УДК 004.056.5:004.056.53
DOI: https://doi.org/10.17721/ISTS.2025.9.32-41

Володимир НАКОНЕЧНИЙ, д-р техн. наук, проф.
ORCID ID: 0000-0002-0247-5400
e-mail: volodym.nakonechnyi@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Микола МОРДВИНЦЕВ, канд. техн. наук, доц.
ORCID ID: 0000-0002-7674-3164
e-mail: pestalocyj@gmail.com
Харківський національний університет внутрішніх справ, Харків, Україна

Вікторія ГУСЄВА, студ.
ORCID ID: 0009-0002-1120-1900
e-mail: viktoriaguseva209@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

Владислав ЛУЦЕНКО, асп.
ORCID ID: 0000-0002-2377-1858
e-mail: vladyslav.lutsenko99@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ГІБРИДНИЙ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ. *Розглянуто гібридний підхід до управління ризиками інформаційної безпеки, що поєднує кількісні та якісні методи оцінювання відповідних ризиків. Це дозволяє підвищити точність, зменшити суб'єктивність оцінок і забезпечити автоматизацію процесу управління ризиками. Актуальність теми повязана з постійним зростанням кількості та складності кіберзагроз, що вимагає розроблення та впровадження ефективних інструментів для управління ризиками та зменшення впливу людського фактора.*

Методи. *Застосовано інтегрований підхід, що базується на методах FAIR, Монте-Карло для кількісної оцінки ймовірностей і CRAMM для якісного аналізу ризиків. Враховано міжнародні стандарти ISO 31000 та ISO/IEC 27005, які регламентують управління ризиками. Проведено ідентифікацію активів, визначено вразливості і класифікацію загроз відповідно до кращих практик інформаційної безпеки. Обґрунтовано застосування методології для формування моделі оцінювання ризиків, яка дозволяє врахувати різні рівні потенційних загроз.*

Результати. *Результати підтвердили адекватність та ефективність гібридного підходу. Запропонована модель дозволила ідентифікувати критичні активи, оцінити рівень ризиків і розробити рекомендації щодо впровадження контрзаходів. Використано метод Монте-Карло для оцінювання ймовірності успішних атак і розрахунку потенційних збитків. Аналіз за CRAMM дозволив визначити вразливості системи та запропонувати відповідні заходи безпеки. Проведено порівняльний аналіз традиційних методів оцінювання ризиків, що показав переваги інтегрованого підходу в умовах динамічного інформаційного середовища.*

Висновки. *Запропонований гібридний підхід сприятиме мінімізації впливу людського фактора, підвищенню точності оцінок і автоматизації управління ризиками. Це дозволить оптимізувати ресурси організації та забезпечити стратегічне планування захисту інформації. Подальші дослідження можуть зосередитися на розробленні інструментів автоматизації для інтеграції запропонованого підходу в реальні інформаційні системи. Рекомендовано подальший розвиток методології через адаптацію до різних сценаріїв загроз у межах організацій із різними профілями безпеки.*

Ключові слова: *інформаційна безпека, управління ризиками, методи CRAMM, Монте-Карло, FAIR, показник Герста, оцінювання ризиків.*

Вступ

Організації, що працюють у сучасному цифровому середовищі, дедалі більше залежать від інформаційних технологій, що робить їх особливо вразливими до кіберзагроз. Безперервне ускладнення та збільшення кількості загроз створюють нові виклики для ефективного управління ризиками в інформаційній безпеці. Традиційні методи управління ризиками, такі як кількісні або якісні підходи, нерідко виявляються недостатньо ефективними для вирішення складних загроз, що постають перед сучасними організаціями.

Забезпечення інформаційної безпеки вимагає застосування комплексних підходів до управління ризиками, які дозволяють вчасно ідентифікувати загрози, оцінювати їхній вплив і розробляти ефективні стратегії для їхньої мінімізації. Кількісні методи, зокрема Монте-Карло, FAIR чи NIST 800-30, надають точні числові дані щодо ймовірностей ризиків, проте часто вимагають значних ресурсів для збору даних. Водночас якісні методи, такі як експертні оцінки (COBRA, OCTAVE), залежать від суб'єктивної думки фахівців, що може вплинути на точність оцінок.

У зв'язку із цим усе більше уваги приділяється гібридним методам, які поєднують сильні сторони обох підходів. Однак навіть ці методи мають обмеження, зокрема і через залежність від ручної роботи та великих часових витрат. У відповідь на вказані виклики актуальним стає питання впровадження автоматизації у процеси управління ризиками, що дозволяє зменшити суб'єктивність оцінок, прискорити процес реагування на загрози та підвищити загальну ефективність безпеки.

Мета цього дослідження полягає у розробленні нового гібридного методу управління ризиками, який поєднує кількісні та якісні підходи, спрямовані на підвищення точності, швидкості і надійності управління ризиками в організаціях.

Об'єктом дослідження є процес управління ризиками в інформаційній безпеці.

Предметом дослідження є поєднання методів оцінювання ризиків у межах процесу забезпечення інформаційної безпеки для вдосконалення методу управління ризиками.

Для досягнення мети дослідження поставлено такі завдання:

- провести аналіз сучасних джерел у сфері інформаційної безпеки й управління ризиками;
- вивчити процеси управління ризиками та їхню роль у забезпеченні інформаційної безпеки;
- систематизувати підходи до класифікації ризиків і етапи забезпечення інформаційної безпеки в організаціях;

ISSN 2707-1758

- дослідити взаємозв'язок між управлінням інформаційною безпекою та бізнес-процесами;
- провести порівняльний аналіз методів оцінювання ризиків, таких як кількісні та якісні підходи;
- розробити гібридний метод управління ризиками на основі комбінації існуючих підходів до їхнього оцінювання;
- оцінити ефективність запропонованого гібридного методу управління ризиками та його вплив на практику забезпечення інформаційної безпеки.

Наукова новизна дослідження полягає в розробленні вдосконаленого процесу управління ризиками за допомогою створення гібридного методу, який використовує переваги відомих підходів до оцінювання ризиків і комбінує їх для точнішого аналізу та швидкого оброблення. Основною особливістю запропонованого методу є використання алгоритмів CRAMM, FAIR і Монте-Карло, а також інтеграція найкращих практик управління ризиками, що дозволяє зменшити суб'єктивність оцінок і підвищити ефективність прийняття рішень.

Огляд літератури. Управління інформаційними ризиками є однією з ключових складових інформаційної безпеки будь-якої організації. Протягом останніх десятиліть цей напрямок активно розвивався завдяки ряду досліджень і практичних підходів, які покращують оцінювання ризиків.

Українські дослідники Юдін О. К. і Бучик С. С. підкреслюють, що головною проблемою в управлінні інформаційними ризиками є правильна ідентифікація загроз і їхня класифікація. Досліджена цими вченими методологія побудови класифікатора загроз є однією з основ для розроблення державних інформаційних ресурсів, але, як зазначають автори, цей метод потребує додаткових інструментів для інтеграції із сучасними вимогами до безпеки (Юдін, & Бучик, 2015).

Інші вчені – McCumber, Wheeler, Graham, також активно досліджували управління ризиками в інформаційній безпеці.

Wheeler у своїх роботах (Wheeler, 2014; Wheeler, 2015) розглядає управління ризиками через призму кількісних підходів. Він вважає, що статистичні моделі, такі як Монте-Карло, є ефективними для оцінювання ризиків, оскільки вони дозволяють отримати точні числові значення ймовірностей виникнення загроз. Проте ці моделі значною мірою залежать від наявності великих обсягів необхідних даних, що не завжди доступно, особливо для малих і середніх організацій.

McCumber пропонує концепцію ризик-менеджменту, де основну увагу приділено процесу кількісного оцінювання ризиків. Автор вважає, що традиційні кількісні методи, наприклад аналіз імовірностей, є незамінними для великих підприємств і фінансових установ, які мають значні обсяги даних для аналізу (McCumber, 2011). Однак він також визнає, що кількісні підходи мають ряд обмежень, зокрема і потребу в точності введених даних і використанні спеціалізованих інструментів для їхнього оброблення.

Дослідник Graham акцентує увагу на необхідності подальшої автоматизації управління ризиками для підвищення точності й оперативності оцінювання (Graham, 2014). Він вважає, що ручне введення даних і проведення аналізу збільшує ризик людських помилок і знижує ефективність процесу управління ризиками.

Методи

Важливим етапом у розвитку методів управління ризиками стало впровадження таких інструментів, як NIST 800-30, FAIR, CRAMM, Risk Watch, COBRA й OCTAVE, кожен з яких має свої переваги і недоліки. Вони забезпечують організаціям структуровані підходи до управління ризиками, враховуючи і кількісні, і якісні аспекти оцінювання.

Метод NIST 800-30 є широко визнаним і стандартизованим підходом до оцінювання ризиків в інформаційній безпеці, особливо у державних і великих організаціях. Цей метод розроблено для ідентифікації загроз, вразливостей і оцінювання впливу ризиків на організацію. Він включає детальний аналіз активів, можливих сценаріїв атак і пропонує підхід до управління ризиками через комплексний аналіз. Однією з головних переваг цього методу є його структурованість і можливість інтеграції в системи інформаційної безпеки різних масштабів (NIST, 2012)

FAIR (Factor Analysis of Information Risk) пропонує кількісне оцінювання ризиків та акцентується на бізнес-аналітиці. Цей метод перетворює якісні дані на кількісні показники, що дозволяє проводити фінансовий аналіз ризиків, оцінювати їхній вплив на бізнес. FAIR застосовує факторний аналіз для оцінювання загроз, що робить його особливо корисним для великих організацій, де ризики мають значний фінансовий вплив. Проте цей метод вимагає великих масивів даних і детальної інформації для ефективної роботи (FAIR Institute, 2022).

CRAMM (CCTA Risk Analysis and Management Method) – це метод, що поєднує кількісні та якісні аспекти оцінювання ризиків. Він розроблений для глибокого аналізу активів і загроз, зокрема й ідентифікації вразливостей і оцінювання ефективності заходів безпеки. Основна його перевага – це структурований підхід до вибору контрзаходів на основі ризиків. Однак він може бути дуже трудомістким і вимагати значних ресурсів для реалізації через велику кількість ручної роботи.

Risk Watch – це автоматизована система для оцінювання ризиків, яка використовує програмні модулі для збору й оброблення даних. Метод базується на швидкому оцінюванні загроз і генеруванні звітів для подальших дій. Він особливо корисний для організацій, які не мають достатньо ресурсів для комплексного аналізу, оскільки дозволяє автоматизувати більшу частину процесу оцінювання. Однак цей метод залежить від якості введених даних і вимагає правильного налаштування (RiskWatch International, n. d.).

COBRA – це інструмент для швидкого оцінювання ризиків, який допомагає визначати можливі загрози і пропонувати відповідні дії для їхньої мінімізації. COBRA призначений для організацій, які мають обмежені ресурси і потребують швидкого аналізу. Він дозволяє точно ідентифікувати ризики та їхні наслідки, однак його функціонал може бути обмеженим для великих організацій, де потрібен більш комплексний підхід. (COBRA, n. d.).

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) розроблений для стратегічного планування інформаційної безпеки. Він включає ідентифікацію активів, загроз і вразливостей організації та фокусується на визначенні стратегічних рішень для мінімізації ризиків. Метод підходить для організацій, які хочуть інтегрувати управління ризиками в загальну стратегію безпеки, однак вимагає значної участі персоналу і високого рівня підготовки (OCTAVE, 2003).

Отже, вибір методу оцінювання ризиків залежить від потреб і можливостей організації. Нижче представлено порівняльну таблицю переваг і недоліків кожного із зазначених методів.

ISSN 2707-1758

Таблиця 1

Переваги та недоліки кожного методу оцінювання ризиків

Метод оцінювання	Переваги	Недоліки
FAIR	Комплексний аналіз, що включає кількісні показники	Підходить переважно для великих підприємств
	Висока ефективність у великих організаціях	Вимагає високого рівня технічних знань
	Точність в оцінюванні ризиків	Потребує значного часу на впровадження
	Орієнтованість на співпрацю між різними відділами	Орієнтація на точні дані та припущення, що може бути складно для менших організацій
	Легке налаштування й адаптація під різні вимоги	Орієнтація на точні дані та припущення, що може бути складно для менших організацій
NIST 800-30	Детальний опис ризиків для інформаційних активів	Процес оцінювання займає багато часу через обсяг даних
	Підходить для організацій будь-якого масштабу	Деякі функції залишаються не автоматизованими
	Гнучкість у застосуванні	Всеосяжний характер методу може зробити його складним у впровадженні для новачків
	Визнаний галузевий стандарт для управління інформаційною безпекою	Відсутність інтеграції з іншими сучасними методами управління ризиками
CRAMM	Ґрунтовне виявлення ризиків та активів	Висока трудомісткість процесу через необхідність ручної роботи
	Комплексний підхід до управління ризиками	Вимагає значних ресурсів для впровадження
	Орієнтованість на безпеку і управління контрзаходами	Потребує залучення експертів для аналізу й оцінювання ризиків
Risk Watch	Простота впровадження та використання завдяки автоматизації	Високі витрати на впровадження та технічну підтримку
	Підтримка кращих галузевих практик	Аналіз ризиків зосереджено переважно на програмно-технічних аспектах
	Інтуїтивно зрозумілий інтерфейс для користувачів	Можливості для кастомізації системи є обмеженими
COBRA	Структурований підхід із великим набором знань про загрози та вразливості	Не підходить для організацій зі складною структурою активів
	Легкість адаптації до специфічних потреб організації	Відсутність детального аналізу рівнів ризику
	Чіткі звіти з рекомендаціями щодо усунення ризиків	Потребує спеціального навчання персоналу для ефективного використання
OCTAVE	Комплексний підхід, що враховує як технічні, так і організаційні ризики	Трудомісткий процес впровадження, особливо для великих організацій
	Орієнтованість на критичні активи організації	Складність у налаштуванні та підтримці
	Здатність виявляти організаційні та технічні загрози одночасно	Складність у налаштуванні та підтримці

Результати

У сучасному цифровому середовищі управління ризиками в інформаційній безпеці вимагає не тільки глибокого розуміння різноманітних загроз, але й ефективних методів їхнього оцінювання та пом'якшення. Враховуючи складність ризиків і необхідність швидкого реагування на нові кіберзагрози, традиційні кількісні або якісні підходи часто виявляються недостатніми для забезпечення достатнього захисту. Гібридні методи, які об'єднують численні підходи до управління ризиками, дозволяють оптимізувати процеси оцінювання загроз і вразливостей поєднанням переваг обох методів.

Запропонований гібридний метод управління ризиками поєднує кількісні та якісні підходи, зокрема й використання моделі Монте-Карло для кількісного оцінювання ризику та методологію CRAMM для якісного оцінювання. Такий підхід дозволяє отримати точніші результати та зменшує вплив людської помилки на процес управління ризиками. Далі детально описано основні етапи реалізації гібридного методу.

Схематичне зображення гібридного методу управління ризиками. Гібридний метод управління ризиками включає три основні етапи: організаційний етап, етап аналізу ризиків і етап управління ризиками. Він базується на міжнародних стандартах ISO 31000 та ISO/IEC 27005, які регламентують управління корпоративними й інформаційними ризиками відповідно. Основною метою методу є надання комплексної оцінки ризику, яка охоплює і бізнес, і аспекти інформаційної безпеки (ISO/IEC 27005, 2018).

На рис. 1 зображено загальну структуру гібридного методу управління ризиками, що демонструє три основні етапи: організаційний, етап аналізу ризиків і етап управління ризиками. Кожен із цих етапів виконує конкретні завдання, спрямовані на ідентифікацію, оцінювання та мінімізацію ризиків.

ISSN 2707-1758

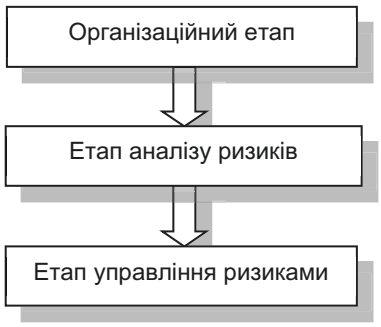

Рис. 1. Етапи гібридного метод управління ризиками

Рисунок 2 відображає перший етап гібридного методу управління ризиками – організаційний етап, який охоплює процес збору даних для їх подальшого аналізу. Подвійні лінії на схемі означають паралельність кроків або групування даних.

На цьому етапі ідентифікація активів організації виконується за методологією OCTAVE, що передбачає класифікацію активів за такими критеріями (OCTAVE, 2003):

1. **Матеріальні активи**: фізичні об'єкти, такі як будівлі, обладнання, інвентар, що мають цінність для організації.
2. **Нематеріальні активи**: нефізичні об'єкти, зокрема й інтелектуальна власність, дані про клієнтів, бізнес-процеси.
3. **Інформаційні активи**: дані або інформація, які мають цінність, наприклад, фінансові звіти, списки клієнтів, комерційні таємниці.
4. **Активи, що стосуються персоналу**: знання, навички та досвід працівників, які виконують критичні функції в організації.
5. **Активи інфраструктури**: IT-системи, мережі, інші технологічні компоненти організації.

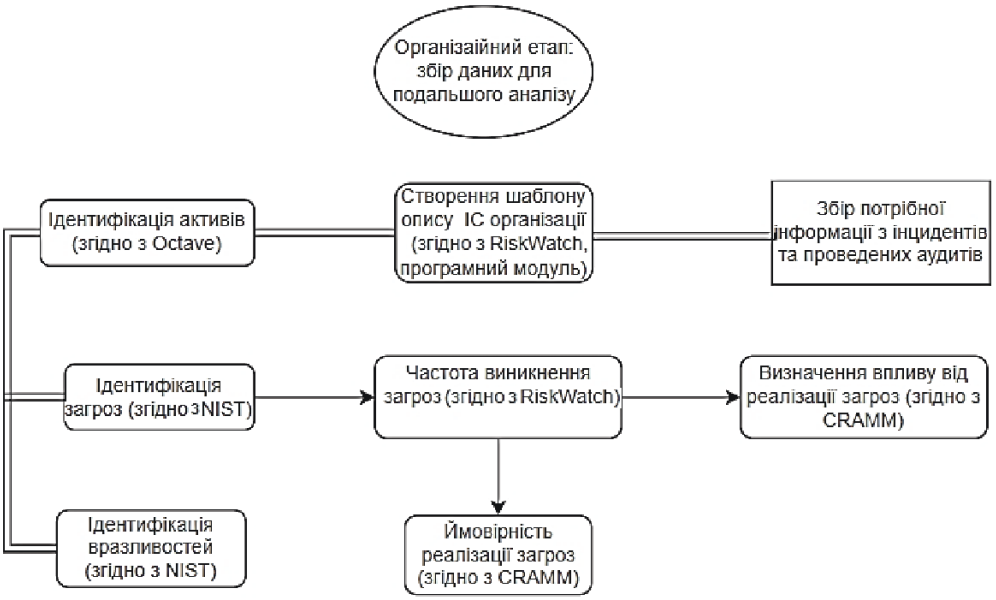

Рис. 2. Перший етап гібридного методу управління ризиками

Після ідентифікації активів за методологією OCTAVE, критичність кожного активу оцінюють для визначення необхідного рівня захисту. Це допомагає організації визначити пріоритети щодо ресурсів для ефективнішого управління ризиками.

Методологія NIST визначає п'ять категорій загроз, які включають природні ризики, людський фактор, екологічні загрози, кіберзагрози та ризики ланцюгів постачання. Усі ці загрози оцінюють з урахуванням їхнього потенційного впливу на бізнес-діяльність і репутацію організації.

Метод NIST 800-30 використовують для ідентифікації вразливостей у системах. Він є універсальним і підходить для організацій будь-якого розміру. Для кожної інформаційної системи застосовують шаблон опису, що містить дані про власника системи, її призначення та масштаб.

За допомогою методів Risk Watch і CRAMM визначають частоту виникнення загроз, ступінь уразливості та цінність активів, на основі чого розраховують ефективність засобів захисту.

Метод CRAMM оцінює ймовірність реалізації загроз за шкалою від 1 до 5. Оцінювання впливу загроз також проводять за шкалою від 1 до 5, залежно від потенційних наслідків для бізнесу.

Другий етап гібридного методу управління ризиками (рис. 3) включає аналіз ризиків на основі зібраних даних. Важливі ризики оцінюють якісно і кількісно, а менш критичні – ігнорують для економії ресурсів.

ISSN 2707-1758

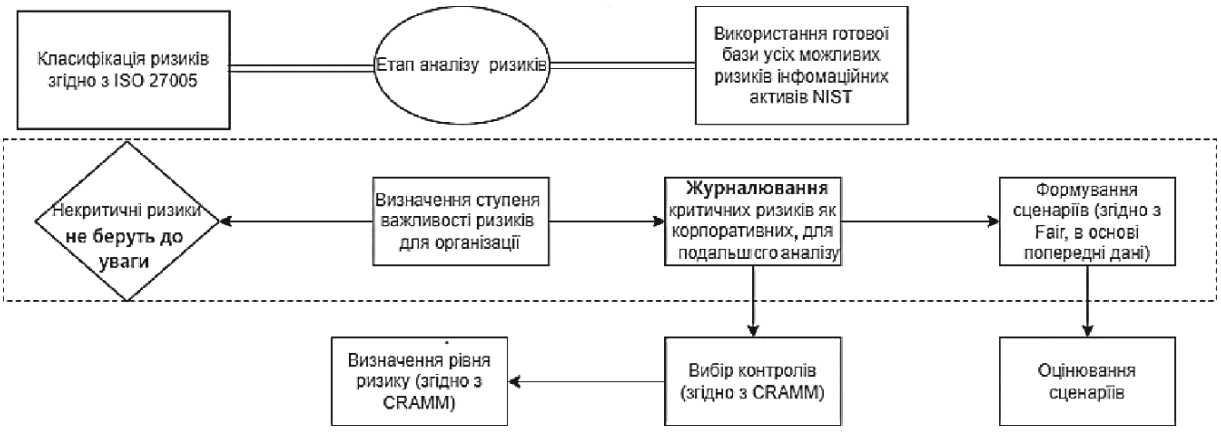

Рис. 3. Другий етап гібридного методу управління ризиками

Для збереження ресурсів і часу спеціалістів автори пропонують не обробляти ризики з низьким рівнем критичності, концентруючись лише на значущих загрозах для бізнесу. Оброблення таких ризиків включає поєднання якісних і кількісних методів їхнього оцінювання, що вимагає реєстрації у базі корпоративних ризиків через їхній вплив на безперервність бізнес-процесів та інформаційних систем.

Стандарт ISO 27005 пропонує класифікацію ризиків за чотирма рівнями: від дуже низького до високого. Ця класифікація використовується в процесі управління ризиками і допомагає організаціям ефективно розставляти пріоритети щодо потенційних загроз.

Метод FAIR передбачає використання сценаріїв ризиків для детального опису загроз і оцінки їхньої ймовірності та потенційного впливу на активи організації. Це дозволяє приймати обґрунтовані рішення та знижувати загальний рівень ризиків.

Метод CRAMM забезпечує вибір та оцінку контролів для пом'якшення виявлених ризиків, що включає перегляд існуючих засобів контролю, впровадження нових та регулярний моніторинг їхньої ефективності.

На третьому етапі гібридного методу управління ризиками (рис. 4) відбувається кількісна оцінка збитків та генерація звітів, що допомагає організації розподіляти ресурси та зменшувати вплив ризиків на бізнес.

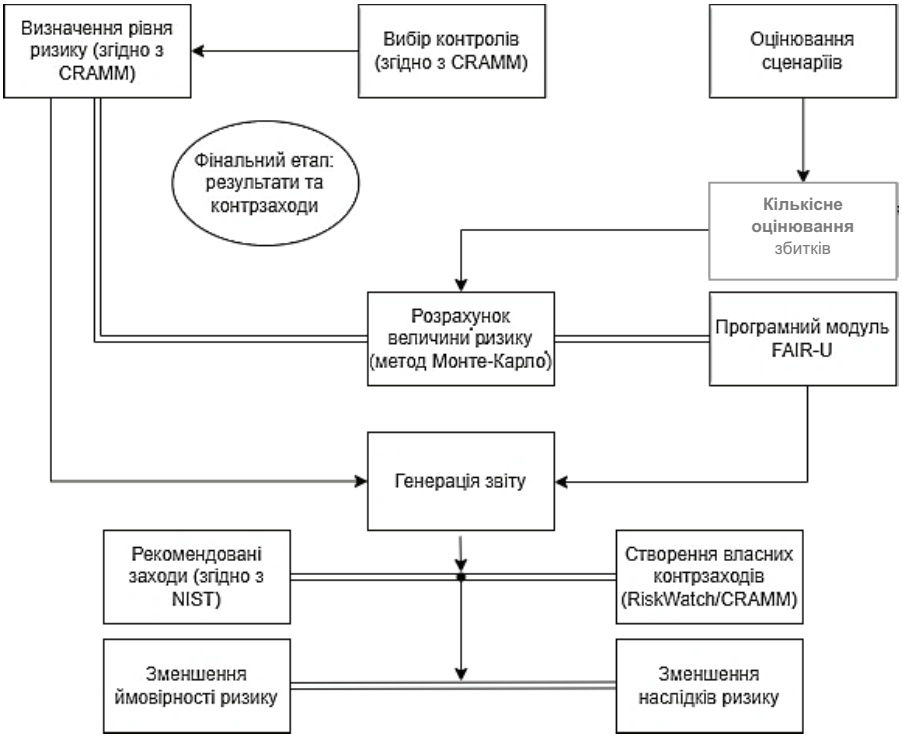

Рис. 4. Третій етап гібридного методу управління ризиками

Кількісне оцінювання збитків є важливим етапом, оскільки дозволяє організації правильно розподілити ресурси та зосередити увагу на більш критичних ризиках. Моделювання за методом Монте-Карло дає реалістичну оцінку ризиків і допомагає у прийнятті рішень. Метод FAIR-U спрощує налаштування моделювання сценаріїв ризику, забезпечуючи точні результати для прийняття рішень.

NIST 800-53 надає комплекс заходів безпеки, що включають рекомендації для впровадження контролів.

ISSN 2707-1758

Організації можуть використовувати методи Risk Watch або CRAMM для впровадження власних контрзаходів.

Існують три типи контролів: превентивні (запобігання ризику, напр., контроль доступу), детективні (виявлення ризиків після їхнього виникнення, як-от системи виявлення вторгнень), і коригувальні (мінімізація наслідків, як-от резервне копіювання даних).

Регулярний перегляд і оновлення процесу управління ризиками є важливим для збереження ефективності контролів і виявлення нових *ризиків*.

Якісне оцінювання ризиків згідно з CRAMM у гібридному методі управління ризиками. Якісне оцінювання ризиків є важливим етапом у CRAMM, що дозволяє виявити й оцінити потенційні загрози для інформаційної безпеки (Major, 1995). Процес містить такі кроки:

1. **Визначення активів**: включають IT-інфраструктуру, конфіденційні дані та персонал із доступом до цих ресурсів.
2. **Визначення загроз**: зокрема, атаки шкідливих програм, фішингові атаки, інсайдерські загрози, перебої в електропостачанні, стихійні лиха.
3. **Виявлення вразливостей**: наприклад, застаріле програмне забезпечення, слабка політика паролів, відсутність контролю доступу, недостатнє навчання працівників.
4. **Оцінювання впливу та ймовірності ризиків**: проводиться на основі табл. 2.

Таблиця 2

Якісне оцінювання ризиків

Ризик	Оцінка впливу	Імовірність
Атаки шкідливих програм	Висока	Середня
Фішингові атаки	Середня	Висока
Внутрішні загрози	Висока	Середня
Перебої в електропостачанні	Висока	Низька
Стихійні лиха	Висока	Низька

5. **Пріоритетність ризиків**: на основі оцінки впливу та ймовірності ризики класифікують за пріоритетністю.
6. **Визначення заходів** для зменшення ризиків, включаючи встановлення антивірусного ПЗ, контроль доступу, навчання співробітників, резервування даних, підготовка до стихійних лих тощо.
7. **Контроль ефективності заходів**: регулярне оцінювання й оновлення заходів для підтримання актуальності й ефективності.

Для підвищення точності кількісної оцінки ризиків у гібридних методах важливо використовувати математичні моделі, що дозволяють моделювати ймовірності виникнення загроз і їхні потенційні наслідки. Причому особливу увагу варто приділити оцінці фінансового впливу ризиків, яка є ключовим аспектом таких методів. В представленому дослідженні розглянуто застосування формул у кількісних підходах, зокрема в методах FAIR і Монте-Карло, для аналізу та прогнозування ризиків.

Оцінювання фінансових втрат (FAIR). Модель FAIR дозволяє оцінити фінансовий вплив ризику на основі двох основних компонентів: імовірності реалізації ризику та середніх втрат.

Формула загальних втрат:

$$L_{total} = P \times (L_p + L_s), \quad (1)$$

де L_{total} – загальні фінансові втрати; P – імовірність реалізації ризику (від 0 до 1); L_p – середні прямі втрати (напр., вартість відновлення системи); L_s – середні непрямі втрати (репутаційні збитки, штрафи тощо).

Наведемо приклад розрахунку:

1. Імовірність реалізації ризику (P) = 0.25.
2. Прямі втрати (L_p) = \$500,000.
3. Непрямі втрати (L_s) = \$200,000.

$$L_{total} = 0.25 \times (500{,}000 + 200{,}000) = 0.25 \times 700{,}000 = 175{,}000.$$

Отже, прогнозовані фінансові втрати становлять \$175,000.

Симуляція за методом Монте-Карло. Вказаний метод Монте-Карло використовують для моделювання сценаріїв ризиків з урахуванням невизначеності (Кравченко, Трощинський, & Іванов, 2022). Цей підхід дозволяє оцінити можливі наслідки ризиків шляхом багаторазової симуляції із використанням випадкових значень, що генеруються в межах визначених діапазонів. Таким способом метод Монте-Карло забезпечує точні прогнози, дозволяючи організаціям оцінювати потенційні втрати та ймовірність виникнення критичних подій. Основні розрахунки базуються на визначенні середнього значення втрат і стандартного відхилення для аналізу варіативності результатів.

Формула середнього значення втрат:

$$L_{avg} = \frac{\sum_{i=1}^{n} L_i}{n}, \quad (2)$$

де L_{avg} – середнє значення втрат після симуляції; L_i – втрати для ітерації *iii*; n – кількість ітерацій.

Формула стандартного відхилення:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (L_i - Lavg)}{n}}^2, \quad (3)$$

де σ – стандартне відхилення втрат.

Наведемо приклад розрахунку:

1. Проведено 5 симуляцій:

L_1 = 150,000, L_2 = 180,000, L_3 = 200,000, L_4 = 170,000, L_5 = 160,000.

Середнє значення втрат шукаємо за формулою (2):

$$Lavg = \frac{150{,}000+180{,}000+200{,}000+170{,}000+160{,}000}{5} = \frac{860{,}000}{5} = 172{,}000.$$

Стандартне відхилення шукаємо за формулою (3):

$$\sigma = \sqrt{\frac{(150.000-172.000)^2+(180{,}000-172{,}000)^2+(200{,}000-172{,}000)^2+(170{,}000-172{,}000)^2+(160{,}000-172{,}000)^2}{5}}$$

ISSN 2707-1758

$$\sigma = \sqrt{\frac{(-22{,}000)^2 + (8{,}000)^2 + (28{,}000)^2 + (-2{,}000)^2 + (-12{,}000)^2}{5}} \approx 17{,}205.$$

Симуляція показує, що середні втрати становлять $172,000, а стандартне відхилення $17,205.

Ефективність заходів безпеки оцінюють за формулою (4). Для оцінювання впливу заходів безпеки можна використовувати коефіцієнт ефективності:

$$E = \frac{Lunmitigated - Lmitigated}{Lunmitigated}, \quad (4)$$

де E – ефективність заходів безпеки (у відсотках); $L_{unmitigated}$ – втрати без впровадження заходів; $L_{mitigated}$ – втрати після впровадження заходів.

Наведемо приклад:

1. Втрати без заходів $L_{unmitigated}$ = $700,000.
2. Втрати після заходів $L_{mitigated}$ = $300,000.

$$E = \frac{700{,}000 - 300{,}000}{700{,}000} = \frac{400{,}000}{700{,}000} \approx 0{,}57\ (57\ \%).$$

Заходи безпеки дозволяють знизити ризик на 57 %.

Використання математичних формул у гібридних методах оцінювання ризиків забезпечує точність і прозорість аналізу. Це дає змогу організаціям не лише оцінити ймовірність реалізації ризиків і їхній фінансовий вплив, а й порівняти ефективність різних заходів безпеки. Такий підхід сприяє ухваленню обґрунтованих рішень, орієнтованих на мінімізацію втрат і раціональне використання ресурсів.

Переваги та обмеження. Метод Монте-Карло дозволяє отримати більш точні та реалістичні оцінки ризику, однак його результати залежать від точності визначених змінних та вибору розподілу ймовірностей. Важливо правильно задати ці параметри для отримання коректних результатів.

Ефективність гібридного методу. Оцінювання ефективності запропонованого гібридного методу управління ризиками на цьому етапі є переважно теоретичним, оскільки метод був сформований на базі найкращих галузевих практик і міжнародних стандартів. Кількісне оцінювання його ефективності викликає певні труднощі, але можна застосувати ряд загально-прийнятих підходів для оцінювання (Богданова, & Петренко, 2019; Бучик, Шалаєв, & Мельник, 2017).

Для візуального представлення ефективності гібридного методу розглянемо ключові аспекти зниження ризиків і фінансових втрат.

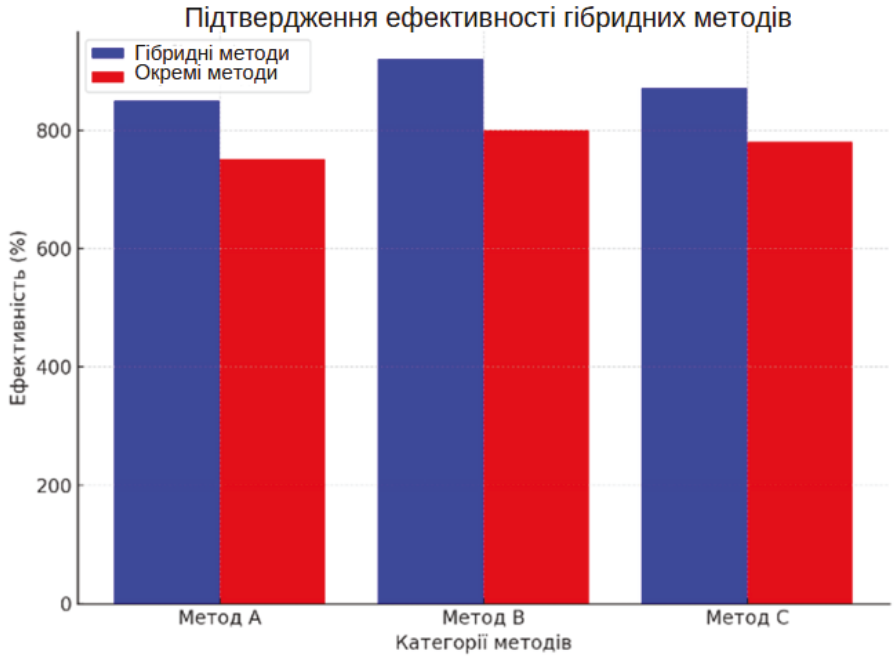

Рис. 5. Діаграма підтвердження якості гібридних методів

Ця діаграма ілюструє ефективність гібридних методів оцінювання ризиків, застосованих для захисту корпоративних систем в інформаційній безпеці. Вона відображає три ключові аспекти.

Поточний рівень ризику – це рівень загроз і ризиків, який залишається незмінним без упровадження гібридних методів. Він характеризує ситуацію до застосування відповідних технологій оцінювання й управління ризиками.

Зниження ризику після застосування гібридних методів показує, наскільки інтегрований підхід, що поєднує якісні та кількісні методи аналізу разом із сучасними технологіями штучного інтелекту, сприяє мінімізації ризиків.

Загальні фінансові втрати демонструють співвідношення між витратами на реалізацію гібридних методів і можливими втратами, яких вдалося уникнути завдяки їхньому застосуванню. Цей показник є ключовим для оцінювання економічної доцільності таких методів.

Діаграма на рис. 5 підтверджує, що використання гібридних підходів значно зменшує ризики та знижує ймовірність критичних інцидентів у корпоративних інформаційних системах. Її структура дозволяє оцінити динаміку змін (напр., у відсотковому зниженні ризику) і сформулювати рекомендації щодо подальшого впровадження цих технологій у реальних умовах.

ISSN 2707-1758

Алгоритм оцінювання ефективності гібридного методу

1. **Детальне вивчення методу** – необхідно провести аналіз ключових компонентів методу, визначити припущення та цілі.
2. **Визначення критеріїв оцінювання** – створення критеріїв, за якими можливо оцінити метод, наприклад: здатність ідентифікувати ризики, масштабованість та ефективність у зменшенні ризиків.
3. **Аналіз зібраних даних** – вивчення результатів оцінювання ризиків, зібраних із реальних прикладів, для виявлення закономірностей і тенденцій.
4. **Порівняння з існуючими методиками** – для визначення, як гібридний метод співвідноситься з іншими моделями управління ризиками.
5. **Коригування методу** – на основі аналізу результатів для підвищення ефективності методу, для детальнішого оцінювання ефективності методу важливо застосувати набір критеріїв, що дозволяють об'єктивно визначити його переваги та недоліки.

Критерії оцінювання ефективності гібридного методу:

1. Відповідність найкращим галузевим практикам.
2. Відповідність міжнародним стандартам.
3. Структурованість методу.
4. Визначення власника ризиків і відповідальних осіб.
5. Налагодженість комунікації між учасниками процесу.
6. Ідентифікація загроз, вразливостей та активів.
7. Якісне та кількісне оцінювання ризиків.
8. Оброблення результатів і впровадження контролів.
9. Зменшення ризиків і пом'якшення їхніх наслідків.
10. Витрати часу та вартість рішення.
11. Структурованість підходу та можливість автоматизації.
12. Адаптивність і легкість налаштування методу.
13. Потреба в навчанні персоналу.

Щоб оцінити ефективність гібридного методу управління ризиками, сформовано таблицю із зазначеними критеріями.

Таблиця 3

Відповідність критеріям для оцінювання ефективності гібридного методу

Критерій	Відповідність
Відповідність передовим галузевим практикам	Гібридний метод відповідає сучасним галузевим стандартам і використовує деякі з них у своєму процесі
Відповідність міжнародним стандартам	Оброблення ризиків підпорядковується двом міжнародним стандартам: ISO 31000, що регламентує процес управління корпоративними ризиками, та ISO/IEC 27005, який стосується управління ризиками інформаційної безпеки
Основи методу	Метод заснований на аналізі переваг та обмежень існуючих методів оцінювання ризиків
Визначення власника ризиків і відповідальних осіб	Власник ризиків – спеціаліст з інформаційної безпеки; учасники процесу чітко визначені
Комунікація між учасниками процесу	У процесі беруть активну участь три сторони: інформаційна безпека, бізнес і корпоративний ризик-менеджмент, що сприяє прийняттю спільних рішень
Ідентифікація загроз	Цей етап виконується відповідно до методики
Ідентифікація вразливостей	Етап ідентифікації вразливостей виконується згідно з вимогами методики
Ідентифікація активів	Вказаний етап відповідає вимогам методики
Якісне оцінювання ризиків	Ризики оцінюють якісно згідно з CRAMM
Кількісне оцінювання ризиків	Ризики оцінюють кількісно за допомогою методів FAIR-U та Монте-Карло
Оброблення результатів	Зібрані дані та їхній аналіз формують основні результати оброблення ризиків
Робота та впровадження контролів	Вибір і впровадження засобів контролю регламентують методом CRAMM
Формування звітів	Звіти формують за допомогою програмних інструментів та за участі спеціалістів
Зменшення ризиків і пом'якшення наслідків	Ці етапи є частиною гібридного методу
Часові витрати на оброблення ризиків	Автоматизація та вибір критичних ризиків зменшує часові витрати на оброблення
Вартість рішення	Рішення є відносно доступним, оскільки можна вибирати необхідні етапи для впровадження
Фокус на критичні ризики	Метод орієнтований на роботу з найкритичнішими ризиками
Структурованість підходу	Підхід до управління ризиками має чітко визначену структуру
Можливість автоматизації	Процес частково автоматизований, і передбачено можливість подальшого вдосконалення
Адаптивність	Метод повністю адаптується під потреби організації
Комплексність	Метод охоплює всі основні етапи процесу управління ризиками

ISSN 2707-1758

Беручи до уваги всі критерії, обрані для оцінювання ефективності методу, можна зробити висновок, що гібридний метод управління ризиками є результативним і безперервним процесом. Він легко підлаштовується під потреби організації та демонструє високу гнучкість для подальшого вдосконалення. Таким способом гібридний метод забезпечує структурований підхід до управління ризиками, який можна адаптувати до специфічних потреб практично довільної за масштабом і формою власності організації.

Дискусія і висновки

У цій статті розглянуто питання управління ризиками в інформаційній безпеці за допомогою гібридних методів, які поєднують як кількісні, так і якісні підходи до оцінювання ризиків. Проведений аналіз існуючих методів, таких як CRAMM, Монте-Карло, NIST 800-30, FAIR та інших, виявив, що жоден із них не може повністю задовольнити потреби організацій, що працюють у складному та швидкозмінному цифровому середовищі. Кількісні методи забезпечують точні результати, але потребують значної кількості даних, у той час як якісні підходи дають можливість врахувати специфічні фактори, але залежать від суб'єктивних оцінок.

Запропонований гібридний метод управління ризиками дозволяє усунути вказані недоліки, поєднуючи кращі сторони обох підходів. Він базується на структурованому процесі, що включає три ключові етапи: організаційний, аналізу ризиків та управління ризиками. Організаційний етап охоплює ідентифікацію активів і загроз, що відповідає методології OCTAVE, а також інструментам NIST і Risk Watch. Другий етап – аналіз ризиків – інтегрує кількісні оцінки за методом Монте-Карло та якісні оцінки за CRAMM, що дозволяє зосередитися на критичних ризиках і раціонально використовувати ресурси. Третій етап спрямований на управління ризиками шляхом упровадження контролів та зменшення їхнього впливу, що забезпечується використанням автоматизованих рішень і постійного моніторингу.

Приклад симуляції за методом Монте-Карло показав, що середнє значення потенційних втрат становить $172,000, а стандартне відхилення – $17,888, що дало змогу спрямувати ресурси на усунення найкритичніших ризиків із високою ймовірністю реалізації.

Використання математичних моделей, таких як FAIR і Монте-Карло, підвищує точність оцінок, зменшує суб'єктивність і покращує процес прийняття рішень, особливо у сфері фінансового аналізу ризиків. Завдяки цьому організації можуть не лише оцінити ймовірність ризиків і їхній фінансовий вплив, а й оптимізувати розподіл ресурсів.

Подальші дослідження можуть зосередитися на інтеграції методів машинного навчання для автоматизації ризик-менеджменту, а також на розробленні рішень для динамічної адаптації під змінні сценарії загроз.

Загалом, гібридний метод управління ризиками демонструє свою ефективність як гнучкий і універсальний інструмент, що може бути адаптований до специфічних потреб організацій різного масштабу.

Внесок авторів: Володимир Наконечний – наукове керівництво, узгодження методології дослідження, рецензування статті; Микола Мордвинцев – формальний аналіз, наукове рецензування, валідація; Вікторія Гусєва – аналіз літературних джерел, математичне моделювання за методами FAIR і Монте-Карло, підготовка висновків, редагування тексту статті, підготовка графічного матеріалу та таблиць; Владислав Луценко – розроблення гібридного методу управління ризиками, проведення якісного оцінювання ризиків за методологією CRAMM, розробка алгоритму оцінки ефективності запропонованого методу.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Богданова, О. В., & Петренко, О. І. (2019). Якісна оцінка ефективності процесу управління ризиками в інформаційній безпеці. *Наукові праці Національного університету цивільного захисту України*, 2(78), 31–37.

Бучик, С. С., Шалаєв, В. О., & Мельник, С. В. (2017). Методика оцінювання інформаційних ризиків в автоматизованій системі. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, 11, 33–43. http://nbuv.gov.ua/UJRN/Psvz_2015_11_6

Кравченко, О. М., Трощинський, І. В., & Іванов, О. В. (2022). Застосування методу Монте-Карло для оцінки ризиків в інформаційній безпеці. *Наукові записки ТНТУ ім. Івана Пулюя. Серія: Інформаційні технології та комп'ютерна інженерія*, 1(88), 45–52.

Юдін, О. К., & Бучик, С. С. (2015). *Державні інформаційні ресурси. Методологія побудови класифікатора загроз*. НАУ.

COBRA (Cloud Offensive Breach and Risk Assessment). (n. d.). *Introduction to Security Risk Analysis*. https://github.com/PaloAlto/Networks/cobra-tool

FAIR Institute. (2022). *Factor Analysis of Information Risk (FAIR) – The FAIR Standard*. https://www.fairinstitute.org/what-is-fair

Graham, J. B. (2014). *Effective Risk Management for Cybersecurity and Information Technology*. Auerbach Publications.

ISO/IEC 27005:2022. (2022). *Information Technology – Security Techniques – Information Security Risk Management*. https://www.iso.org/standard/80585.html

Major, M. (1995). *A Practical Guide to the CRAMM Methodology*. McGraw-Hill Book Company.

McCumber, J. (2011). *Risk Management in Information Security*. SANS Institute.

NIST (National Institute of Standards and Technology). (2012). *Guide for Conducting Risk Assessments*. Special Publication 800-30 Rev. 1. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

OCTAVE (2003). *Methodology for Information Risk Assessment.* https://www.itgovernance.co.uk/files/Octave.pdf

RiskWatch International. (n. d.). *The RiskWatch Advantage – Risk Assessment Software*. https://www.riskwatch.com/

Wheeler, E. (2014). *Information Security Risk Management: Frameworks, Metrics, and Best Practices*. Apress.

Wheeler, E. (2015). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Syngress.

References

Bogdanova, O. V., & Petrenko, O. I. (2019). Qualitative assessment of the effectiveness of risk management in information security. *Scientific Papers of the National University of Civil Protection of Ukraine*, 2(78), 31–37 [in Ukrainian].

Buchyk, S. S., Shalayev, V. O., & Melnyk, S. V. (2017). Methodology for assessing information risks in automated systems. *Problems of Creation, Testing, Application and Operation of Complex Information Systems*, 11, 33–43 [in Ukrainian]. http://nbuv.gov.ua/UJRN/Psvz_2015_11_6

COBRA (Cloud Offensive Breach and Risk Assessment). (n. d.). *Introduction to Security Risk Analysis*. https://github.com/PaloAlto/Networks/cobra-tool

FAIR Institute. (2022). *Factor Analysis of Information Risk (FAIR) – The FAIR Standard*. https://www.fairinstitute.org/what-is-fair

Graham, J. B. (2014). *Effective Risk Management for Cybersecurity and Information Technology*. Auerbach Publications.

ISO/IEC 27005:2022. (2022). *Information technology – Security techniques – Information security risk management*. https://www.iso.org/standard/80585.html

Kravchenko, O. M., Troshchynskyi, I. V., & Ivanov, O. V. (2022). Application of the Monte Carlo method for risk assessment in information security. *Scientific Notes of Ternopil Ivan Puluj National Technical University. Series: Information Technologies and Computer Engineering*, 1(88), 45–52 [in Ukrainian].

Major, M. (1995). *A Practical Guide to the CRAMM Methodology*. McGraw-Hill Book Company.

McCumber, J. (2011). *Risk Management in Information Security*. SANS Institute.

NIST (National Institute of Standards and Technology). (2012). *Guide for Conducting Risk Assessments*. Special Publication 800-30 Rev. 1. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

OCTAVE (2003). *Methodology for Information Risk Assessment.* https://www.itgovernance.co.uk/files/Octave.pdf

ISSN 2707-1758

RiskWatch International. (n. d.). *The RiskWatch Advantage – Risk Assessment Software*. https://www.riskwatch.com/risk-assessment-software/

Wheeler, E. (2014). *Information Security Risk Management: Frameworks, Metrics, and Best Practices*. Apress.

Wheeler, E. (2015). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Syngress.

Yudin, O. K., & Buchyk, S. S. (2015). *State information resources. Methodology for building a threat classifier.* NAU [in Ukrainian]. http://er.nau.edu.ua/handle/NAU/31911

Отримано редакцією журналу / Received: 17.05.25
Прорецензовано / Revised: 16.06.25
Схвалено до друку / Accepted: 22.06.25

Volodymyr NAKONECHNYI, DSc (Engin.), Prof.
ORCID ID: 0000-0002-0247-5400
e-mail: nakonechnyiv@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola MORDVYNTSEV, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7674-3164
e-mail: pestalocyj@gmail.com
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine

Viktoriia HUSIEVA, Student
ORCID ID: 0009-0002-1120-1900
e-mail: husievav@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Vladyslav LUTSENKO, PhD Student
ORCID ID: 0000-0002-2377-1858
e-mail: vladyslav.lutsenko99@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

HYBRID APPROACH TO INFORMATION SECURITY RISK MANAGEMENT

Background. ***The article explores a hybrid approach to information security risk management that combines quantitative and qualitative risk assessment methods. This approach improves accuracy, reduces subjective judgments, and enables the automation of the risk management process. The relevance of the topic is driven by the continuous increase in the number and complexity of cyber threats, which require the development and implementation of effective tools for risk management and mitigation of human factor impact.***

Methods. ***An integrated approach was applied, based on the FAIR and Monte Carlo methods for quantitative probability assessment, and CRAMM for qualitative risk analysis. International standards ISO 31000 and ISO/IEC 27005, which regulate risk management, were taken into account. Asset identification, vulnerability assessment, and threat classification were carried out according to the best practices of information security. The methodology for developing a risk assessment model that considers various levels of potential threats was substantiated.***

Results. ***The results confirmed the adequacy and effectiveness of the hybrid approach. The proposed model allowed for the identification of critical assets, risk level assessment, and the development of recommendations for implementing countermeasures. The Monte Carlo method was used to estimate the probability of successful attacks and calculate potential losses. CRAMM analysis helped identify system vulnerabilities and propose appropriate security measures. A comparative analysis of traditional risk assessment methods showed the advantages of the integrated approach in a dynamic information environment.***

Conclusions. ***The proposed hybrid approach contributes to minimizing human factor influence, improving assessment accuracy, and automating risk management. This will optimize organizational resources and support strategic information protection planning. Further research may focus on developing automation tools to integrate the proposed approach into real information systems. It is recommended to continue developing the methodology to adapt it to different threat scenarios within organizations with diverse security profiles.***

Keywords: ***information security, risk management, Monte Carlo, CRAMM, threat assessment, cybersecurity.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

ISSN 2707-1758