Хмельницький національний університет
https://orcid.org/0009-0001-5177-0297
e-mail: rikunkostik@gmail.com

МЕТОДИКА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

У статті розглядається питання аналізу ризиків інформаційної безпеки, зокрема ризиків інформаційної безпеки у фінансових установах. Це питання заслуговує на особливу увагу, оскільки подібні установи переважно працюють із персональними даними клієнтів, заволодіння якими може надати несанкціонований доступ до фінансових ресурсів. Крім того, кожна подібна установа зобов'язана забезпечувати захист збережених клієнтських даних і дотримуватися режиму банківської таємниці.

На сьогоднішній день не існує стандартизованої методики аналізу та оцінювання ризиків інформаційної безпеки для фінансових установ. Тому у даній роботі розроблено конкретну методику аналізу та оцінювання ризиків інформаційної безпеки в подібних установах, створену на основі чинних стандартів і методик побудови системи захисту інформації на підприємств.

Ключові слова: оцінювання ризиків, CRAMM, RiskWatch, якісний аналіз, кількісний аналіз, конфіденційність, цілісність, доступність.

TITOVA Vira, KLOTS Yurii, KOLBA Serhii,
SYROTENKO Dmytro, RYKUN Kostiantyn
Khmelnitskyi National University

METHODOLOGY FOR ASSESSING INFORMATION SECURITY RISKS IN A FINANCIAL INSTITUTION

The relevance of this study lies in the necessity to devote special attention to information security risks within financial institutions. This necessity arises from the high value of information assets in such organizations. Their significance increases due to the presence of clients' personal data, as unauthorized access to such data could potentially enable illicit access to financial resources.

Therefore, the information used in the operations of financial institutions requires enhanced protection to preserve its key properties: confidentiality, integrity, and availability. However, to date, there is no standardized methodology for information security risk analysis and assessment that would be mandatory for all financial institutions. The existing and widely applied methodologies are largely generic, designed for organizations across various economic sectors, and fail to take into account the unique characteristics and specific operational contexts of each institution. Thus, there is a clear need to develop a specific methodology for the analysis and assessment of information security risks in the financial sector, grounded in existing international standards.

This article addresses the issue of information security risk analysis, with particular attention to risks within financial organizations. This topic warrants special consideration, as such institutions primarily operate with clients' personal data, possession of which may potentially provide access to financial resources. Moreover, every financial institution is obliged to ensure the protection of stored client data and to maintain banking confidentiality. At present, there is no standardized methodology for the analysis and assessment of information security risks specifically designed for financial organizations. Therefore, this study proposes a dedicated methodology for analyzing and assessing information security risks in such institutions, developed on the basis of existing standards and approaches to building information protection systems within enterprises.

Keywords: risk assessment, CRAMM, RiskWatch, qualitative analysis, quantitative analysis, confidentiality, integrity, availability.

Стаття надійшла до редакції / Received 16.08.2025
Прийнята до друку / Accepted 22.10.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сьогодні аналізу складних ризиків інформаційної безпеки (ІБ) приділяється дедалі більше уваги. Це пояснюється низкою основних причин:

– безперервним зростанням використання інформаційних технологій у діяльності практично будь-якої сучасної організації;

– підвищенням цінності інформації, що обробляється та генерується в процесі роботи компанії;

– інтеграцією різноманітних інформаційних продуктів з метою задоволення всіх потреб підприємства.

Актуальність даної статті полягає у необхідності приділення особливої уваги ризикам ІБ в фінансових установах. Це зумовлено високою вартістю інформаційних ресурсів у подібних компаніях. Їхня цінність зростає через наявність персональних даних клієнтів, адже особа, яка має доступ до таких даних, потенційно може отримати несанкціонований доступ до фінансових ресурсів.

Отже, інформація, що використовується у діяльності фінансових установ , потребує особливого захисту від втрати своїх ключових властивостей, таких як: конфіденційність, цілісність та доступність.

Однак на сьогоднішній день не існує стандартизованої методики аналізу та оцінки ризиків ІБ, яка була б обов'язковою для застосування у всіх фінансових установах. Усі розроблені та активно використовувані методики є досить загальними для організацій, що працюють у різних секторах економіки, і не враховують особливостей та специфіки діяльності кожної організації окремо. Водночас існує методика аналізу та оцінки ризиків ІБ в установах банківської системи, запропонована стандартом ISO 27001 [1], однак вона має лише рекомендаційний характер.

Таким чином, є потреба у розробці конкретної методики аналізу та оцінки ризиків ІБ у фінансовій сфері на основі існуючих стандартів.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Управління ризиками ІБ є ключовим елементом побудови ефективної системи захисту інформації фінансової установи. Серед найпоширеніших методик і програмних засобів аналізу ризиків виділяються Microsoft Risk Management Framework, CRAMM, FRAP та RiskWatch. Кожен із підходів має власні переваги, обмеження та сферу доцільного застосування.

Методика Microsoft базується на чотирьох етапах управління ризиками [2]. Це оцінка, прийняття рішень, реалізація контролю та оцінка ефективності. Використовується разом із програмним засобом Microsoft Security Assessment Tool (MSAT), який допомагає виявляти уразливості в IT-середовищі. Переваги: зрозуміла структура, підтримка якісної та кількісної оцінки, наявність безкоштовного інструменту MSAT. Недоліки: обмежена глибина аналізу технологічних процесів, орієнтація переважно на середні організації.

CRAMM (CCTA Risk Analysis and Management Method) поєднує якісну та кількісну оцінку ризиків [3]. Програмне забезпечення автоматизує ідентифікацію ресурсів, визначення загроз, уразливостей і формування рекомендацій щодо контрзаходів. Переваги: точність, комплексність, можливість формування різних сценаріїв аналізу. Недоліки: значна трудомісткість і потреба у кваліфікованих експертах; висока вартість ліцензії.

FRAP (Facilitated Risk Analysis Process) орієнтований на якісний аналіз ризиків і використовує прості інструменти збору експертних оцінок, такі як опитування, мозковий штурм, статистичний аналіз [3]. Переваги: швидкість проведення, невисока вартість, доступність для невеликих компаній. Недоліки: суб'єктивність результатів, низький рівень деталізації та відсутність автоматизованої підтримки.

RiskWatch – це програмний продукт, що реалізує кількісну оцінку ризиків на основі показників Annual Loss Expectancy (ALE) та Return on Investment (ROI) [4]. Переваги: точна економічна оцінка збитків і ефективності заходів захисту, автоматизація процесу, генерація детальних звітів. Недоліки: висока вартість програмного забезпечення, потреба в значному обсязі вхідних даних, орієнтація на великі корпоративні структури.

Узагальнюючи вищевикладене, можна зазначити, що Microsoft забезпечує стратегічний рівень управління безпекою. Методика FRAP є доцільною для швидкої попередньої оцінки або навчальних цілей. Найбільш збалансованими для застосування у фінансових установах можна вважати CRAMM та RiskWatch.

Порівняльний аналіз методів виявлення аномалій в мережевому трафіку

Методика аналізу та оцінювання ризиків ІБ для фінансової установи повинна забезпечувати якісну та кількісну оцінку ризику, що базується на визначенні ступеня ймовірності реалізації загроз ІБ виявленими та/або потенційними джерелами загроз, а також на оцінюванні тяжкості наслідків реалізації загрози.

В основу якісного методу оцінювання ризику доцільно покласти алгоритм, який використовується в методиці CRAMM, оскільки він передбачає розподіл рівнів ризику за шкалою від 1 до 7. Це дозволяє застосовувати більш гнучкий підхід до визначення категорій ризиків. Як вхідні дані в цьому методі використовуються три основні показники:

– рівень загрози («дуже високий», «високий», «середній», «низький», «дуже низький»);
– рівень уразливості ресурсу («високий», «середній», «низький»);
– критичність ресурсу (розмір очікуваних фінансових втрат) за шкалою від 1 до 7.

Співвідношення критичності ресурсу, рівня загрози та вразливості є наступним (табл. 1).

Таблиця 1

Співвідношення критичності ресурсу, рівня загрози та вразливості

Рівень загрози / **Критичність ресурсу**	дуже низький	низький	середній	високий	дуже високий
низький	1	2	3	4	5
середній	2	3	4	5	6
високий	3	4	5	6	7

Кількісний метод доцільно запозичити з алгоритму методики RiskWatch, оскільки для фінансових установ особливо важливим є поділ оцінок за типами загроз із акцентом на вразливостях.

Ризик загрози розраховується для конкретної вразливості:

$$TR = \frac{ER}{100} \times \frac{P(VL)}{100}, \tag{1}$$

де ER – критичність реалізації загрози у %;

$P(VL)$ – імовірність реалізації загрози через дану вразливість у %.

Отримуємо рівень загрози через вразливість в діапазоні від 0 до 1.

Розраховуємо ризик за ресурсом:

$$R = \max(TR \times CR), \tag{2}$$

де CR – критичність ресурсу, яка задається в грошовому еквіваленті або у вигляді рівнів.

Ризики в межах 0-2 вважаються прийнятними. Ризики в межах 2,01-5 потребують мінімізації з подальшою переоцінкою. Ризики вище 5 визнаються критичними та потребують негайного реагування.

Таблиця 2

Відповідність якісного та кількісного аналізу ризиків ІБ

ER		$P(VL)$	
0-20%	дуже низький	0-33%	низький
21-40%	низький	34-66%	середній
41-60%	середній	67-100%	високий
61-80%	високий		
81-100%	дуже високий		

В якості прикладу для перевірки запропонованої методики візьмемо робоче місце працівника фінансової установи. Інформаційним ресурсом є робоча станція, яка містить: персональні дані клієнтів; інформацію про рахунки; інформацію про транзакції; корпоративну пошту.

Далі складемо перелік загроз та уразливостей. Величини критичності реалізації загроз та ймовірності їх реалізації були отримані шляхом експертного оцінювання.

Загроза 1. Халатність співробітника: залишив робоче місце, не вийшовши з системи.
$ER = 100\%$

Вразливість 1. Автоматичний вихід із системи відбувається лише через 15 хвилин бездіяльності користувача.

$P(VL) = 50\%$

Загроза 2. Доступ сторонньою особою до логіна та пароля працівника.
$ER = 100\%$
Вразливість 2.1. Співробітник зберігає логін і пароль під клавіатурою.
$P(VL) = 30\%$
Вразливість 2.2. Відсутність мережевого захисту від несанкціонованого доступу.
$P(VL) = 80\%$

Для **загрози 1** критичність ресурсів становить $CR = 6$. Для **загрози 2**, яка реалізується через **вразливість 2.1** критичність ресурсів $CR = 5$. Для загрози 2, яка реалізується через **вразливість 2.2** критичність ресурсів становить $CR = 7$.

Розрахуємо ризик загрози за кожною вразливістю, для чого використаємо (1).

$$TR_1 = \frac{ER_1}{100} \times \frac{P(VL)_1}{100} = 0.5$$
$$TR_{2.1} = \frac{ER_2}{100} \times \frac{P(VL)_{2.1}}{100} = 0.3$$
$$TR_{2.2} = \frac{ER_2}{100} \times \frac{P(VL)_{2.2}}{100} = 0.8$$

Розраховуємо ризик за ресурсом (2):

$$R = \max((TR_1 \times CR_1), (TR_{2.1} \times CR_{2.1}), (TR_{2.2} \times CR_{2.2})) = \max((3), (1.5), (5.6))$$

З отриманих розрахунків можна зробити висновки, що ризик **загрози 2** через **вразливість 2.1** можна вважати прийнятним, і це логічно, бо імовірність, що хтось зі сторонніх осіб скористається логіном та паролем під клавіатурою, зайнявши місце співробітника, є невисокою. Ризик **загрози 1** потребує мінімізації, наприклад зменшення часу бездіяльності до автоматичного виходу з систему до 5 хвилин. Ризик **загрози 2** через **вразливість 2.2** – викрадення логіну та паролю працівника через зовнішні канали зв'язку є критичним та потребує негайного реагування, зокрема встановлення мережевого захисту.

Остаточним приймається ризик найвищого рівня, тому що він має найбільший вплив.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті були розглянуті та враховані стандарти у сфері захисту інформації та аналізу ризиків ІБ. У процесі дослідження було вирішено такі завдання:

– систематизовано інформацію про ризики ІБ, визначено важливість їх аналізу та оцінювання для побудови системи захисту інформації на підприємстві;
– розглянуто та враховано наявні рекомендації у сфері аналізу ризиків ІБ фінансових установ;
– проаналізовано та зіставлено існуючі методики оцінювання ризиків ІБ в контексті розробки системи управління ІБ фінансової установи.

Критерії порівняння було обрано на основі інформації про діяльність фінансових установ. За результатами порівняння виокремлено дві методики, які стали основою для створення рекомендацій щодо аналізу та оцінювання ризиків.

Розроблена методика враховує не лише особливості структури та діяльності фінансових установ, але й накопичений досвід у сфері розробки алгоритмів аналізу та оцінювання ризиків інформаційної безпеки.

Її основу становить процес оцінювання ризиків ІБ методом аналізу загроз і вразливостей. Спочатку рівень ризику визначається якісним методом, після чого було розраховується коефіцієнт кількісного показника.

У подальшому розроблена методика може застосовуватися для аналізу та оцінювання ризиків ІБ фінансових установ.

Література

1. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та

захист конфіденційності. Системи керування інформаційною безпекою. Вимоги.

2. Zhai, Xinyu. Risk Management Analysis on Microsoft Corporation// Highlights in Business, Economics and Management. 2023. Vol. 8. P. 373-378. https://doi.org/10.54097/hbem.v8i.7232

3. Memon, M.; Hameed, S. Information Security Risk Plans within Enterprise Architecture Framework// International Journal of Advanced Computer Science and Technology. 2019. Т. 8, № 10. С. 82-88. https://doi.org/10.30534/ijacst/2019/018102019

4. Kaur, Ekaspreet; Kaur, Simrata; Singh, Harjot; Kaur, Bisman; Pannu, H. S. Riskwatch: A Model for Improved Preoperative Risk Assessment of Anesthesia in Medical Science Using Machine Learning. 2024. https://doi.org/10.21203/rs.3.rs-4742242/v1

References

1 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

2. Zhai, Xinyu. Risk Management Analysis on Microsoft Corporation// Highlights in Business, Economics and Management. 2023. Vol. 8. P. 373-378. https://doi.org/10.54097/hbem.v8i.7232

3. Memon, M.; Hameed, S. Information Security Risk Plans within Enterprise Architecture Framework// International Journal of Advanced Computer Science and Technology. 2019. Т. 8, № 10. С. 82-88. https://doi.org/10.30534/ijacst/2019/018102019

4. Kaur, Ekaspreet; Kaur, Simrata; Singh, Harjot; Kaur, Bisman; Pannu, H. S. Riskwatch: A Model for Improved Preoperative Risk Assessment of Anesthesia in Medical Science Using Machine Learning. 2024. https://orcid.org/10.21203/rs.3.rs-4742242/v1