Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Дослідження методів та засобів оцінки ризиків інформаційної безпеки
(назва теми)

Виконав: студент 2 курсу, групи БКз-812м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних мереж
КОЦЮРУБА Р.Б.
(ПРІЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.
(ПРІЗВИЩЕ та ініціали)

Рецензент НІКУЛІЩЕВ Г.І.
(ПРІЗВИЩЕ та ініціали)

2023

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
Андрій КОРОТУН
«____» _____2023року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

КОЦЮРУБИ Руслана Борисовича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження методів та засобів оцінки ризиків інформаційної безпеки
Investigation of methods and tools of information security risk assessment

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 476
2. Строк подання студентом проєкту (роботи) 11.12.2023
3. Вихідні дані до проєкту (роботи) Проаналізувати міжнародні та національні стандарти в сфері управління ризиками інформаційної безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Міжнародні стандарти оцінки ризиків інформаційної безпеки; Національні стандарти оцінки ризиків інформаційної безпеки; Засоби аналізу та оцінки інформаційних ризиків; Моделювання процесів управління ризиками в середовищі CORAS.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), ___слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання «04» вересня 2023року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	Виконано
2.	Огляд стандартів ISO/IEC.	19.09.23 – 04.10.23	Виконано
3.	Дослідження стандартів NIST-800, BS 7799, AS/NZS 4360.	05.10.23 – 18.10.23	Виконано
4.	Аналіз методів оцінки ризиків інформаційної безпеки	19.10.23 – 02.11.23	Виконано
5.	Дослідження засобів оцінки ризиків інформаційної безпеки	03.11.23 – 20.11.23	Виконано
6.	Моделювання управління ризиками в середовищі CORAS	21.11.23 – 30.11.23	Виконано
7.	Оформлення матеріалів магістерської роботи.	01.12.23 – 05.12.23	Виконано

Студент _____ Руслан КОЦЮРУБА
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 98 с., 7 табл., 29 рис., 3 дод., 48 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАСОБИ БЕЗПЕКИ, ОЦІНКА РИЗИКІВ, РИЗИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СТАНДАРТ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Актуальність теми. Незважаючи на збільшення інвестицій в заходи з кібербезпеки, такі інциденти, як витік даних, зараження шкідливим програмним забезпеченням та кібератаки на урядові та комерційні організації, демонструють тенденцію до зростання. Реагування на кіберінциденти повинно бути вчасним і ефективним, а це не можливо виконати без постійного перегляду та вдосконалення систем управління та оцінки рівня ризиків інформаційної безпеки.

Мета роботи:

– дослідити нормативну базу в сфері аналізу та оцінки ризиків інформаційної безпеки з урахуванням міжнародних та національних стандартів ;

– провести порівняльний аналіз сучасних програмних засобів оцінки інформаційних ризиків.

Об’єкт дослідження – стандарти та засоби аналізу та оцінки ризиків інформаційної безпеки.

Предмет дослідження – методи ідентифікації, оцінки та обробки інформаційних ризиків та програмні засоби, які розроблені на їх основі.

Методи дослідження: порівняльний аналіз, формалізація, системний підхід.

Задачі дослідження:

– провести дослідження керівних документів щодо управління та оцінки ризиків інформаційної безпеки з урахуванням вимог та рекомендацій міжнародних та національних стандартів в сфері ризик-менеджменту;

– провести порівняльний аналіз методів та засобів управління та оцінки інформаційних ризиків;

– на основі проведеного аналізу програмних засобів провести моделювання процесів управління та оцінки ризиками.

Практичне значення одержаних результатів. Результати проведеного дослідження можуть бути використані фахівцями з ризик-менеджменту під створення підсистеми управління ризиками в рамках комплексної системи захисту інформації.

Апробація результатів. Прийнято участь у Міжнародній науково-практичній конференції «Кібербезпека в Україні: правові та організаційні питання», Одеський державний університет внутрішніх справ, 17 листопада 2023 р., м. Одеса. Доповідь на тему: «Огляд стандартів управління та оцінки ризиків інформаційної безпеки».

ABSTRACT

Explanatory note to the master's thesis: 98 pages, 7 tables, 29 figures, 3 app., 48 sources.

INFORMATION SECURITY, SECURITY MEASURES, RISK ASSESSMENT, INFORMATION SECURITY RISK, STANDARD, INFORMATION SECURITY MANAGEMENT

Actuality of theme. Despite increased investment in cybersecurity measures, incidents such as data breaches, malware infections, and cyberattacks on government and commercial organizations are on the rise. Responding to cyber incidents must be timely and effective, and this cannot be done without constant review and improvement of management systems and assessment of the level of information security risks.

The purpose of the work is:

– research the regulatory framework in the field of information security risk analysis and assessment, taking into account international and national standards;

– perform a comparative analysis of modern software tools for assessing information risks.

The object of research is standards and tools for analyzing and evaluating information security risks.

The subject of the study is methods of identification, assessment and processing of information risks and software tools developed on their basis.

Research methods: comparative analysis, formalization, systematic approach.

Research objectives:

– to conduct a study of the guiding documents on the management and assessment of information security risks, taking into account the requirements and

recommendations of international and national standards in the field of risk management;

– perform a comparative analysis of methods and means of information risk management and assessment;

– on the basis of the analysis of software tools, carry out modeling of risk management and assessment processes.

Practical significance of the obtained results. The results of the study can be used by risk management specialists to create a risk management subsystem within the framework of a comprehensive information security system.

Approbation of the results. Participation in the International Scientific and Practical Conference "Cybersecurity in Ukraine: Legal and Organizational Issues", Odesa State University of Internal Affairs, November 17, 2023, Odesa. Report on the topic: "Review of information security risk management and assessment standards".

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БМ – байєсівські мережі;

ІБ – інформаційна безпеки;

ІТ – інформаційні технології

СУІБ/СМІБ – системи управління (менеджменту) інформаційною безпекою;

AS/NZS – Австралійський/Новозеландський стандарт (The Australian/New Zeeland Standard for Risk Management);

BS – британський стандарт (British Standards);

BSI – британський інститут стандартів (British Standards Institution);

CCTA – Центральне агентство зв’язку та телекомунікацій (Central Communication and Telecommunication Agency);

CORAS – система консультативного об’єктивного аналізу ризиків (Consultative Objective Risk Analysis System);

CRAMM – Метод аналізу та управління ризиками (Risk Analysis and Management Method);

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія);

IPL – незалежні рівні захисту (independent protection layers);

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації);

ISMS – система управління інформаційною безпекою (information security management system);

ISRA – часовий та об’єктно-орієнтований метод (information security risk assessment);

MBRA – методологія оцінки ризику на основі моделі (model-based risk assessment).

NIST – національний інститут стандартів і технологій (National Institute of Standards and Technology);

OCTAVE – операційно критична оцінка загроз, активів і вразливостей (The Operationally Critical Threat, Asset, and Vulnerability Evaluation);

PDCA – планування (Plan) – Виконання (Do) – Перевірка (Check) – Вплив/Управління/Коригування (Act);

RMF – платформа управління ризиками (risk management framework);

SIL – рівень цілісності безпеки (safety integrity levels);

SP – спеціальна публікація (special publication);

UML – уніфікована мова моделювання (Unified modeling language).

ВСТУП

Незважаючи на збільшення інвестицій в заходи з кібербезпеки, такі інциденти, як витік даних, зараження шкідливим програмним забезпеченням та кібератаки на урядові та комерційні організації, демонструють тенденцію до зростання.

Реагування на кіберінциденти повинно бути вчасним і ефективним, а це не можливо виконати без постійного перегляду та вдосконалення систем управління та оцінки рівня ризиків інформаційної безпеки.

Ризик-менеджмент – це безперервний процес, який включає ідентифікацію, аналіз і реагування на фактори ризику з акцентом на контроль майбутніх результатів шляхом вжиття відповідних (адекватних) заходів.

Система управління ризиками повинна гарантувати наявність достатніх ресурсів, виділених для усунення будь-яких можливостей, пов’язаних з ризиком. Ефективне управління ризиками забезпечує можливість зменшити як можливість виникнення ризику, так і його потенційний вплив.

Управління ризиками також вважається інструментом навчання та підвищення обізнаності, який допомагає бізнес-лідерам приймати правильні рішення та створювати культуру безпечнішої роботи. Організації використовують системи управління ризиками, щоб отримати повну та точну картину поточного ландшафту ризиків в організації. Також, ризик-менеджмент дає організації інструменти для правильного визначення потенційних ризиків і боротьби з ними.

У зв'язку з цим, дослідження методів та засобів ризик-менеджменту, якому присвячена ця магістерська робота, є актуальним завданням.

1 ОГЛЯД СТАНДАРТІВ УПРАВЛІННЯ ТА ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Основною складовою системи управління (менеджменту) інформаційною безпекою (СУІБ/СМІБ) в організації (підприємстві, установі) є підсистема управління ризиками (ризик-менеджмент) [1-3].

Менеджмент ризиків передбачає: аналіз ризиків, ідентифікацію та оцінку ризиків, розроблення та практичну реалізацію заходів, направлених на мінімізацію ризиків, оцінку ефективності та контроль впровадження тих чи інших заходів ризик-менеджменту.

Нормативну базу в сфері оцінки ризиків та визначення загроз інформаційним ресурсам, що обробляються в інформаційно-комунікаційних системах, складають національні та міжнародні стандарти, що дають узагальнені рекомендації щодо побудови та оцінки ризиків інформаційної безпеки в рамках СУІБ [1, 2].

В цьому розділі будуть розглянуті основі стандарти в сфері управління ризиками інформаційної безпеки (ІБ), деякі з них прийняті як Державний Стандарт України (рис 1.1).

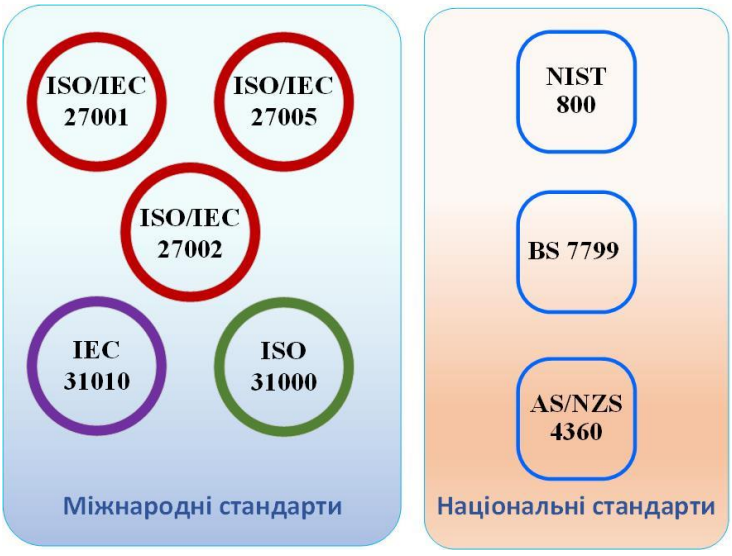


Рисунок 1.1 – Стандарти оцінки та управління ризиками ІБ

В роботі використовується терміни та визначення відповідно до словника СУІБ, що надається стандартом ISO/IEC 27000 [4] (додаток А).

1.1 Міжнародні стандарти

1.1.1 Стандарт ISO/IEC 27001

Стандарт ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements» входить до серії стандартів ISO/IEC 27000. Оновлена версія стандарту прийнята в жовтні 2022 року Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) [5].

З 22 серпня 2023 року цей стандарт діє як Державний Стандарт України: ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги».

Цей нормативний документ визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення СУІБ для організації. Документ також містить вимоги до оцінки та обробки (зниження) ризиків інформаційної безпеки (ризик-менеджменту), пристосованих під потреби організації. Вимоги, викладені в стандарті, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи форми власності. Положення, викладені в стандарті, стосуються таких тем (в дужках номери розділів) [5 – 7]:

- організаційний контекст (4);
- керівництво (5);
- планування(6);
- підтримка (7);
- експлуатація (8);

– оцінювання ефективності (9);

– вдосконалення (10).

Кожна з цих тем описує частину системи управління інформаційною безпекою. Стандарт ISO 27001 зосереджений на меті вищого рівня – переконатися, що організації мають структуру (систему управління), яка гарантує, що організація покращує інформаційну безпеку. Ця СУІБ – це не ІТ-система, а опис процесів у організації. Вона складається з цілей, ресурсів, політики та описів процесів. Тільки ці елементи вищого рівня вимагаються ISO 27001. Виключення будь-якої з вимог, зазначених у розділах 4 – 10, є неприйнятним, якщо організація заявляє про відповідність цьому стандарту.

ISO 27001 базується на двох концепціях. Перша – полягає в управлінні ризиками: перш ніж вживати будь-яких дій, керівництво повинно зрозуміти, які активи варто захищати, які є ризики та як ці ризики контролюються. Друга концепція – це безперервний цикл заходів Шухарта-Демінга PDCA [8 – 10]: «Планування (Plan) – Виконання (Do) – Перевірка (Check) – Вплив/Управління/Коригування (Act)». Перш ніж діяти, потрібно мати чітку мету (план) і продумати, якою буде перевірка, чи виконуються дії, і що робити після перевірки (рис. 1.2).

Рисунок 1.2 – Модель PDCA [8]

Для кожної з тем, перелічених вище, стандарт ISO 27001 визначає детальні вимоги для проходження сертифікації. Нижче наведено короткий перелік усіх описаних елементів (в дужках вказані номери пунктів ISO 27001).

1. Розуміння організації та її контексту (4.1).
2. Розуміння потреб та очікувань зацікавлених сторін (4.2).
3. Визначення сфери застосування СУІБ (4.3).
4. Система управління інформаційною безпекою (4.4).
5. Керівництво та зобов’язання (5.1).
6. Політика (5.2).
7. Організаційні ролі, відповідальність та повноваження (5.3).
8. Дії щодо ризиків і можливостей (6.1): загальні (6.1.1), оцінка ризиків інформаційної безпеки (6.1.2) та оброблення (зниження) ризиків інформаційної безпеки (6.1.3). Частиною цього є створення угоди (заяви) про застосовність, яка вказує на те, які найкращі методи контролю реалізовано, а які ні.
9. Цілі інформаційної безпеки та планування їх досягнення (6.2).
10. Планування змін (6.3).
11. Ресурси (7.1).
12. Компетенція (7.2): відповідне навчання/компетенції для персоналу, відповідального за СУІБ.
13. Обізнаність (7.3) для всього персоналу в сфері застосування СУІБ
14. Комунікація (7.4): план внутрішньої та зовнішньої комунікації щодо інформаційної безпеки
15. Документована інформація (7.5): достатня документація про СУІБ, включаючи розмір організації, складність і компетентність персоналу (7.5.1), яка відповідним чином оновлюється (7.5.2) та контролюється (7.5.3).
16. Операційне (робоче) планування та контроль (8.1): в основному це виконання заходів PDCA (рис. 1.3) та їх доведення за допомогою документації.

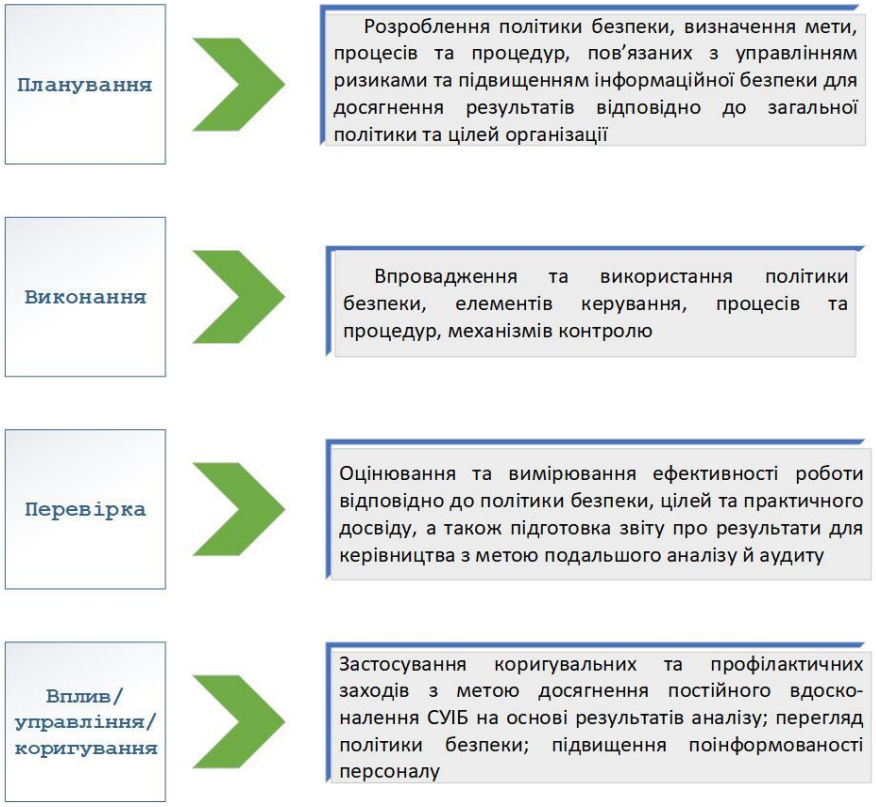


Рисунок 1.3 – Опис циклу PDCA для СУІБ [9]

17. Оцінювання (8.2) та обробка (8.3) ризиків інформаційної безпеки через регулярні проміжки часу

18. Моніторинг, вимірювання, аналіз та оцінка (9.1) ефективності СУІБ шляхом визначення досягнення цілей

19. Внутрішній аудит (9.2): організація повинна проводити внутрішні аудити через заплановані проміжки часу (9.2.1), планувати, створювати, впроваджувати та підтримувати програму(и) аудиту, включаючи частоту, методи, відповідальність, вимоги до планування та звітність (9.2.2)

20. Перевірка з боку керівництва (9.3). Вище керівництво повинно, на плановій основі, переглядати СУІБ організації, щоб переконатися в її постійній придатності, адекватності та ефективності (9.3.1). Вхідними даними для перегляду з боку керівництва є стан виконаних заходів з попередніх перевірок; зміни у зовнішніх і внутрішніх питаннях, які стосуються СУІБ; зміни в потребах і очікуваннях зацікавлених сторін;

зворотній зв'язок щодо ефективності інформаційної безпеки; результати оцінки ризику; можливості для постійного вдосконалення тощо (9.3.2). Результати перегляду з боку керівництва (9.3.3) повинні включати рішення щодо можливостей постійного вдосконалення та будь-яких потреб у внесенні зміни до СУІБ.

21. Постійне вдосконалення (10.1): організація повинна постійно покращувати придатність, адекватність та ефективність СУІБ.

22. Невідповідність і коригувальні дії (10.2): це частина правильного виконання циклу PDCA, збору відгуків про кожну зустріч від учасників та інші кроки вдосконалення. Якщо виникає невідповідність, організація повинна реагувати на це, і, якщо є можливість, вжити заходів щодо її контролю та виправлення, а також боротися з наслідками, визначаючи потребу в діях для усунення причин невідповідності, щоб вона не повторилася або не виникла в іншому місці.

Останнім розділом стандарту є Додаток А (нормативний), в яку наведені засоби управління (контролі) інформаційною безпекою. Контролі безпосередньо виведені із засобів управління, які наведені у ISO/IEC 27002:2022 [11], пункти 5 – 8, і мають використовуватись у контексті 6.1.3:

- організаційні контролі (5);
- контролі персоналу (6);
- фізичні контролі (7);
- технологічні контролі (8).

В додатку Б представлений витяг з таблиці А.1 стандарту в частині, що стосується управління ризиками ІБ.

Відповідно до ISO/IEC 27001, система управління інформаційною безпекою, – це системний підхід до управління інформаційними ризиками, включаючи безліч засобів контролю інформаційної безпеки, необхідних для зменшення неприйнятних ризиків, а також інші способи обробки ризиків: уникнення, передача або прийняття ризиків. СУІБ є основою для послідовного керування ними всіма.

1.1.2 Стандарт ISO/IEC 27002

Стандарт ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection - Information security controls» [11]. Прийнятий як Державний Стандарт України: ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки».

ISO/IEC 27002:2022 визначає три основні джерела вимог щодо інформаційної безпеки, які допомагають визначити заходи безпеки [12].

1. Оцінка ризиків: оцінка ризиків для організації з урахуванням загальної бізнес-стратегії та цілей організації. Визначення засобів контролю залежить від рішень організації після оцінки ризиків.

2. Законодавство та регуляторні акти: Законодавчі, статутні, регулятивні та договірні вимоги, яким має відповідати організація та її зацікавлені сторони (торгові партнери, постачальники послуг тощо), а також їхнє соціокультурне середовище. При визначенні заходів контролю слід також брати до уваги всі відповідні національні та міжнародні закони та правила.

3. Чинники життєвого циклу: набір принципів, цілей та бізнес-вимог для всіх етапів життєвого циклу інформації, які організація розробила для підтримки своєї діяльності. Інакше кажучи, інформація має життєвий цикл: від створення до утилізації. Цінність інформації та ризики для неї можуть змінюватися протягом усього життєвого циклу (наприклад, несанкціоноване розкриття чи крадіжка фінансових рахунків компанії), тому інформаційна безпека залишається важливою в тій чи іншій мірі на всіх етапах. Проекти розробки нових та заміни існуючих систем надають можливості для покращення заходів безпеки, беручи до уваги ризики організації та досвід, що були отримані з інцидентів протягом життєвого циклу інформації.

Стандарт ISO/IEC 27002 містить довідковий набір з 93 загальних засобів контролю інформаційної безпеки [11, 13], включаючи вказівки щодо впровадження:

– у контексті СУІБ на основі ISO/IEC27001;

– для впровадження засобів контролю інформаційної безпеки на основі міжнародно визнаної найкращої практики;

– для розробки керівних принципів управління інформаційною безпекою для конкретної організації.

Узагальнена структура стандарту представлена на рисунку 1.4.

Рисунок 1.4 – Структура стандарту ISO/IEC 27002:2022 [14]

Класифікація засобів/заходів керування (контролів), наведена в розділах 5-8, називається темами. Контролі класифікуються як [11, 14]:

– персональні, якщо вони стосуються окремих працівників, – 8 контролів;

– фізичні, якщо вони стосуються фізичних об'єктів, – 14 контролів;

– технологічні, якщо вони стосуються техніки – 34 контролів;

– організаційні, якщо вони не відносяться до жодної з вище вказаних категорій, – 37 контролів.

Організація може використовувати атрибути для створення різноманітних подань (представлень), які є різними категоріями контролів, що розглядаються з точки зору, відмінної від тем. Атрибути можна використовувати для фільтрації, сортування або представлення контролів в різних переглядах для різних аудиторій. Додаток А стандарту (Annex A) є інформаційним та пояснює, як цього можна досягти, і надає приклад подання.

Кожен засіб керування пов’язаний з п’ятьма атрибутами з відповідними значеннями атрибутів (перед ними ставиться «#», щоб зробити їх доступними для пошуку), а саме:

а) тип контролю (control type) – це атрибут для перегляду засобів керування з точки зору того, коли та як контроль змінює ризик щодо виникнення інциденту інформаційної безпеки. Значення атрибутів складаються з Попереджуючого (Preventive) – контроль, який призначений для запобігання виникненню інциденту інформаційної безпеки, Виявляючого (Detective) – контроль діє, коли відбувається інцидент інформаційної безпеки та Коригувального (Corrective) – контроль діє після інциденту інформаційної безпеки;

б) властивості інформаційної безпеки (information security properties) – це атрибут для перегляду контролів з точки зору того, збереженню якої характеристики інформації цей контроль сприятиме. Значення атрибутів складаються з Конфіденційності (Confidentiality), Цілісності (Integrity) та Доступності (Availability);

в) концепції кібербезпеки (cybersecurity concepts) – це атрибут для перегляду контролів з точки зору їх асоціації з концепціями кібербезпеки, визначеними в структурі кібербезпеки, описаній у IS0/IEC TS 27110. Значення атрибутів складаються з Ідентифікувати (Identify), Захищати (Protect), Виявляти (Detect,), Реагувати (Respond) та Відновлювати (Recover).

г) операційні можливості (operational capabilities) – це атрибут для перегляду контролів з точки зору практикуючого спеціаліста щодо можливостей інформаційної безпеки. Значення атрибутів складаються з Керівництва (Governance), Управління_активами (Asset_management), Захист_інформації (Information_protection), Безпека_людських_ресурсів (Human_resource_security), Фізична_безпека (Physical_security), Безпека_ систем_і_мереж (System_and_network_security), Безпека_додатків (Application_ security), Безпечне_налаштування (Secure_configuration), Ідентифікація_та_ управління_доступом (Identity_and_access_management), Управління_ загрозами_та_вразливістю (Threat_and_vulnerability_management), Безперервність (Continuity), Безпека_взаємовідносин_із_постачальниками (Supplier_ relationships_security), Закон_та_відповідність (Legal_and_compliance), Управління_подіями_інформаційної_безпеки (lnformation_ security_event_ management) та Забезпечення_інформаційної_безпеки (Information_security _assurance);

д) домени безпеки (security domains) – це атрибут для перегляду контролів з точки зору чотирьох доменів інформаційної безпеки:

– «Управління та екосистема» включає «Управління безпекою інформаційної системи та управління ризиками» та «Управління кібербезпекою екосистеми» (включаючи внутрішні та зовнішні зацікавлені сторони);

– «Захист» включає «Архітектуру безпеки IT». «Адміністрування IT-безпеки», «Ідентифікація та управління доступом», «Підтримка IT-безпеки» та «Фізична безпека та безпека навколишнього середовища»;

– «Оборона» включає «Виявлення» та «Керування інцидентами комп’ютерної безпеки»;

– «Стійкість» включає «Безперервність операцій» та «Кризове управління».

Значення атрибутів складаються з Керівництво_та_Екосистема (Governance_and_Ecosystem), Захист (Protection), Оборона (Defense) та Стійкість (Resilience).

Атрибути, наведені в цьому стандарті, вибрано тому, що вони вважаються достатньо загальними для використання різними типами організацій. Організації можуть ігнорувати один або кілька атрибутів, наведених у цьому документі. Вони також можуть створювати власні атрибути (з відповідними значеннями атрибутів), щоб створювати власні організаційні представлення.

Макет кожного контролю містить наступне [11]:

– коротка назву контролю;

– таблиця атрибутів: таблиця показує значення кожного атрибута для даного контролю;

– контроль: що таке контроль;

– ціль: навіщо потрібно здійснювати контроль;

– рекомендації: як слід здійснювати контроль;

– інша інформація: пояснювальний текст або посилання на інші пов’язані документи.

В додатку В наведений витяг із таблиці А.1 (матриці контролів та значень атрибутів) додатку А стандарту ISO/IEC 27002.

На практиці більшість організацій, які прийняли ISO/IEC 27001, також використовують додаток А, а отже, ISO/IEC 27002 як загальну основу або структуру для своїх засобів контролю, вносячи різні зміни, якщо це необхідно, щоб відповідати їхнім конкретним вимогам до обробки інформаційних ризиків.

1.1.3 Стандарт ISO/IEC 27005

Стандарт ISO/IEC 27005:2022 «Information security, cybersecurity and privacy protection - Guidance on managing information security risks» [15]. Прийнятий як Державний Стандарт України: ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки».

Цей нормативний документ містить вказівки, щоб допомогти організаціям, незалежно від типу, розміру чи галузі [16 – 18]:

– виконувати вимоги ISO/IEC 27001 щодо дій з усунення ризиків інформаційної безпеки;

– здійснювати діяльність з управління ризиками інформаційної безпеки, зокрема оцінку та зменшення ризиків інформаційної безпеки.

Стандарт ISO/IEC 27005:2022 складається з шести основних розділів та додатку, які розкривають детальні поради щодо [15]:

1. Управління ризиками інформаційної безпеки (5 Information security risk management) – описує ітеративний (безперервний) процес виявлення, оцінки та оброблення ризиків інформаційної безпеки, що включає як стратегічні/довгострокові, так і операційні (експлуатаційні)/середньо-короткострокові цикли (рис. 1.5).

2. Встановлення контексту (6 Context establishment) – в основному стосується методів визначення критеріїв ризику. Бізнес-контекст організації для управління інформаційними ризиками та безпекою описано в розділі 10.

3. Процес оцінки ризиків інформаційної безпеки (7 Information security risk assessment process) – описує процес систематичного виявлення, аналізу, оцінювання та визначення пріоритетів ризиків ІБ.

4. Процес обробки ризиків інформаційної безпеки (8 Information security risk treatment process) – описується в основному з точки зору

використання засобів контролю інформаційної безпеки для «модифікації» (пом’якшення або підтримки) ризиків ІБ.

5. Експлуатація (9 Operation) – визначає, що процес оцінки ризиків ІБ, відповідно до ISO/IEC 27001:2022, п. 6.1, повинен бути інтегрований в організаційні операції та повинен виконуватися через заплановані інтервали або тоді, коли пропонуються або відбуваються суттєві зміни. Процес оцінки ризиків ІБ повинен враховувати критерії, встановлені ISO/IEC 27001:2022, п 6.1.2 а).

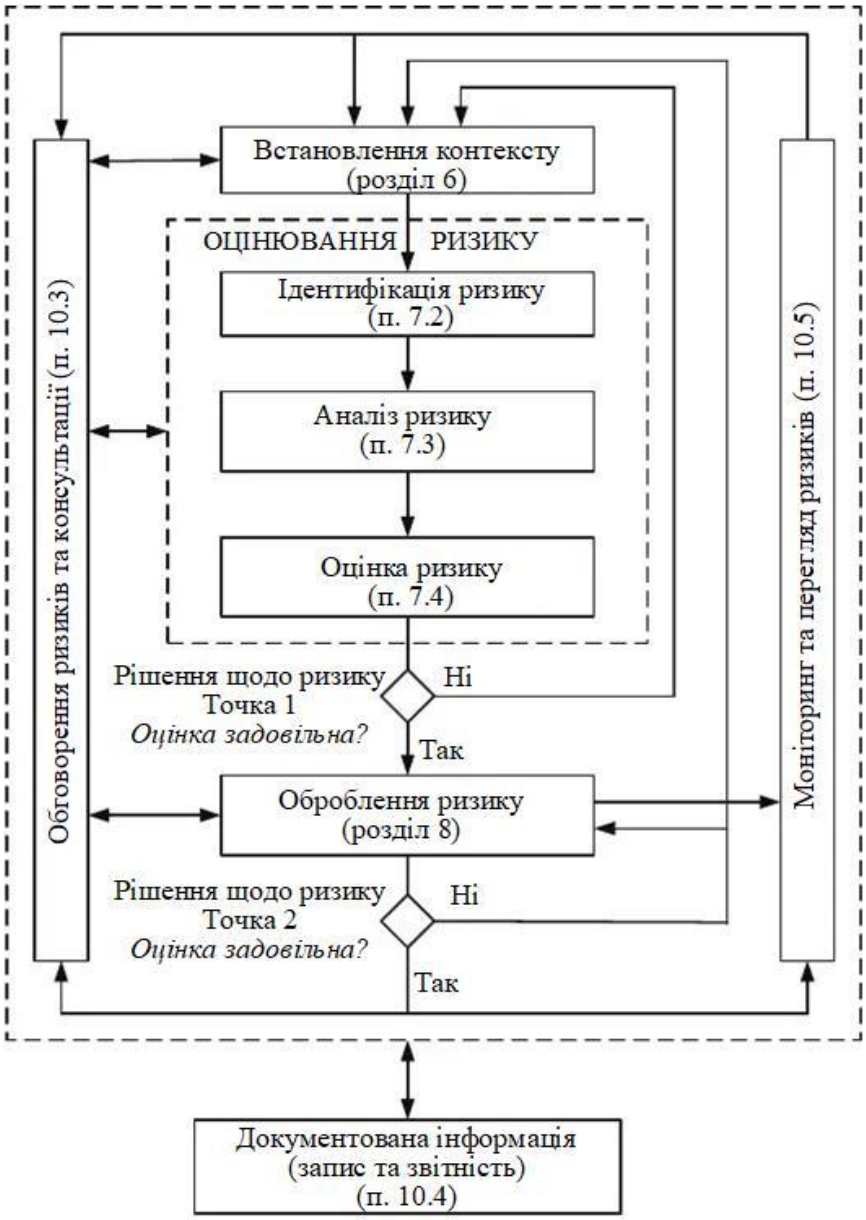


Рисунок 1.5 – Процес управління ризиками інформаційної безпеки [15]

6. Використання пов’язаних процесів СУІБ (10 Leveraging related ISMS processes) – це, по суті, переробка та розширення стандарту ISO/IEC 27001, які визначають, що організація повинна мати на високому рівні (наприклад, стратегічному) розуміння важливих питань, які можуть вплинути на СУІБ, як позитивно, так і негативно. Заплановані результати повинні забезпечувати збереження конфіденційності, цілісності та доступності інформації шляхом застосування процесу управління ризиками та знання того, якими ризиками адекватно керують.

В додатку А (інформативний/довідковий) стандарту приведена додаткова інформація про критерії ризику та практичні методики (поради), такі як приклади загроз, вразливостей тощо.

В пункті А.2 «Практичні методики» (Practical techniques) пропонується під час ідентифікації та оцінки ризиків інформаційної безпеки брати до уваги наступні компоненти:

а) компоненти, пов'язані з минулим:

1) події та інциденти безпеки (як всередині організації, так і за її межами);

2) джерела ризику;

3) використані вразливості;

4) виміряні наслідки;

б) компоненти, пов'язані з майбутнім:

1) загрози;

2) вразливості;

3) наслідки;

4) сценарії ризику.

Взаємозв'язки між компонентами ризику інформаційної безпеки представлені на рисунку 1.6

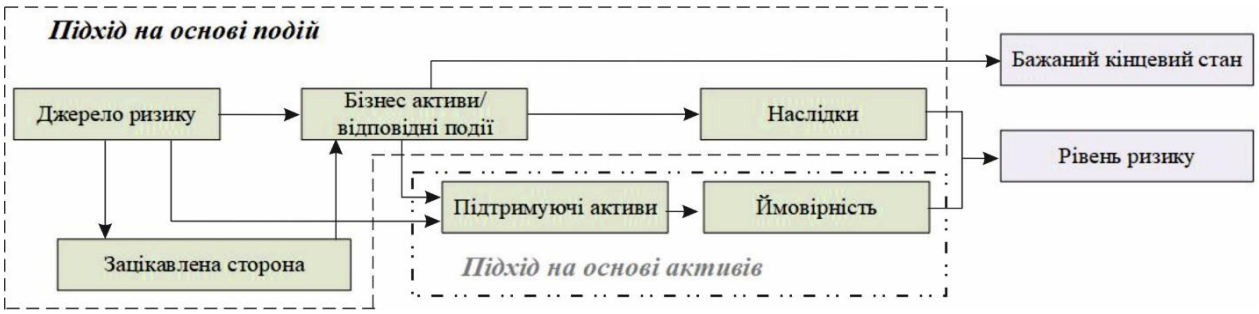


Рисунок 1.6 – Складові оцінки ризиків інформаційної безпеки [15]

Процес ідентифікації ризиків (пошуку, розпізнавання та опису ризиків) передбачає ідентифікацію джерел ризику та подій. Метою ідентифікації ризиків є створення списку ризиків на основі тих подій, які можуть запобігти, вплинути або затримати досягнення цілей інформаційної безпеки.

ISO/IEC 27001:2022, п. 6.1.2, вимагає від організації визначити та застосувати процес оцінки ризиків інформаційної безпеки, який визначає ризики інформаційної безпеки. Існує два підходи, які зазвичай використовуються для визначення ризиків [15, 17]:

– підхід, заснований на подіях: визначає стратегічні сценарії шляхом розгляду джерел ризиків та того, як вони використовують або впливають на зацікавлені сторони для досягнення бажаної цілі ризику;

– підхід на основі активів: визначає операційні сценарії, деталізовані з точки зору активів, загроз і вразливостей.

1.1.4 Стандарт ISO 31000

Стандарт ISO 31000:2018 «Risk management – Guidelines» [19]. З 1 січня 2019 року діє як Державний Стандарт України: ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови».

Стандарт ISO 31000:2018 [19, 20]:

– надає рекомендації щодо управління ризиками, з якими стикаються організації. Застосування цих інструкцій можна налаштувати для будь-якої організації та її контексту;

– забезпечує загальний підхід до управління будь-яким типом ризику і не стосується конкретної галузі чи сектора;

– можна використовувати протягом усього життя організації та застосовувати до будь-якої діяльності, включаючи прийняття рішень на всіх рівнях.

Цей стандарт призначений для використання фахівцями, які створюють і захищають цінності в організаціях шляхом: управління ризиками, прийняття рішень, встановлення та досягнення цілей, і підвищення продуктивності. Організації будь-якого типу та розміру стикаються із зовнішніми та внутрішніми факторами та впливами, через які вони не можуть досягти своїх цілей.

ISO 31000 визначає, що управління ризиками [20]:

– є ітеративним (повторюваним) процесом і допомагає організаціям у встановленні стратегії, досягненні цілей і прийнятті обґрунтованих рішень;

– є частиною корпоративного управління, а також має фундаментальне значення для управління на всіх рівнях. Це сприяє вдосконаленню систем управління;

– є частиною всієї діяльності, пов’язаної з організацією, і включає взаємодію із зацікавленими сторонами;

– враховує зовнішній і внутрішній контекст організації, включаючи людську поведінку та культурні фактори;

– ґрунтується на принципах, структурі та процесі, викладених у цьому стандарті, як показано на рис. 1.7.

Зазначені компоненти можуть повністю або частково існувати в організації, однак їх, можливо, потрібно адаптувати або вдосконалити, щоб управління ризиками було доцільним, ефективним та послідовним.

Принципи (principles), викладені на рис. 1.7, надають вказівки щодо характеристик ефективного та результативного управління ризиками, відображають його цінності та пояснюють його призначення та цілі. Принципи є основою для управління ризиками, і їх слід враховувати під час встановлення структури та процесів управління ризиками в організації. Ці принципи мають дозволити організації керувати впливом невизначеності на досягнення її цілей.

Розробка структури (framework) охоплює інтеграцію, проектування, впровадження, оцінку та вдосконалення управління ризиками в усій організації. Організація повинна оцінити існуючі практики та процеси управління ризиками, оцінити будь-які прогалини та усунути ці прогалини в межах структури. Компоненти структури та те, як вони взаємодіють, мають бути адаптовані до потреб організації.

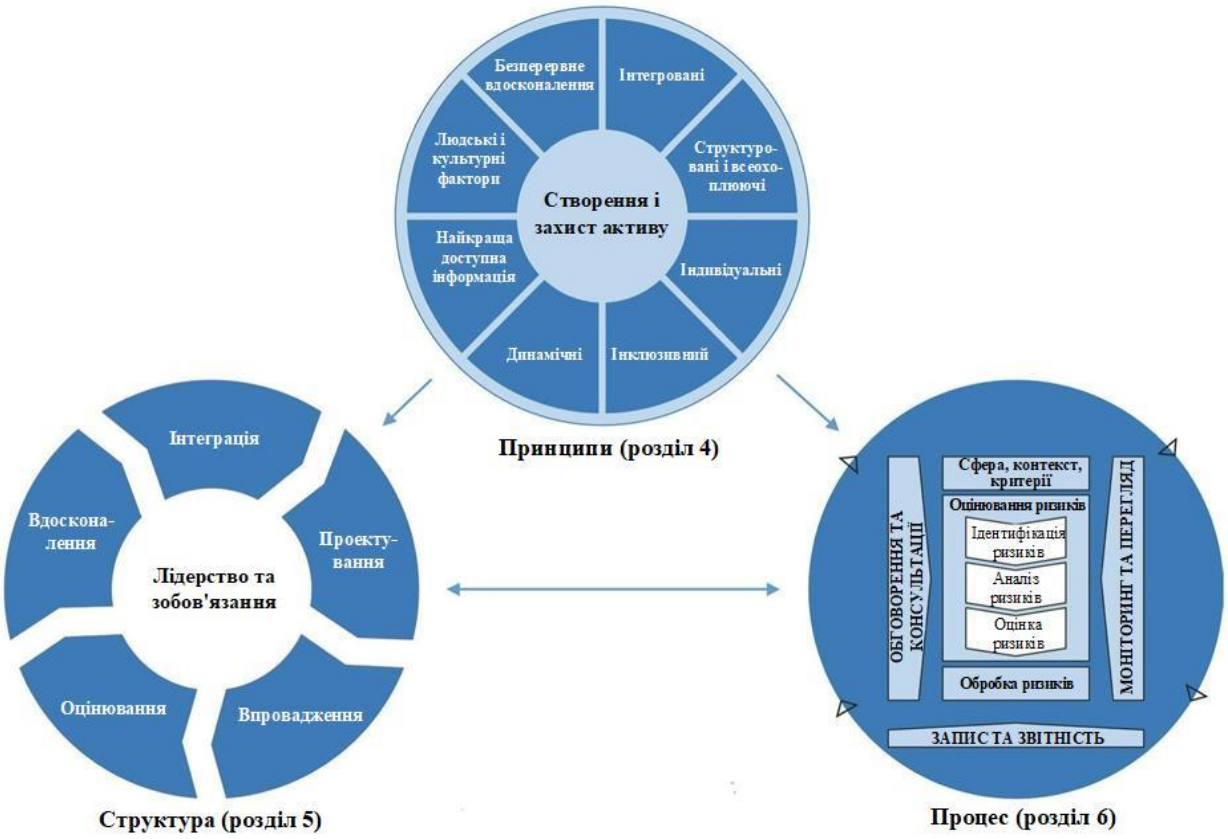


Рисунок 1.7 – Складові оцінки ризиків інформаційної безпеки [19]

Процес (process) управління ризиками включає систематичне застосування політик, процедур та практик до діяльності з інформування та консультування, встановлення контексту та оцінки, обробки, моніторингу, аналізу, реєстрації та звітності про ризики. Процес управління ризиками має бути невід'ємною частиною управління та прийняття рішень та інтегрований у структуру, операції та процеси організації. Його можна застосовувати на стратегічному, операційному, програмному чи проектному рівнях. В організації може бути багато застосувань процесу управління ризиками, налаштованих для досягнення цілей і відповідно до зовнішнього та внутрішнього контексту, в якому вони застосовуються. Динамічний і мінливий характер людської поведінки та культури слід враховувати протягом усього процесу управління ризиками. Хоча процес управління ризиками часто представляють як послідовний, на практиці він є ітеративним (повторюваний).

1.1.5 Стандарт IEC 31010

Стандарт IEC 31010:2019 «Risk management – Risk assessment techniques» [21]. З 31 грудня 2023 року вступає в дію як Державний Стандарт України: ДСТУ EN IEC 31010:2022 «Керування ризиками - методи оцінки ризиків».

Цей стандарт містить вказівки щодо вибору та застосування методів оцінки ризику в широкому діапазоні ситуацій. Методи, які використовуються IEC 31010:2019, спрямовані на надання допомоги у прийнятті рішень у випадках, коли існує невизначеність, для надання інформації про певні ризики та як частина процесу управління ризиками.

У документі наведено результати низки методів із посиланнями на інші документи, де ці методи описані більш детально. IEC 31010:2019 містить наступні значні технічні зміни по відношенню до попереднього видання [22]:

– більш детально надано процес планування, впровадження, перевірки та підтвердження використання методів;

– збільшено кількість і діапазон застосування методик.

Загальні рекомендації щодо впровадження методів оцінки ризиків включають п’ять розділів [23].

1. Планування оцінки: цей процес передбачає підготовку організації до початкової та поточної оцінки ризиків. Ці вказівки включають визначення обсягу та мети оцінки, розуміння організаційного контексту для оцінки ризику, включаючи знання та досвід малих і середніх підприємств в організації, визначення цілей оцінки, встановлення критеріїв для вимірювання ризику та розуміння того, як соціальні та людські фактори можуть впливати на обидва оцінка та постійне управління ризиками.

2. Управління інформацією: збір інформації є критично важливою частиною оцінки ризику, і методи, які використовуються для виконання цього завдання, повинні узгоджуватися з критеріями та цілями організації. Організації повинні мати можливість отримувати інформацію (зокрема, визначати надійність і категорію джерел інформації), аналізувати дані в межах їх життєвого циклу та встановлювати потенційну невизначеність інформації. Крім того, на цьому етапі процесу оцінювання організація повинна моделювати дані та моделі ризиків. Моделювання даних у цьому контексті означає відображення проблем, результатів і представлень процесів у моделі, яка робить оцінку вхідних і вихідних даних життєздатною.

3. Застосування методів оцінки: у цьому посібнику описано, як визначити джерела ризику, визначити ризики, дослідити ефективність існуючих засобів контролю та проаналізувати ймовірність ризиків. Ця інструкція також вказує організаціям дотримуватися методів, визначених у додатках A та B цього стандарту.

4. Перегляд аналізу: організації повинні мати можливість перевірити та затверджувати результати своєї оцінки ризиків на основі моделей і показників, розроблених на попередніх етапах. Це також включає роботу над

будь-якою потенційною невизначеністю, яка може вплинути на аналіз цих результатів (наприклад, системні змінні або ненадійні джерела даних). Також, організації повинні використовувати результати для прийняття рішень.

5. Застосування результатів для прийняття рішень: будь-які рішення щодо вимірювання ризиків та їхнього впливу на систему, прийняття рішень щодо прийнятних ризиків і вибір між різними типами ризиків на основі переваги мають ґрунтуватися на описаному процесі оцінки ризиків.

Відповідно до розбивки процесу оцінки ризику, IEC 31010 надає додаток конкретних методів, які організація може використовувати для виконання свого аналізу. Крім того, ці методи чітко відображаються в процесі оцінки ризику, визначеному в ISO 31000 (рис. 1.8).

Отримання інформації від зацікавлених сторін (стейкхолдерів) та експертів (B1): ця група методів зосереджена на тому, як точно й ефективно збирати інформацію від профільних експертів та інших зацікавлених сторін. Деякі методи, включають структурований мозковий штурм, досягнення консенсусу групою експертів (метод Дельфі), метод номінальної групи, інтерв’ю та опитування.

Ідентифікація ризиків (B2): це група методів направлена на визначення того, як організація точно збирає інформацію та визначає ризики у своїх системах. Методи цієї групи включають використання класифікації та таксономії, використання аналізу режимів і наслідків відмов (failure modes and effects analysis, FMEA) та аналіз режимів відмов, наслідків і критичності (failure modes, effects and criticality analysis, FMCEA), використання досліджень небезпеки та працездатності (hazard and operability, HAZOP), аналізу сценаріїв (scenario analysis) і структурованих методів «що-якщо» (structured what if technique, SWIFT).

Визначення джерел, причин і факторів ризику (B3): ця група методів виділяє здатність організації належним чином розуміти причини ризиків шляхом вивчення взаємозв'язків між ризиками. Ці методи включають аналіз

нематеріальних джерел ризику (підхід Небезпек – Cindynic approach) і груповий причинно-наслідковий аналіз (метод аналізу Ісікави - Ishikawa analysis method).

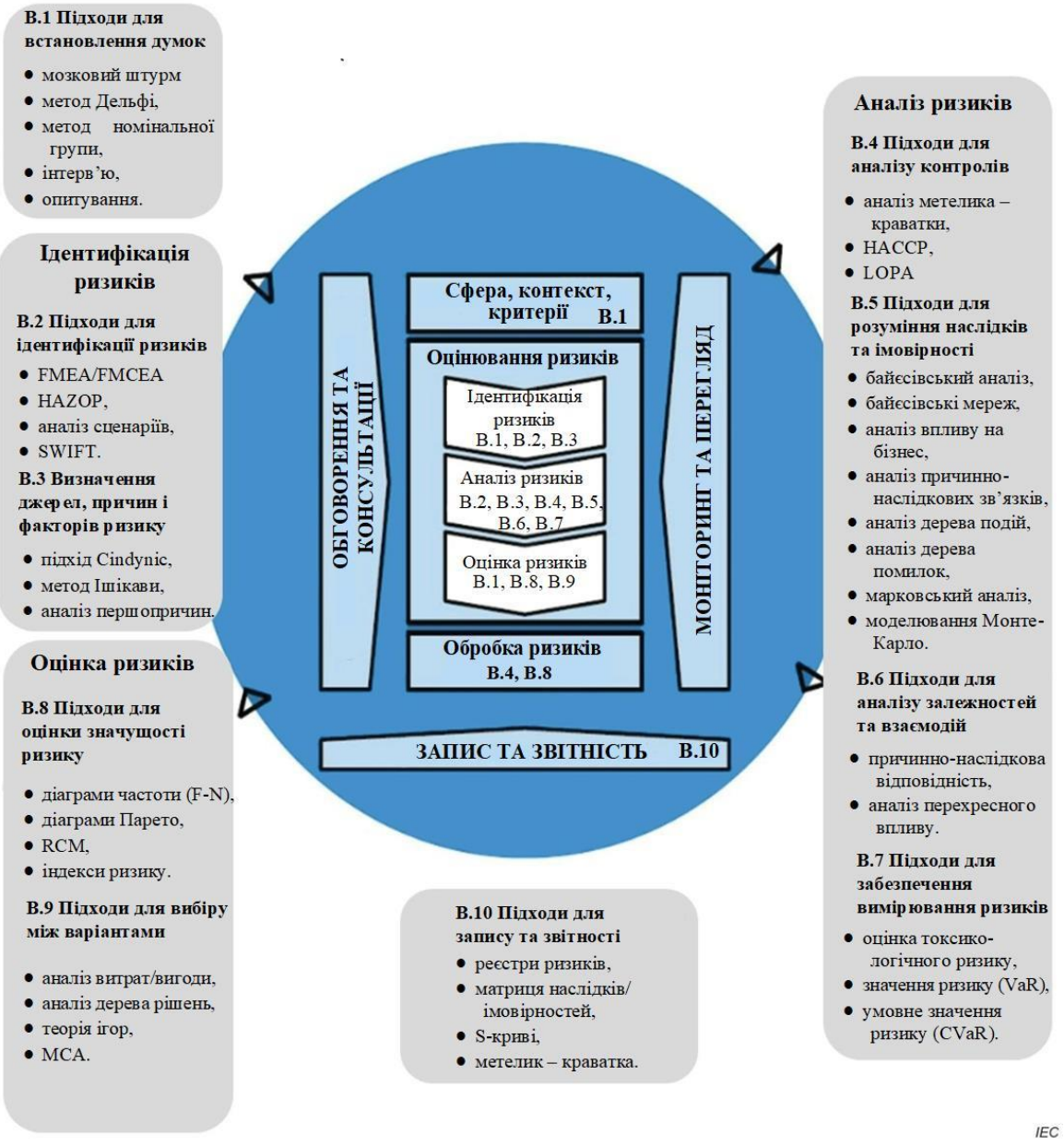


Рисунок 1.8 – Застосування методів у процесі управління ризиками ISO 31000 [21]

Аналіз засобів контролю (B4): ця група методів підкреслює здатність організації визначати, чи засоби контролю є адекватними та відповідними для виявлених ризиків. Ця група включає аналіз краватки-метелика (bow tie analysis), аналіз небезпек і критичних контрольних точок (hazard analysis and

critical control points, HACCP) і аналіз рівнів захисту (layers of protection analysis, LOPA).

Розуміння наслідків і ймовірності (B5): ці методи допомагають організації зрозуміти більш значний вплив ризиків залежно від контексту та історії системи. Ці методи включають байєсівський аналіз, байєсівські мережі та діаграми впливу, аналіз впливу на бізнес (business impact analysis, BIA), аналіз причинно-наслідкових зв'язків (cause-consequence analysis, CCA), аналіз дерева подій (event tree analysis, ETA), аналіз дерева помилок (fault tree analysis, FTA), аналіз надійності людини (human reliability analysis, HRA), марковський аналіз , моделювання Монте-Карло та аналіз впливу на конфіденційність (privacy impact analysis, PIA).

Аналіз залежностей і взаємодій (B6): ці методи вимагають, щоб організація виконувала причинно-наслідкове відображення або використовувала ланцюжки аргументів або логіку, що показує взаємозв'язки між подіями, засобами контролю та ризиками. Вони включають в себе причинно-наслідкову відповідність (causal mapping) та аналіз перехресного впливу (cross impact analysis).

Забезпечення вимірювання ризику (B7): ці методи забезпечують способи вимірювання впливу ризику на системи або широку громадськість. Ці методи включають оцінку токсикологічного ризику (toxicological risk assessment), значення ризику (value at risk, VaR) та умовне значення ризику (conditional value at risk, CVaR) або очікуваний дефіцит (expected shortfall, ES).

Оцінка значущості ризику (B8): ця група методів визначає способи визначення того, як ставитися до ризику в контексті організації. Це включає в себе перевірку на дотримання принципу «розумно - практично» щодо стійкості до ризику, використання діаграм частоти (F-N) і діаграм Парето, оцінювання на основі обслуговування орієнтованого на надійність (reliability centred maintenance, RCM) і використання взаємозв'язаних індексів ризику.

Вибір між варіантами (B9): ці методи пов'язані зі здатністю організації приймати рішення між двома додатковими шляхами управління

ризиками, включаючи рішення щодо прийнятного ризику та запроваджених заходів контролю. Ці методи включають аналіз витрат/вигоди (cost/benefit analysis, CBA), аналіз дерева рішень (decision tree analysis), теорію ігор і багатокритеріальний аналіз (Multi-criteria analysis, MCA).

Запис та звітність (B10): ці методи стосуються здатності організації записувати інформацію про ризики в базу даних, щоб забезпечити розуміння змінюючого потенціалу ризику та його оцінки. Ці методи включають реєстри ризиків, ведення документів щодо технічного обслуговування та моделювання за допомогою S-кривих.

1.2 Національні стандарти

1.2.1 Стандарт NIST 800

Національним інститутом стандартів і технологій (National Institute of Standards and Technology) США розроблені спеціальній публікації (special publication) NIST SP серії 800 [24 – 25], які містять вказівки, рекомендації, технічні характеристики та щорічні звіти про діяльність NIST у сфері кібербезпеки. Публікації SP 800 розроблені для вирішення та підтримки потреб безпеки та конфіденційності інформації та інформаційних систем Федерального уряду США. Серія, створена в 1990 році, розповідає про дослідження Лабораторії інформаційних технологій (Information Technology Laboratory), рекомендації та заходи з поширення комп’ютерної безпеки, а також про її спільну діяльність з галузевими, урядовими та академічними організаціями.

Одним із найбільш часто використовуваних методів управління ризиками інформаційної безпеки на рівні системи є платформа (фреймворк) управління ризиками (risk management framework, RMF) – розроблена на основі стандартів [25]:

– NIST SP 800-30 «Guide for Conducting Risk Assessments» («Посібник з проведення оцінки ризиків»);

– NIST SP 800-39 «Managing Information Security Risk» («Управління ризиками інформаційної безпеки»);

– NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управління ризиками для інформаційних систем та організацій»);

– NIST SP 800-137 «Information Security Continuous Monitoring» («Безперервний моніторинг інформаційної безпеки») [xx].

RMF надає організаціям структурований підхід до ефективного управління інформаційними ризиками. Фреймворк служить дорожньою картою, яка допомагає організаціям виявляти, оцінювати та усувати ризики.

RMF включає сім кроків [26]: підготовчий етап для забезпечення готовності організацій до виконання процесу та шість основних кроків. Всі сім кроків є важливими для успішного виконання RMF (рис. 1.9).

1. Підготуватися (Prepare) до виконання RMF з точки зору організації та системного рівня, встановивши контекст і пріоритети для управління ризиком безпеки та конфіденційності.

2. Категоріювати (Categorize) систему та інформацію, що обробляється, зберігається та передається системою на основі аналізу впливу втрат.

3. Вибрати (Select) початковий набір засобів контролю для системи та налаштувати контролі, щоб зменшити ризик до прийнятного рівня на основі оцінки ризику.

4. Впровадити (Implement) засоби контролю та описати, як контролі використовуються в системі та середовищі її функціонування.

5. Оцінити (Assess) засоби контролю, щоб визначити, чи вони реалізовані правильно, чи працюють за призначенням і чи дають бажані результати щодо задоволення вимог щодо безпеки та конфіденційності.

6. Авторизувати (Authorize) систему або загальні засоби контролю на основі визначення того, що ризик для операцій та активів організації, окремих осіб, інших організацій є прийнятним.

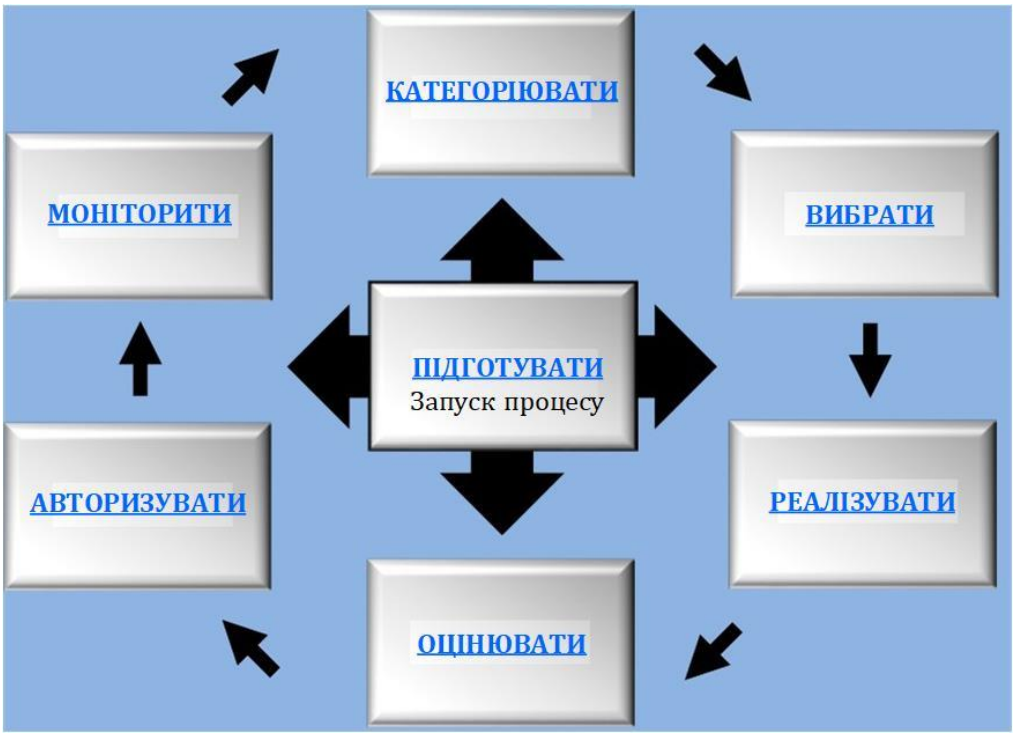


Рисунок 1.9 – Структура RMF

7. Моніторити/контролювати (Monitor) систему та пов’язані з нею засоби контролю, включаючи оцінку ефективності контролю, документування змін у системі та робочому середовищі, проведення оцінки ризиків та аналізу впливу, а також звітування про стан безпеки та конфіденційності системи.

1.2.2 Стандарт BS 7799

BS 7799, Code of Practice for Information Security Management – це британський стандарт «Кодекс практики управління інформаційною

безпекою», вперше опублікований Британським інститутом стандартів (British Standards Institution, BSI) в 1995 році. Пізніше було також опубліковано ще дві частини стандарту (перша – BS 7799-1) [27].

Оригінальний стандарт BS 7799 містив структурований підхід до управління інформаційною безпекою – описував близько 127 засобів контролю інформаційної безпеки в 10 розділах або категоріях. Кожний контроль розроблено для вирішення визначеної цілі контролю.

В 2000 році стандарт BS 7799-1 був спрощений і прийнятий як ISO/IEC 17799: Information Technology - Code of practice for information security management (Інформаційні технології – Кодекс практики управління інформаційною безпекою). В 2005 році ISO/IEC 17799 було включено до родини стандартів ISO/IEC 27000 як стандарт ISO/IEC 27002.

Друга частина стандрту BS 7799-2: Information Security Management Systems - Specification with guidance for use (Системи управління інформаційною безпекою – Специфікація з інструкціями щодо використання). була опублікована у 1999 році як формальна специфікація, що підтримує оцінку відповідності та сертифікацію. BS 7799-2 пояснює, як розробити та впровадити систему управління інформаційною безпекою (information security management system, ISMS).

У версії BS 7799-2 2002 року було введено цикл PDCA, узгоджуючи його зі стандартами якості, такими як ISO 9000. В 2005 році BS 7799-2 був прийнятий як стандарт ISO/IEC 27001.

Третя частина стандарту BS 7799-3: Information security management systems - Guidelines for information security risk management (Системи управління інформаційною безпекою – Рекомендації щодо управління ризиками інформаційної безпеки) була опублікована у 2005 році. BS 7799-3 фокусується на ідентифікації, аналізі, обробці та моніторингу інформаційних ризиків [28]. Він був адаптований і прийнятий як стандарт ISO/IEC 27005 у 2008 році. Тим часом BS 7799-3 продовжує розвиватися паралельно. Його було переглянуто в 2017 році, а в 2023 році було запропоновано проект для спрощення інструкцій спеціально для невеликих організацій [29].

1.2.3 Стандарт AS/NZS 4360

Австралійський/Новозеландський стандарт для управління ризиками (The Australian/New Zeeland Standard for Risk Management, AS/NZS 4360) був введений в дію як міжнародний стандарт Австралії та Нової Зеландії в 1995 році та переглянутий у 2004 році. Відтоді його було включено до міжнародного стандарту AS/NZS ISO 31000:2009 [30, 31].

Стандарт AS/NZS 4360 надає загальну основу для процесу управління ризиками (блок-схема процесу представлена на рис 1.10), яка поділяє елементи процесу оцінки ризиків на кілька підпроцесів [31]: «Встановлення контексту», «Ідентифікація ризиків», «Аналіз ризиків», «Оцінювання ризиків» та «Обробка ризиків».

Метою цього стандарту [30] є надання вказівок, які дозволять державним, приватним або громадським підприємствам, групам і окремим особам досягти:

– більш впевнена і строга основа для прийняття рішень і планування;

– краще визначення можливостей і загроз;

– отримання користі від невизначеності та мінливості;

– більш ефективний розподіл і використання ресурсів;

– покращення управління інцидентами та зменшення збитків і вартості ризику, включаючи комерційні страхові премії;

– підвищення впевненості та довіри зацікавлених сторін;

– покращення дотримання відповідного законодавства; і

– краще корпоративне управління.

Стандарт також описує два процеси, які мають виконуватися паралельно з сеансами оцінки ризиків у рамках управління ризиками: «Моніторинг та перегляд» та «Обговорення та консультації».

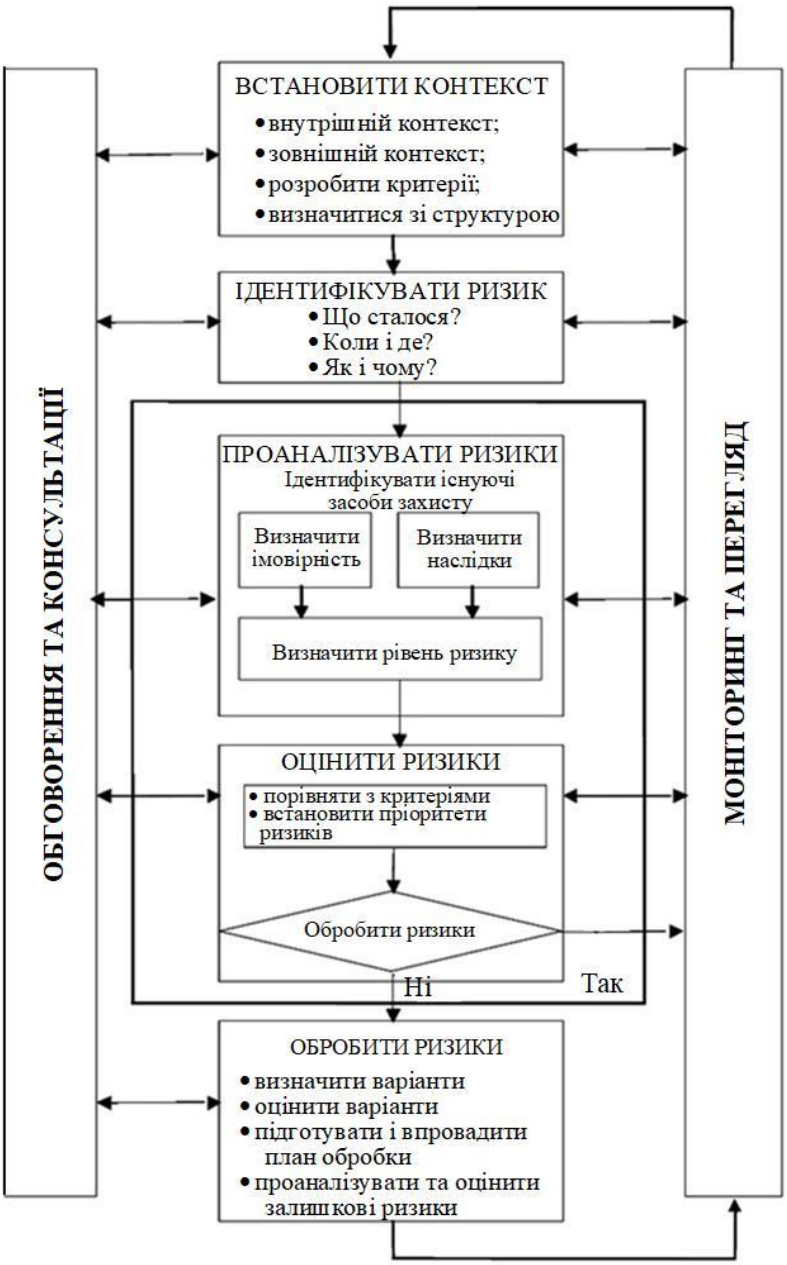


Рисунок 1.10 – Процес управління ризиками [30]

1.3 Висновки до розділу 1

В першому розділі були розглянуті ключові міжнародні та національні стандарти в сфері управління та оцінки ризиків інформаційної безпеки. Наявні стандарти управління ризиками надають організаціям ефективні інструменти контролю інформаційної безпеки з метою зменшення ризиків,

які можуть вплинути на їх прогрес. Адаптуючи ці стандарти до власного унікального контексту та постійно вдосконалюючи методи управління ризиками, організації та підприємства можуть ефективно захищати свою діяльність.

Розробка та впровадження (сертифікація) СУІБ в організації на основі розглянутих стандартів робить її більш прозорою по відношенню до зацікавлених сторін (партнерів, клієнтів тощо), так як інформує їх про те, що всі процеси в організації відповідають міжнародно визнаним нормативам.

2 МЕТОДИ І ЗАСОБИ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналіз ризику має на меті визначити рівень ризику. ISO/IEC 27001:2022, п. 6.1.2, вимагає, щоб для кожного ідентифікованого ризику аналіз ризику базувався на оцінці наслідків ризику та оцінці ймовірності ризику для визначення рівня ризику.

Методики аналізу ризику на основі наслідків і ймовірності (ISO/IEC 27005:2022, п. 7.3.1) базуються на трьох підходах (рис. 2.1):

– якісному (qualitative), з використанням шкали кваліфікаційних атрибутів (наприклад, високий, середній, низький);

– кількісному (quantitative), з використанням шкали з числовими значеннями (наприклад, грошова вартість, частота або ймовірність виникнення); або

– змішаному, напівкількісному (semiquantitative), з використанням якісних шкал із присвоєними числовими значеннями.

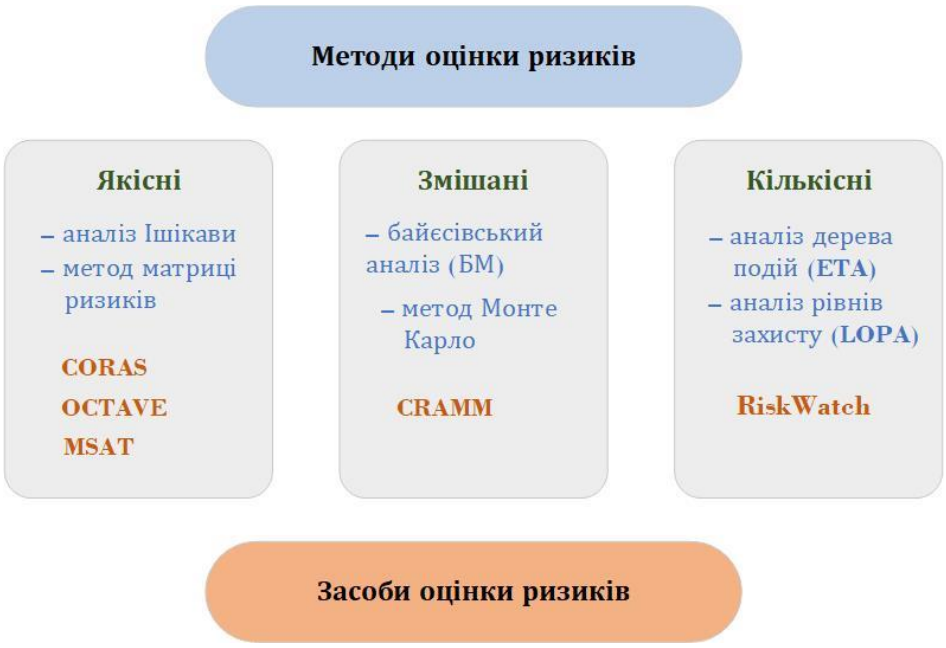


Рисунок 2.1 – Методи та засоби оцінки ризиків інформаційної безпеки

Різні аналітики (експерти) мають різні судження щодо невизначеності під час інтерпретації балів на шкалі ймовірності та наслідків. Еталонні шкали повинні пов’язувати категорії наслідків, ймовірності та ризику із загальними однозначно визначеними об’єктивними значеннями, можливо вираженими такими термінами, як фінансові збитки в грошових одиницях та умовна частота виникнення протягом обмеженого періоду, які є специфічними для кількісного підходу. Зокрема, якщо використовується якісний підхід, аналітики ризику повинні проходити навчання та періодично практикуватися за контрольною шкалою, щоб підтримувати калібрування своїх суджень.

2.1 Якісні підходи

Якісні методи надають оцінку ризику, використовуючи лінгвістичні/вербальні змінні з графічним представленням у вигляді таблиць, графів, блок-схем тощо. Далі будуть розглянуті найпоширеніші методи якісної оцінки ризиків.

Причинно-наслідковий аналіз (метод аналізу Ішікави) [22] – використовує командний підхід для визначення можливих причин будь-якої бажаної чи небажаної події, впливу, проблеми чи ситуації. Можливі сприяючі фактори, цьому методі, впорядковано в широкі категорії, щоб охопити людські, технічні та організаційні проблеми. Інформація подається у вигляді діаграми Ішікави (також називається «риб’яча кістка») (рис. 2.2).

Основні кроки виконання аналізу такі:

– встановити подію, яку потрібно проаналізувати, і помістити її в рамку як голову діаграми «риб’яча кістка». Подія може бути як позитивною (об'єкт), так і негативною (проблема);

– узгодити основні категорії причин. Приклади поширених категорій: матеріали, методи та процеси, середовище, обладнання, трудові

ресурси, вимірювання (можна використовувати будь-який набір узгоджених категорій, які відповідають обставинам, що аналізуються).

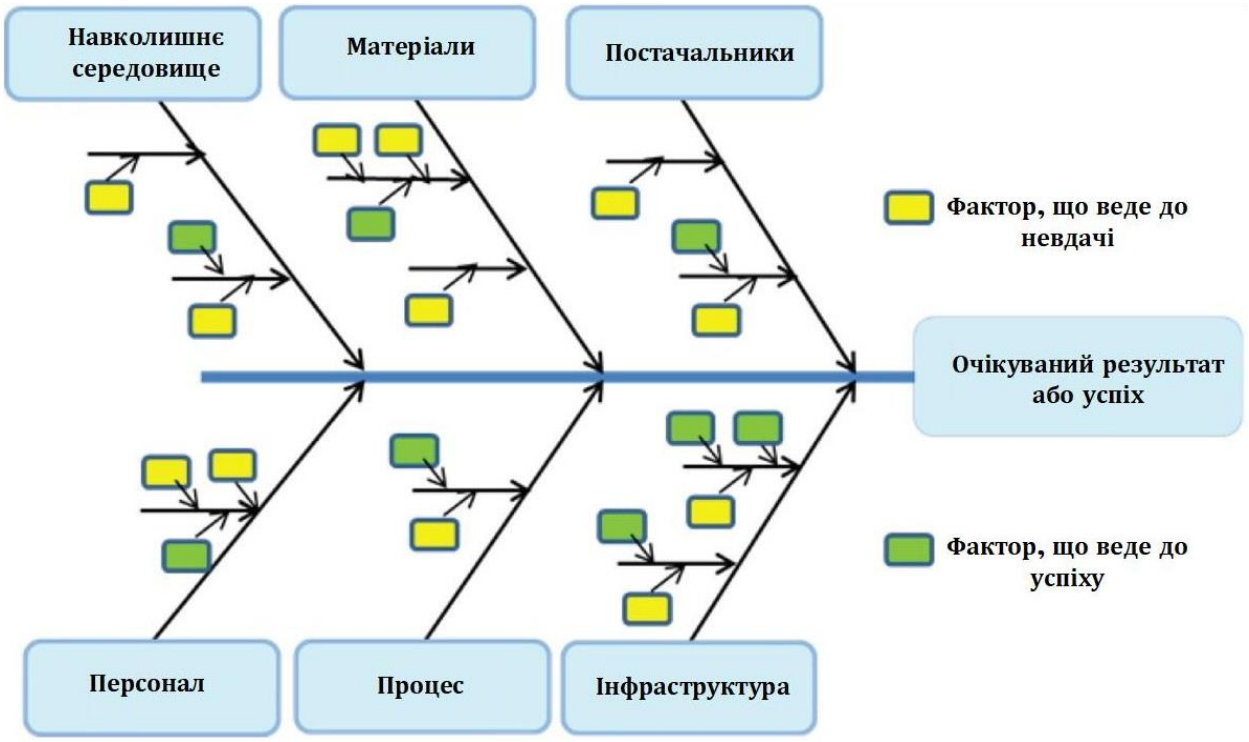


Рисунок 2.2 – Приклад діаграми Ішікави [22]

– ітеративно (багаторазово) досліджувати причини та фактори впливу в кожній категорії, додаючи кожну з кісток діаграми «риб’яча кістка»: ставити запитання "чому?" і "як це може статися?";

– переглянути всі гілки, щоб перевірити послідовність і повноту та переконатися, що причини стосуються основного наслідку.

– визначити найважливіші фактори на основі думки команди (експертів) та наявних доказів.

Діаграма часто розроблюється в рамках семінару [22, 32].

Аналіз Ішікави можна використовувати під час виконання аналізу першопричин подій, які відбулися, або для визначення факторів, які можуть сприяти результатам, які ще не відбулися. Метод можна використовувати для

вивчення ситуацій на будь-якому рівні в організації протягом будь-якого часового масштабу.

До сильних сторін методики Ішікави можна віднести наступне [22]:

– заохочує та використовує групові знання;

– забезпечує цілеспрямований підхід до мозкового штурму або аналогічних методів ідентифікації;

– можна застосовувати до широкого кола ситуацій;

– забезпечує структурований аналіз причин з графічним висновком, що легко читається;

– дозволяє людям повідомляти про проблеми у нейтральній обстановці;

– можна використовувати для виявлення факторів, що сприяють як бажаним, так і небажаним впливам.

Обмеження даного методу включають наступне:

– поділ причинно-наслідкових факторів на основні категорій на початку аналізу означає, що взаємодія між категоріями не може бути врахована належним чином.

– потенційні причини, які не охоплені вибраними категоріями, не визначені.

Метод матриці ризиків (матриця наслідків/імовірностей) [22] – це спосіб відображення ризиків відповідно до їх наслідків та імовірностей, та об’єднання цих характеристик для відображення рейтингу значущості ризику. Налаштовані шкали для наслідків і імовірностей визначені для осей матриці. Шкали можуть мати будь-яку кількість балів – найбільш поширені три-, чотири- або п’ятибальні шкали (табл. 2.1). Шкала (або шкали) наслідків може відображати позитивні чи негативні наслідки. Шкали мають бути безпосередньо пов’язані з цілями організації та повинні поширюватися від максимального достовірного наслідку до найменшого цікавого наслідку.

Таблиці 2.2 і 2.3 представляють приклади альтернативних способів представлення шкал імовірності. Вірогідність може бути виражена або

ймовірнісними термінами, як у таблиці 2.2, або частотними термінами, як у таблиці 2.3.

Таблиця 2.1 – Приклад шкали наслідків [15]

Наслідки	Опис
5 – Катастрофічні (catastrophic)	**Наслідки для сектора або регулювання за межами організації** Значний вплив на оточуюче середовище сектору з наслідками, які можуть бути тривалими. Та/або: труднощі для держави, і навіть неспроможність, забезпечити регуляторну функцію або одну з життєвоважливих місій. Та/або: критичні наслідки для безпеки людей і майна (серйозні кібератаки на державні установи, руйнування основних інфраструктур тощо).
4 – Критичні (critical)	**Руйнівні наслідки для організації** Нездатність організації забезпечити всю або частину своєї діяльності з можливими серйозними наслідками для безпеки людей і майна. Організація, швидше за все, не вийде з ситуації (її виживання знаходиться під загрозою), сектори діяльності або державні сектори, в яких вона працює, ймовірно, постраждають несуттєво, без будь-яких довгострокових наслідків.
3 – Серйозні (serious)	**Значні наслідки для організації** Значне погіршення виконання діяльності з можливими значними наслідками для безпеки людей і майна. Організація подолає ситуацію з серйозними труднощами (робота в сильно деградованому режимі), без жодного галузевого чи державного впливу.
2 – Значні (significant)	**Значні, але обмежені наслідки для організації** Погіршення виконання діяльності без наслідків для безпеки людей і майна. Організація впорається із ситуацією, незважаючи на деякі труднощі (робота в деградованому режимі).
1 – Незначні (minor)	**Незначні наслідки для організації** Жодних наслідків для операцій або виконання діяльності або для безпеки людей і власності. Організація подолає ситуацію без особливих труднощів.

Ймовірнісне представлення вказує на середню імовірність виникнення ризикової події за визначений період, тоді як частотне представлення вказує кількість разів, коли ризикова подія, як очікується, відбудеться в середньому за визначений період часу. Оскільки два підходи просто виражають те саме з двох різних точок зору, можна використовувати будь-яке подання, залежно

від того, яке організація вважає найбільш зручним для даної категорії ризиків [33].

Вербальні позначки, такі як «низький», «середній» і «високий», можуть бути додані до рейтингу при використанні будь-якого підходу для оцінки імовірності.

Таблиця 2.2 – Приклад шкали імовірності [15]

Імовірність	**Опис**
5 – Майже напевно (almost certain)	Джерело ризику напевно досягне своєї мети, використовуючи один із розглянутих методів атаки. Імовірність ризикового сценарію дуже висока.
4 – Дуже ймовірно (vety likely)	Ймовірно, джерело ризику досягне своєї мети, використовуючи один із розглянутих методів атаки. Імовірність ризикового сценарію висока.
3 – Ймовірно (likely)	Джерело ризику може досягти своєї мети, використовуючи один із розглянутих методів атаки. Імовірність сценарію ризику значна.
2 – Скоріше малоймовірно (rather unlikely)	Джерело ризику має відносно мало шансів досягти своєї мети, використовуючи один із розглянутих методів атаки. Імовірність сценарію ризику низька.
1 – Малоймовірно (unlikely)	Джерело ризику має дуже мало шансів досягти своєї мети, використовуючи один із розглянутих методів атаки. Імовірність сценарію ризику дуже низька.

Такі позначки будуть корисними під час обговорення рівнів імовірності із зацікавленими сторонами, які не є спеціалістами з ризиків. Однак вони є суб’єктивними і тому неминуче неоднозначними. Отже, їх не слід використовувати як первинні дескриптори (одиниці опису контексту) під час виконання оцінювання або звітування.

Корисність якісних шкал і узгодженість оцінок ризиків, які випливають з них, повністю залежать від узгодженості, з якою позначки категорій інтерпретуються всіма зацікавленими сторонами [22]. При використанні словесних дескрипторів імовірності, наслідків або ризику, вони повинні формально посилатися на однозначні шкали, прив’язані до числових або раціометричних опорних точок (як у таблицях 2.1 і 2.2). Усі зацікавлені сторони мають бути ознайомлені з еталонними шкалами, щоб забезпечити

послідовність інтерпретації даних якісної оцінки та результатів. У таблиці 2.3 представлено приклад якісного підходу.

Критерієм прийняття ризику може бути значення, вище якого ризики вважаються неприпустимий.

Таблиця 2.3 – Приклад якісного підходу до критеріїв ризику [15]

Імовірність	**Наслідок**				
	Катастрофічний	Критичний	Серйозний	Значний	Незначний
Майже напевно	Дуже високий	Дуже високий	Високий	Високий	Середній
Дуже ймовірно	Дуже високий	Високий	Високий	Середній	Низький
Ймовірно	Високий	Високий	Середній	Низький	Низький
Скоріше малоймовірно	Середній	Середній	Низький	Низький	Дуже низький
Малоймовірно	Низький	Низький	Низький	Дуже низький	Дуже низький

Використовуючи матрицю ризиків з кольоровим кодуванням, що відображає шкали наслідків та імовірності, організації можуть графічно подати розподіл ризиків за результатами однієї або декількох оцінок ризиків. Така матриця ризиків також може використовуватися для сигналізації про відношення організації, що займається ризиками, до значень ризику та вказівки того, чи ризик зазвичай приймати або обробляти [15, 33].

Матриця ризиків із використанням трьох кольорів (червоний, жовтий і зелений) може бути застосована для представлення трьох ступенів оцінки ризику, як представлено в таблиці 2.4.

Якщо матриця ризиків використовується для порівняння результатів початково виконаної оцінки ризику з результатами повторної оцінки тих самих ризиків, зниження ризику можна легше представити, якщо застосувати більше кольорів до поточних рівнів ризику.

Переваги методу матриці ризиків включають наступне:

– відносно простий у використанні;

– забезпечує швидке ранжування ризиків за різними рівнями значущості;

– забезпечує чітке візуальне відображення відповідної значущості ризику за наслідками, ймовірністю або рівнем ризику;

– можна використовувати для порівняння ризиків із різними типами наслідків.

Таблиця 2.4 – Приклад шкали оцінювання в поєднанні з триколірною матрицею ризику [15, 34]

Рівень ризику	**Оцінка ризику**	**Опис**
Низький (зелений)	Прийнятний, як є	Ризик можна прийняти без подальших дій.
Помірний (жовтий)	Терпимий, під контролем	Потрібно проводити подальші дії щодо управління ризиками та встановлювати дії в рамках постійного вдосконалення в середньостроковій та довгостроковій перспективі.
Високий (червоний)	Неприйнятний	Заходи щодо зниження ризику обов'язково повинні бути вжиті в короткостроковій перспективі. В іншому випадку потрібно відмовитися від усієї діяльності або її частини.

Обмеження методу включають наступне:

– щоб розробити якісну матрицю, потрібні хороші знання;

– важко визначити загальні шкали, які застосовуються в різних обставинах, що стосуються організації;

– важко однозначно визначити масштаби, щоб дозволити користувачам послідовно зважувати наслідки та імовірність;

– достовірність рейтингів ризику залежить від того, наскільки добре були розроблені та відкалібровані шкали;

– використання методу дуже суб'єктивне, і різні експерти часто присвоюють дуже різні оцінки одному ризику. Це залишає його відкритим для маніпуляцій;

– важко поєднати або порівняти рівень ризику для різних категорій наслідків.

2.2 Кількісні підходи

Кількісні методи оцінки рівня ризику базуються на визначенні ймовірності (P) настання небажаної події (реалізації загрози) та наслідку/збитків/втрат/шкоди (A). При цьому рівень ризику обчислюється за формулою [33]:

$$R = P \cdot A, \tag{2.1}$$

Для визначення ймовірності реалізації загрози використовується апарат теорії ймовірностей та математичної статистики, як правило, - байєсівський аналіз даних та метод Монте Карло.

Байєсівський аналіз дозволяє використовувати як дані, так і суб'єктивну інформацію для прийняття рішень [22]. Байєсівський аналіз базується на теоремі Байєса, яка забезпечує ймовірнісну основу для зміни думки у світлі нових доказів. Загалом теорема Байєса виражається формулою (2.2):

$$P\left(H_j \middle| D\right) = \frac{P\left(D \middle| H_j\right)}{\sum_n P\left(H_n\right) P\left(D \middle| H_n\right)}, \tag{2.2}$$

де: $P(H)$ – апріорна (попередня) оцінка ймовірності n-ї гіпотези H; $P(D)$ – апріорна (попередня) оцінка ймовірності події D; $P\left(H \middle| D\right)$ –

ймовірність H за умови, що D відбулася (апостеріорна оцінка); $P(D|H)$ – ймовірність D, якщо H відбулася.

В даному випадку маємо деякі дані (D), які ми хочемо використати для оновлення нашого попереднього розуміння (або його відсутності) ризику. Ми хочемо використати ці дані для оцінки відносних переваг ряду (N) конкуруючих і непересічних гіпотез, які ми позначатимемо H_n (де n = 1, 2, …, N). Тоді теорема (2.2) може бути використана для обчислення ймовірності j-ї гіпотези (j = 1, 2,…, n).

Байєсівський аналіз є засобом висновку на основі даних, як оціночних, так і емпіричних [22]. Даний метод можна використовувати для надання висновку щодо параметрів у моделі ризику, розробленій для конкретного контексту (наприклад, ймовірність події, швидкість події або час до події).

Переваги байєсівського аналізу полягають в наступному:

– висновки легко зрозуміти;

– забезпечує механізм використання суб’єктивних переконань щодо проблеми;

– забезпечує механізм для поєднання попередніх думок (гіпотез) з новими даними.

Обмеження байєсівського аналізу наступні:

– може створювати апостеріорні розподіли, які сильно залежать від вибору апріорного;

– розв'язання складних проблем може потребувати великих обчислювальних витрат і бути трудомістким.

На основі байєсівського аналізу будуються байєсівські мережі (БМ) [35] – це графічні моделі, вузли яких представляють випадкові величини (дискретні та/або безперервні). Вузли з’єднані спрямованими дугами, які представляють прямі залежності (які часто є причинно-наслідковими зв’язками) між змінними.

Вузли, що вказують на вузол X_i, називаються батьківськими та позначаються $pa(X_i)$. Зв’язок між змінними визначається кількісно через розподіли умовних ймовірностей, що пов’язані з кожним вузлом, позначеним $P(X_i|pa(X_i))$, де стан вузлів-потомків залежить від комбінації значень батьківських вузлів.

Базова БМ містить змінні, які представляють невизначені події та можуть бути використані для оцінки імовірності чи ризику або для висновку про ключові фактори ризику, що призводять до визначених наслідків.

Переваги БМ включають наступне [22]:

– доступне програмне забезпечення, яке відносно просте у використанні та розумінні;

– мають прозору структуру та здатні швидко запускати сценарії та аналізувати чутливість результатів до різних припущень;

– можуть включати суб'єктивні переконання щодо проблеми разом із даними.

Обмеження включають наступне [22]:

– визначення всіх взаємодій для складних систем є обчислювально складним, коли таблиці умовної ймовірності стають занадто великими;

– встановлення параметрів вимагає знання багатьох умовних ймовірностей, які, як правило, забезпечуються експертними оцінками;

– користувач може вводити помилки, але результат все одно може дати правдоподібну відповідь; перевірка екстремумів може допомогти знайти помилки.

Метод Монте-Карло [36] – це спосіб проведення розрахунків і отримання результатів, які виконуються під час аналізу ризику та включають розподіли.

Виконувати обчислення за допомогою розподілів нелегко, оскільки часто неможливо отримати аналітичні рішення, якщо розподіли не мають чітко визначених форм, і лише з обмеженнями та припущеннями, які можуть бути нереалістичними.

Моделювання Монте Карло, як правило, передбачає взяття випадкових значень вибірки з кожного вхідного розподілу, виконання обчислень для отримання результату, а потім повторення процесу через серію ітерацій для побудови розподілу результатів. Результат можна надати як розподіл ймовірностей значення або деяку статистику, наприклад середнє значення.

Системи можна розробляти за допомогою електронних таблиць та інших звичайних інструментів, але доступні більш складні програмні інструменти, які допомагають із більш складними вимогами.

Переваги аналізу Монте-Карло включають наступне [22]:

– може враховувати будь-який розподіл у вхідній змінній, включаючи емпіричні дані, отримані зі спостережень пов'язаних систем;

– моделі відносно прості у розробці та можуть бути розширені, якщо виникне потреба;

– можуть бути представлені будь-які впливи або зв'язки, включаючи такі ефекти, як умовні залежності;

– він забезпечує міру точності результату;

– доступне програмне забезпечення.

Обмеження аналізу Монте-Карло включають [22]:

– точність рішень залежить від кількості симуляцій;

– використання техніки залежить від можливості представити невизначеності в параметрах за допомогою правильного розподілу;

– важко створювати моделі, які адекватно представляє ситуацію.

– великі та складні моделі ускладнюють участь зацікавлених сторін у процесі.

Аналіз Монте-Карло запобігає наданню надмірної ваги малоймовірним результатам із значними наслідками, визнаючи, що всі такі результати навряд чи відбудуться одночасно в вибірці ризиків. Це може призвести до виключення екстремальних подій з розгляду, особливо якщо розглядається велика вибірка. Це може викликати необґрунтовану впевненість у особи, яка приймає рішення.

2.3 Змішані підходи

Аналіз дерева подій (ETA) – це графічна техніка, яка представляє взаємовиключні послідовності подій, які можуть виникнути після початкової події, залежно від того, чи функціонують різні системи, призначені для зміни наслідків, чи ні [22, 36]. Дерево можна визначити кількісно, щоб забезпечити ймовірності різних можливих результатів (рис. 2.3).

Дерево починається з початкової події, а потім для кожної лінії заходу безпеки малюються лінії, що представляють її виконання (успіх) або невиконання (невдачу). Ймовірність невдачі або успіху може бути призначена кожному елементу контролю на основі експертної оцінки, даних або аналізу окремого дерева помилок. Ймовірності є умовними ймовірностями (наприклад, ймовірність функціонування елемента – це не ймовірність, отримана в результаті випробувань за нормальних умов, а ймовірність функціонування в умовах початкової події).

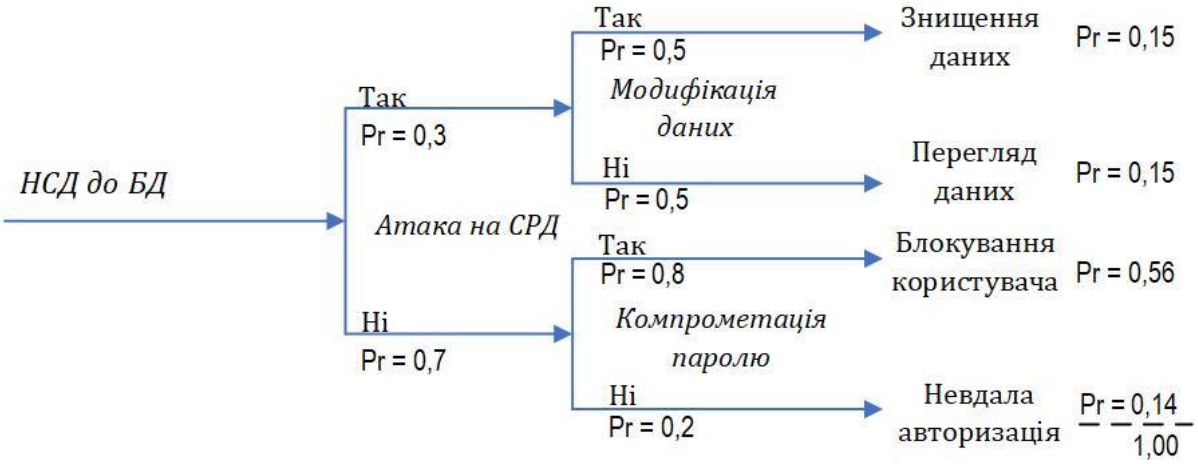


Рисунок 2.3 – Приклад аналізу дерева подій у випадку несанкціонованого доступу до бази даних

Частота різних результатів представлена добутком окремих умовних ймовірностей та ймовірності або частоти початкової події, враховуючи, що різні події є незалежними. На рисунку 2.3 ймовірність початкової події дорівнює 1.

ETA використовується для аналізу потенційних сценаріїв та послідовностей подій після початкової події, для розгляду прийнятності засобів контролю та відносної важливості різних засобів контролю (при оцінці загального рівня ризику), а також для дослідження того, як на результати впливають різні елементи керування. Цей підхід можна застосовувати на будь-якому рівні організації та до будь-якого типу початкової події [22, 36, 37].

На виході моделювання за ETA отримуємо наступне [22]:

– якісний опис потенційних результатів початкових подій;

– кількісні оцінки показників/частот подій або ймовірностей і відносної важливості різноманітних послідовностей відмов і подій, що сприяють цьому;

– кількісні оцінки ефективності засобів контролю.

Переваги методу ETA включають наступне:

– потенційні сценарії після початкової події аналізуються, а вплив успіху чи невдачі засобів контролю показано у чіткій діаграмі, яку, за потреби, можна визначити кількісно;

– визначає кінцеві події, які в іншому випадку можна було б не передбачити;

– визначає потенційні одноточкові збої, зони вразливості системи та контрзаходи з низькою окупністю, а отже, може бути використаний для підвищення ефективності контролю.

Обмеження ETA полягають в наступному:

– для всебічного аналізу необхідно визначити всі потенційні початкові події. Завжди існує ймовірність пропустити деякі важливі початкові події або послідовності подій;

– обробляються лише стани успіху та невдачі системи, і важко включити частково робочі засоби керування, події відкладеного успіху чи відновлення.

Аналіз рівнів захисту (LOPA) аналізує зниження ризику, яке досягається набором засобів контролю. Зі списку виявлених ризиків вибирається пара «причина-наслідок» та ідентифікуються незалежні рівні захисту (independent protection layers, IPL) [22, 36].

IPL – це пристрій, система або дія, яка здатна запобігти розвитку сценарію до небажаних наслідків. Кожен IPL має бути незалежним від причинної події або будь-якого іншого рівня захисту, пов’язаного зі сценарієм, і повинен бути перевірений. IPL включає [22]:

– конструктивні особливості;
– засоби фізичного захисту;
– системи блокування та відключення;
– критичні тривоги та ручне втручання;
– фізичний захист після події;
– системи реагування на надзвичайні ситуації.

Стандартні процедури та/або інспекції безпосередньо не створюють перешкод для відмови, тому загалом їх не слід розглядати як IPL. Оцінюється ймовірність відмови кожного IPL і виконується розрахунок порядку величини, щоб визначити, чи є загальний захист достатнім для зниження ризику до прийнятного рівня.

Частоту виникнення небажаного наслідку можна знайти шляхом поєднання частоти початкової причини з ймовірностями відмови кожного IPL, беручи до уваги будь-які умовні модифікатори. Прикладом умовного модифікатора є те, чи буде особа присутня та чи можна на неї вплинути.

Для частот і ймовірностей використовуються порядки величини. LOPA можна якісно використовувати для перегляду рівнів захисту між причинним фактором і наслідком. Даний метод також може використовуватися кількісно для розподілу ресурсів на обробку шляхом аналізу зниження ризику, спричиненого кожним рівнем захисту. Цей метод

може бути застосований до систем з довгостроковим або короткостроковим часовим горизонтом і зазвичай використовується для роботи з операційними ризиками.

LOPA також можна використовувати кількісно для специфікації IPL і рівнів цілісності безпеки (safety integrity levels, SIL) для інструментальних систем, а також для демонстрації того, що заданий SIL досягти.

Переваги LOPA включають наступне [22, 38]:

– вимагає менше часу та ресурсів, ніж аналіз дерева подій або повна кількісна оцінка ризику, але є більш строгим, ніж суб'єктивні якісні судження;

– допомагає визначити та зосередити ресурси на найбільш критичних рівнях захисту;

– визначає операції, системи та процеси, для яких недостатньо гарантій;

– зосереджений на найсерйозніших наслідках.

Обмеження LOPA включають наступне [22, 38]:

– зосереджується на одній парі «причина-наслідок» і одному сценарії за раз; складні взаємодії між ризиками або між засобами контролю не розглядаються;

– коли використовується кількісно, це може не врахувати збої загального режиму;

– не застосовується для дуже складних сценаріїв, де існує багато пар причинно-наслідкових зв’язків або де є різноманітні наслідки, що впливають на різні зацікавлені сторони.

2.4 Методики і засоби оцінки ризиків

Для оцінки ризиків інформаційної безпеки розроблений цілий ряд методик (з якісною, кількісною та змішаною оцінкою ризиків), які

реалізовані у відповідних програмних комплексах. Сучасні засоби оцінки ризиків відповідають міжнародним і національним стандартам, розглянутим в першому розділі магістерської роботи.

2.4.1 CRAMM

CCTA (Central Communication and Telecommunication Agency, Центральне агентство зв'язку та телекомунікацій) Risk Analysis and Management Method (Метод аналізу та управління ризиками, CRAMM) включає широкий спектр інструментів оцінки ризиків, які повністю відповідають стандартам BS 7799 та ISO 27001, і які вирішують такі завдання, як [36, 39, 40]:

- моделювання залежності активів;
- оцінка впливу на бізнес;
- виявлення та оцінка загроз і вразливостей;
- оцінка рівня ризику;
- визначення необхідних і виправданих заходів контролю на основі оцінки ризику.

CRAMM забезпечує поетапний підхід, що охоплює як технічні (наприклад, апаратне та програмне забезпечення IT), так і нетехнічні (наприклад, фізичні та людські) аспекти безпеки. Щоб оцінити ці компоненти, CRAMM ділиться на три етапи, як показано на рисунку 2.4 [36]:

- ідентифікація та оцінка активів: CRAMM дає змогу ідентифікувати апаратне та програмне забезпечення, дані (інформацію, що зберігається в IT-системі) та місцезнаходження активів, які складають інформаційну систему. Кожен із цих активів можна оцінити. Фізичні активи оцінюються за відновною вартістю. Дані та активи програмного забезпечення

оцінюються з точки зору впливу, який виникне, якщо інформація стане недоступною, знищена, розкрита або змінена;

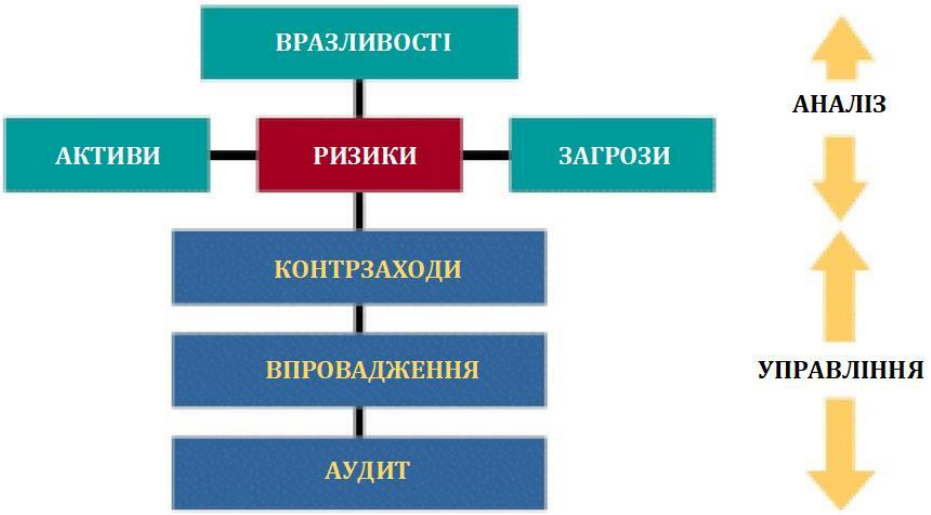


Рисунок 2.4 – Етапи методу CRAMM [39]

– оцінка загрози та вразливості: зрозумівши масштаби потенційних проблем, наступним етапом є визначення того, наскільки ймовірно такі проблеми виникнуть. CRAMM охоплює повний спектр навмисних і випадкових загроз, які можуть вплинути на інформаційну систему, включаючи:

злам, віруси, бої обладнання або програмного забезпечення, навмисне пошкодження або тероризм, помилки персоналу. Цей етап завершується обчисленням рівня основного або фактичного ризику;

– вибір контрзаходів і рекомендації: CRAMM містить дуже велику бібліотеку контрзаходів, яка складається з понад 3000 детальних контрзаходів, організованих у понад 70 логічних груп. Програмне забезпечення CRAMM використовує показники ризиків, визначені на попередньому етапі, і порівнює їх із рівнем безпеки (порогом, пов’язаним із кожним контрзаходом), щоб визначити, чи є ризики достатньо великими, обґрунтувати встановлення того чи іншого контрзаходу. CRAMM надає

низку довідкових засобів, включаючи відкат (повернення назад). Функції визначення пріоритетів «А якщо?» та інструменти звітності для допомоги у впровадженні контрзаходів та активному управлінні виявленими ризиками.

На рисунку 2.5 приведений інтерфейс програми CRAMM.

Основними сильними сторонами цієї методології оцінки ризиків є такі [39, 41]:

– CRAMM надає різноманітні інструменти для оцінки ризиків, що означає, що більшість процесів автоматизовані. Це робить процес оцінки ризику дуже легким.

– методологія повністю відповідає стандартам BS 7799 та ISO 27001, що також збільшує її застосовність.

Основними недоліками цієї методології є такі [8]:

– методологія є узагальненою; отже, все ще існує потреба в розробці або розширенні методології для конкретного етапу вимог.

– CRAMM не може надати кількісну оцінку ризику. Отже, існує необхідність розширити цю методологію в цьому напрямку.

CRAMM чітко не говорить про атрибути безпеки (конфіденційність, цілісність і доступність тощо).

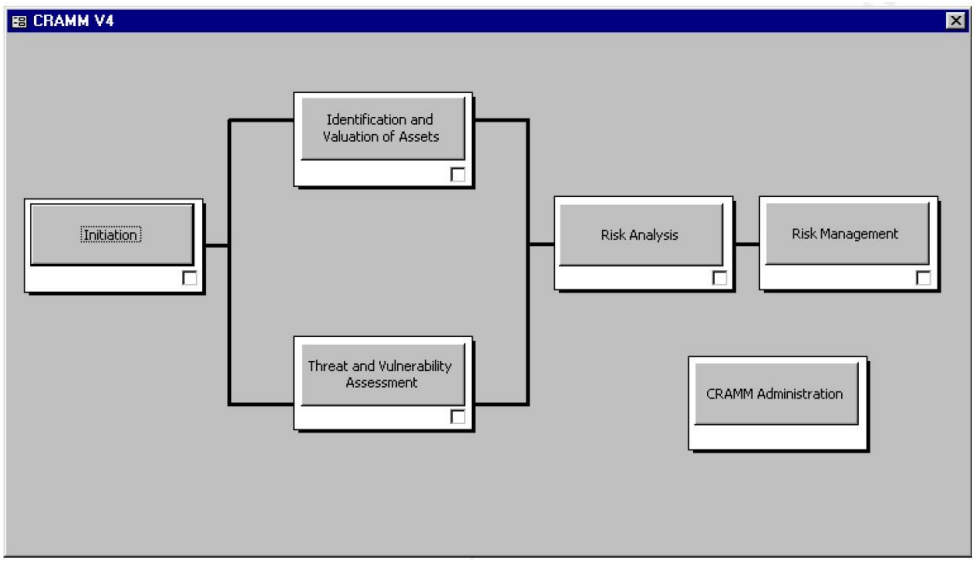


Рисунок 2.5 – Інтерфейс CRAMM [41]

2.4.2 OCTAVE

Операційно критична оцінка загроз, активів і вразливостей (The Operationally Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE) визначає основні компоненти комплексної, систематичної, контекстно-орієнтованої оцінки ризиків інформаційної безпеки відповідно до стандартів ISO/IEC 27001 – 27005.

Дотримуючись методу OCTAVE, організація може приймати рішення щодо захисту інформації на основі ризиків для критичних активів інформаційних технологій (конфіденційності, цілісності та доступності). Операційні або бізнес-підрозділи та IT-відділ працюють разом, щоб задовольнити потреби інформаційної безпеки підприємства.

Відповідно до методу OCTAVE, ризик можна виразити як добуток впливу ризику на ймовірність його виникнення [41, 42]:

$$\textit{Ризик} = \textit{вплив} \times \textit{ймовірність}. \qquad (2.3)$$

На рисунку 2.6 показано деревовидну структуру методів OCTAVE, яка використовується для кожного активу в організації. Вразливість, агент загрози, мета зловмисника та вплив атаки на актив ідентифікуються за допомогою деревовидної структури.

Використовуючи триетапний підхід, OCTAVE вивчає організаційні та технологічні питання, щоб скласти повну картину потреб підприємства в інформаційній безпеці.

Етап 1 – створення профілів загроз на основі активів: це організаційна оцінка. Перевіряються ключові сфери досвіду в організації, щоб визначити важливі інформаційні активи, загрози для цих активів, вимоги до безпеки активів, те, що організація зараз робить для захисту своїх інформаційних

активів (практики стратегії захисту), а також слабкі сторони в організаційних політиках та практиці (організаційна вразливість).

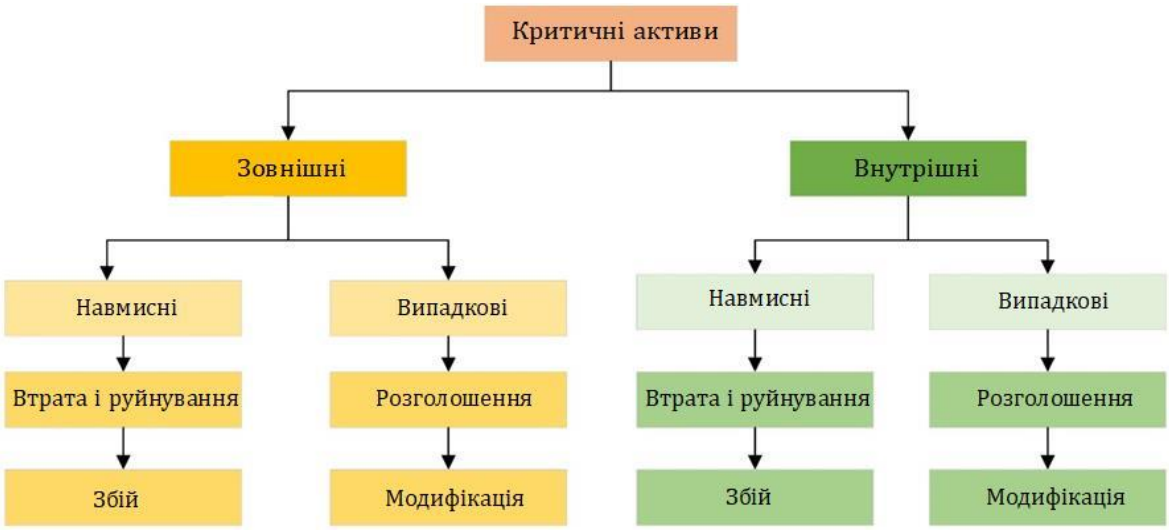


Рисунок 2.6 – Деревоподібна структура для методу OCTAVE [42]

Етап 2 – визначення вразливостей інфраструктури: це оцінка інформаційної інфраструктури. Ключові робочі компоненти інфраструктури інформаційних технологій перевіряються на слабкі місця (технологічні вразливості), які можуть призвести до несанкціонованих дій.

Етап 3 – розробка стратегії та планів безпеки: на цьому етапі аналізуються ризики. Інформація, отримана в результаті оцінювання організаційної та інформаційної інфраструктури (етапи 1 і 2), аналізується для виявлення ризиків для підприємства та оцінки ризиків на основі їх впливу на місію організації.

Кожний етап методу OCTAVE містить два або більше процесів [42].

Етап 1 - створення профілів загроз на основі активів:

– процес 1 (визначення знань вищого керівництва);

– процес 2 (визначте знання про операційну сферу);

– процес 3 (визначення знань персоналу);

– процес 4 (створення профілів загроз).

Етап 2 – визначення вразливостей інфраструктури:

– процес 5 (визначення ключових компонентів);

– процес 6 (оцінювання вибраних компонентів).

Етап 3 – розробка стратегії та планів безпеки:

– процес 7 (проведення аналізу ризиків);

– процес 8 (розробка стратегії захисту).

Основними сильними сторонами цієї методології є [39]:

– враховуються всі критичні операційні загрози, активи та вразливості; це підвищує точність оцінки ризику;

– методологія не лише надає значення оцінки ризику, але й надає певну стратегію безпеки та плани, що підвищує застосовність процесу.

Основними недоліками цієї методології оцінки ризиків є [39]:

– критерії оцінки ризику базуються лише на якісній шкалі (високий, середній, низький);

– методологія є узагальненою; отже, все ще існує потреба в розробці або розширенні методології для конкретного етапу вимог;

– методологія розглядає лише три атрибути для оцінки ризику: конфіденційність, цілісність та доступність;

– методологія значною мірою базується на думках; учасники семінару можуть або не можуть бути добре обізнані з останніми подіями у відповідній сфері.

2.4.3 MSAT

Одним із інструментів, який може допомогти визначити та усунути ризики безпеки, є Microsoft Security Assessment Tool (Інструмент оцінки безпеки компанії Microsoft, MSAT), безкоштовна утиліта, яка представляє електронну анкету, у якій описується середовище безпеки організації [43].

Утиліта розроблена для організацій середнього розміру з 50–500 комп'ютерами, MSAT ставить 172 запитання, упорядкованих за різними категоріями, а потім надає аналіз ситуації та рекомендації щодо її покращення. MSAT починається з набору запитів про бізнес-модель організації, яка використовується для створення профілю бізнес-ризику (business risk profile, BRP), який оцінює ризики безпеки організації порівняно з іншими у відповідній галузі.

Заповнення анкети зазвичай займає декілька години, і може припинятися та продовжуватися в будь-який момент. В MSAT передбачено декілька категорій зі зразками питань [36, 44].

1. Основна інформація: «Скільки клієнтів і серверів у вашій організації?».

2. Безпека інфраструктури: «Ваші співробітники працюють віддалено?», «Чи мають зовнішні підрядники доступ до вашої мережі?».

3. Безпека програм: «Чи розробляє ваша організація програми?», «Чи зберігаються у вашій організації конфіденційні дані, оброблені вашими програмами?».

4. Безпека операцій: «Чи підключається ваша корпоративна мережа до зовнішніх мереж?», «Чи отримує ваша організація канали даних від зовнішніх сторін?».

5. Безпека людей: «Чи виконує ваша організація обслуговування комп'ютерів аутсорсингом?», «Чи дозволяєте ви працівникам завантажувати конфіденційні дані компанії на свої робочі станції?»,

6. Навколишнє середовище: «Скільки співробітників у вашій організації?», «Чи велика плинність кадрів у вашому відділі IT?».

Далі MSAT генерує оцінку, яка використовує вимірювання, що називається індексом глибокого захисту (defense-in-depth index, DiDI), який зосереджується на запроваджених в організації процесах безпеки. Для цього використовуються ті самі категорії з типовими запитаннями: «Чи використовує ваша організація брандмауери на кожному робочому місці?»,

«Ви використовуєте спеціальні макроси у своїх програмах Microsoft Office?», «Чи мають ваші користувачі права адміністратора на своїх робочих станціях?», «Чи є у вас політика щодо розгортання виправлень і оновлень на ваших ПК?».

На основі отриманих відповідей MSAT пропонує три звіти: підсумковий (summary report), повний (complete report) і порівняльний (comparison report).

Підсумковий звіт (рис. 2.7) відображає гістограму з результатами.

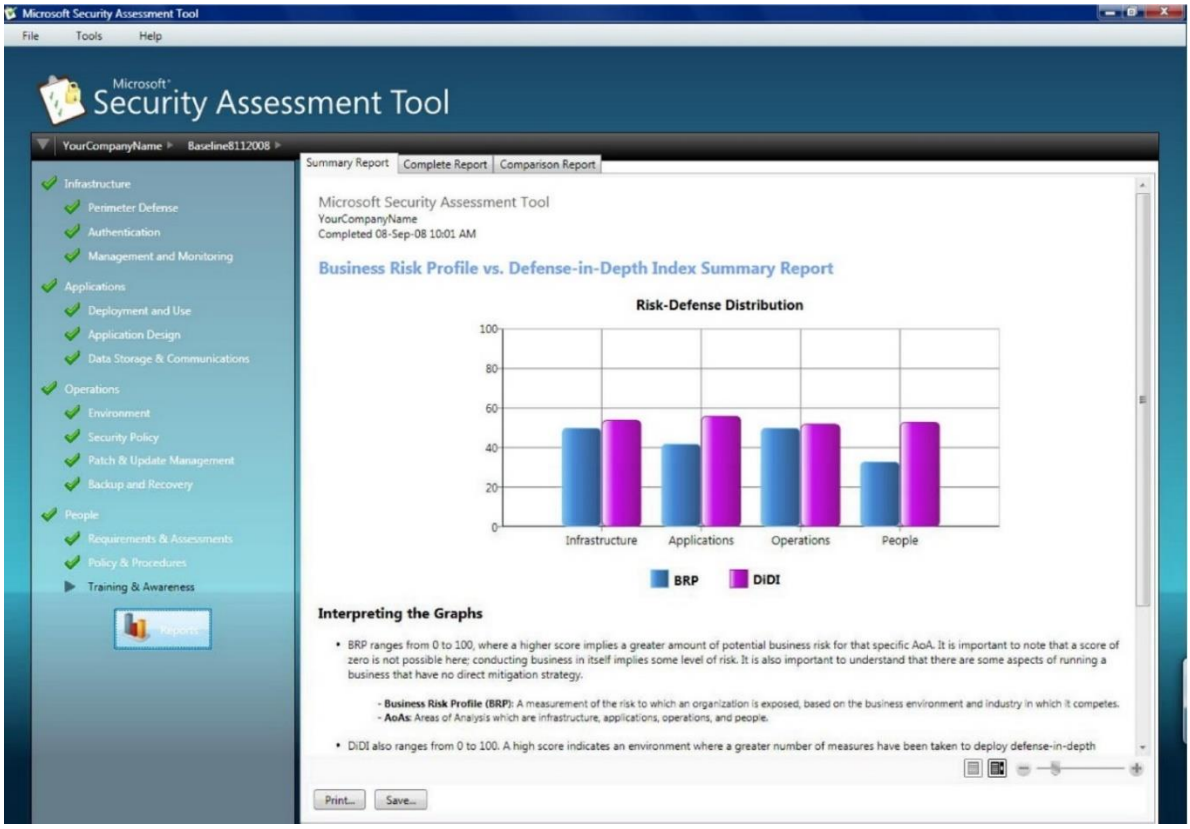


Рисунок 2.7 – Підсумковий звіт [44]

Високий бал у BRP означає більший ризик, тоді як високий бал у DiDI означає більшу безпеку. Як зазначає MSAT, хоча низький BRP і високий DiDI можуть здаватися кращими, насправді важливіше вивчати окремі області. Повний звіт вказує на те, чи відповідає безпека організації найкращим практикам, чи потребує їх удосконалення чи їх серйозно бракує.

Нарешті, порівняльний звіт, використовуючи безпечний веб-сайт MSAT, дає можливість порівняти свої результати з результатами інших організацій.

Основними перевагами MSAT є:

– дозволяє оцінити ефективність інвестицій, вкладених у впровадження заходів безпеки;

– надає нормативні вказівки на основі стандартів безпеки ISO|IEC 27002 та NIST-800;

– має безкоштовну ліцензію та зручний інтерфейс.

Основними недоліками цієї методології оцінки ризиків є наступні:

– не дає можливості знайти оптимальний баланс між заходами, спрямованими на запобігання, виявлення, виправлення або відновлення інформаційних активів;

– не надає кількісної оцінки ризиків;

– не розрахована на крупні компанії.

2.4.4 CORAS

Система консультативного об’єктивного аналізу ризиків (Consultative Objective Risk Analysis System, CORAS) – це метод оцінки ризиків, який відповідає вимогам стандартів ISO/IEC 27005 та AS/NZS 4360 [39]. Метод оцінки ризику CORAS є напівкількісним, часовим та об’єктно-орієнтованим методом ISRA (information security risk assessment), який побудований на уніфікованій мові моделювання (Unified modeling language, UML). Його операційний підхід базується на створенні діаграм для представлення зв’язків і взаємозв’язків між ресурсами, ризиками та загрозами (рис. 2.8).

У методі CORAS аналіз ризиків безпеки проводиться в сім кроків [42].

Крок 1: перший крок передбачає ознайомчу зустріч. Основним пунктом порядку денного цієї зустрічі є те, щоб представники клієнта представили свої загальні цілі аналізу та мету. Таким чином, на початковому

етапі аналітики збиратимуть інформацію на основі презентацій та обговорень клієнта.

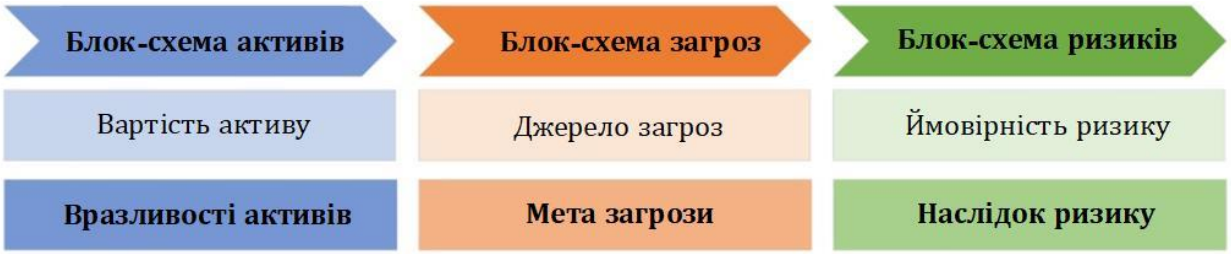


Рисунок 2.8 – Діаграма базової структури CORAS [42]

Крок 2: другий крок також передбачає окрему зустріч з представниками клієнта. Однак, цього разу аналітики представлять своє розуміння того, що вони дізналися під час першої зустрічі та вивчивши документацію, надану їм клієнтом. Другий крок також передбачає приблизний аналіз безпеки високого рівня. Під час цього аналізу визначаються перші загрози, уразливості, сценарії загроз і небажані інциденти. Вони будуть використані для допомоги в спрямуванні та визначенні обсягу більш детального аналізу, який ще має відбутися.

Крок 3: третій крок передбачає більш точний опис цілі, що підлягає аналізу, а також усі припущення та інші попередні умови. Крок третій припиняється, коли вся ця документація буде затверджена клієнтом.

Крок 4: цей крок організовано як семінар, залучений від людей, які мають досвід роботи з метою аналізу. Мета полягає в тому, щоб визначити якомога більше потенційних небажаних інцидентів, а також загроз, вразливостей і сценаріїв загроз.

Крок 5: п’ятий крок також організований як семінар. Цього разу для оцінки наслідків і значень ймовірності для кожного з виявлених небажаних інцидентів.

Крок 6: цей крок дає клієнту першу загальну картину ризику. Це, як правило, ініціює деякі налаштування та виправлення.

Крок 7: останній крок присвячений визначенню обробки, а також вирішенню питань співвідношення витрат і вигоди від обробки. Цей крок найкраще організувати у вигляді семінару.

Переваги цієї методології оцінки ризиків є такі [39, 42]:

– це методологія оцінки ризику на основі моделі (model-based risk assessment, MBRA), що об’єднує аспекти методів оцінки ризику та найсучаснішу методологію моделювання з використання мови UML;

– методологія містить багато автоматизованих процедур, що збільшує використання CORAS для об'єктно-орієнтованих проектів.

Основними недоліками цієї методології є:

– методологія є узагальненою; отже, все ще існує потреба в розробці або розширенні методології для конкретного кроку вимог;

– у CORAS чітко не зазначено, як відображається серйозність загроз і вразливостей. Тому необхідно переглянути цю перспективу;

– CORAS не може надати кількісну оцінку ризику. Отже, необхідно розширити цю методологію в цьому напрямку.

2.4.5 RiskWatch

Програмне забезпечення RiskWatch представляє собою сімейство утиліт, побудованих на спільному програмному ядрі на основі стандартів ISO/IEC 27001, 27002, NIST 800, які моделюють процеси управління різними видами ризиків [36, 45].

Оцінка та управління ризиками в RiskWatch визначається двома критеріями: очікуваними річними втратами (annual loss expectancy, ALE) та оцінкою повернення інвестицій (return on investment, ROI).

RiskWatch надає точну кількісну оцінку співвідношення втрат від дії загроз безпеки та затрат на впровадження системи захисту.

За допомогою RiskWatch можна проаналізувати ризики та зробити обґрунтований вибір заходів та засобів захисту. Методика, що використовується в програмі, включає чотири етапи.

На першому етапі визначається предмет дослідження: тип організації, склад досліджуваної системи (загалом) (рис. 2.9), основні вимоги у сфері безпеки.

На другому етапі вводяться дані, які описують конкретні характеристики системи. Для виявлення можливих вразливостей використовується анкетування з базою, що містить понад 600 питань, пов'язаних з категоріями ресурсів.

Третій етап – це визначення кількісної оцінки ризику: розрахунок профілю ризиків та вибір заходів безпеки.

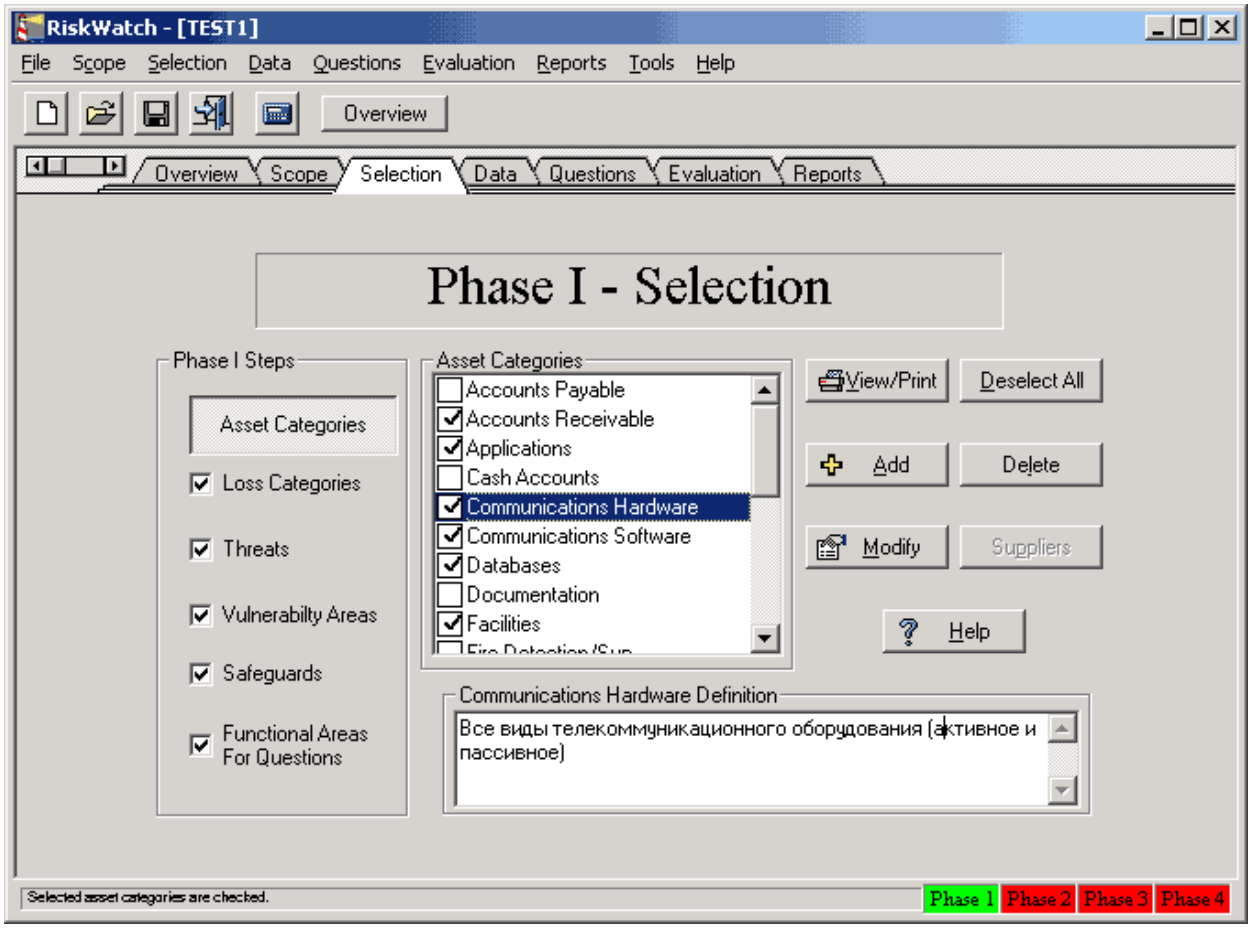


Рисунок 2.9 – Опис ресурсів інформаційної системи [45]

На четвертому етапі створюються звіти.

Основними перевагами RiskWatch є [46]:

– точне кількісне оцінювання ризиків;

– можливість програмної реалізації;

– забезпечення відповідності вимогам стандартів.

До недоліків RiskWatch можна віднести [46]:

– не враховує організаційних та адміністративних факторів;

– велика вартість ліцензії.

В таблиці 2.5 представлена порівняльна характеристика розглянутих засобів оцінки ризиків.

Таблиця 2.5 – Порівняння програмного інструментарію для управління ризиками ІБ [36, 39, 47]

КРИТЕРІЇ ПОРІВНЯННЯ	**CRAMM**	OCTAVE	**Risk Watch**	**CORAS**	**MSAT**
1	**2**	3	**4**	**5**	6
Ризики					
Використання категорій ризиків	+	+	+	+	+
Використання поняття максимально допустимого ризику	+	+	+	+	+
Підготовка плану заходів щодо зниження ризиків	+	+	+	–	+
Управління					
Інформування керівника	+	+	+	+	+
План робіт по зниженню ризиків	–	+	+	–	+
Включає проведення тренінгів, семінарів, зборів	–	+	+	–	+
Оцінка бізнес-ризиків / операційних ризиків / ІТ-ризиків	–	+	+	+	–
Оцінка ризиків на організаційному рівні	+	+	–	+	+
Оцінка ризиків на технічному рівні	+	+	+	+	+
Пропоновані способи зниження ризиків					
Обхід (усунення) ризику	–	–	+	–	–
Зниження ризику	+	+	+	+	+
Прийняття ризику	–	+	–	+	+
Процеси					
Використання елементів ризику					
Матеріальні активи	+	+	+	+	+
Нематеріальні активи	+	+	+	+	+
Загрози	+	+	+	+	+

Продовження таблиці 2.5

1	**2**	3	**4**	**5**	6
Цінність активів	+	+	+	+	+
Вразливості	+	+	+	+	+
Заходи безпеки	+	+	+	–	+
Потенційний збиток	+	+	+	+	+
Імовірність реалізації загроз	+	–	+	+	+
Типи ризиків, що розглядаються					
Бізнес-ризики	–	+	+	+	–
Ризики, пов'язані з порушенням законодавчих актів	–	–	–	–	+
Ризики, пов'язані з використанням технологій	–	+	–	+	+
Комерційні ризики	+	+	+	+	+
Ризики, пов'язані з залученням третіх осіб	+	+	+	+	+
Ризики, пов'язані з залученням персоналу	+	+	–	+	+
Повторні оцінки ризиків	–	+	+	–	+
Визначення правил прийняття ризиків	–	–	–	–	+
Способи вимірювання величини ризиків					
Якісна оцінка	+	+	–	+	+
Кількісна оцінка	+	–	+	–	–
Способи управління					
Якісне ранжування ризиків	+	+	+	+	+
Кількісне ранжування ризиків	–	–	+	–	–
Використання незалежної оцінки	–	+	–	+	+
Розрахунок повернення інвестицій	–	–	–	–	–

2.5 Висновки до розділу 2

За підсумками проведеного аналізу методів та засобів оцінки ризиків інформаційної безпеки можна зробити наступні висновки.

1. Використання вербальних/лінгвістичних змінних в якісних підходах (засобах) дає більш доступне (наочне) подання інформаційних процесів в організації. При цьому до оцінки рівня ризиків можуть залучатися не тільки фахівці з безпеки, але й інші зацікавлені сторони.

2. Для кількісного представлення рівня ризику найчастіше використовується два показники – ймовірність реалізації загрози та значення (як правило вартісне) збитку, який понесла організація.

3. З практичної точки зору, змішані методики (засоби) дають об’єктивнішу оцінку рівня ризику ніж строго якісні чи кількісні.

Загальним недоліком всіх розглянутих підходів є те, що достовірність отриманих результатів оцінки ризику є суб’єктивною так як залежить від думок експертів (іноді діаметрально протилежних).

3 МОДЕЛЮВАННЯ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ В СЕРЕДОВИЩІ CORAS

Методологія CORAS, призначена для аналізу ризиків безпеки, надає інструмент для моделювання (оцінки) ризиків і загроз, які можуть виникати протягом всього часу роботи організації. Програмне забезпечення CORAS використовує уніфіковану мову моделювання UML [48].

UML – це відкритий стандарт, який використовує графічні позначення для створення абстрактної моделі системи.

3.1 Елементи інтерфейсу CORAS

У програмному забезпеченні CORAS використовуються десять графічних елементів [48], представлених в таблиці 3.1.

Таблиця 3.1 – Елементи програми CORAS

Вигляд елемента	Назва англійською мовою	Назва українською мовою
	Asset	Цінність, інформація, що підлягає захисту
	Stakeholder	Зацікавлені сторони
	Threat Human Accidental	Загроза ненавмисна, людського походження
	Threat Human Deliberate	Загроза навмисна, людського походження
	Threat Non Human	Загроза нелюдського походження
	Threat Scenario	Сценарій загрози
	Vulnerability	Вразливість
	Unwanted Incident	Небажаний інцидент
	Risk	Ризик
	Treatment	Протидія загрозі

На рисунку 3.1 представлено головне вікно програми.

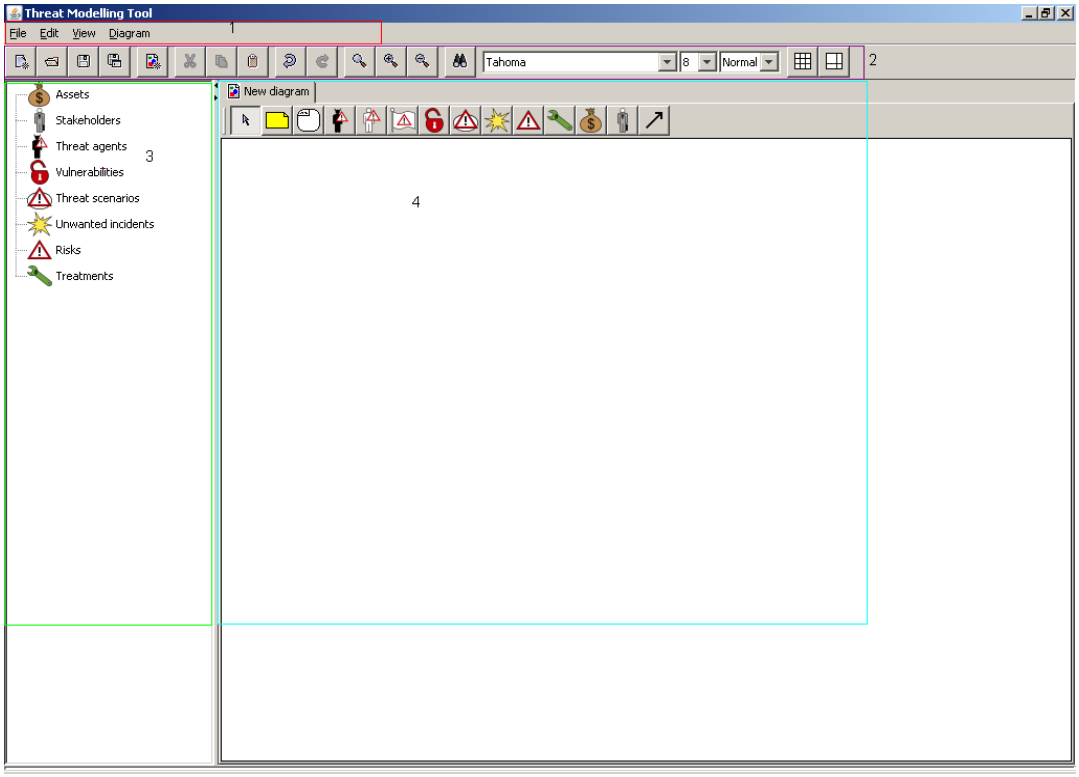


Рисунок 3.1 – Головне вікно програми CORAS

3.2 Моделювання ризиків інформаційної системи IT-компанії

Об’єктом дослідження є центр розробки програмного забезпечення (IT-компанія), яка являє собою приміщення з тринадцяти кімнат: сім кімнат розробників, кімната менеджерів, кімната керівництва, яка також виконує функцію приймальної, кухня, їдальня, кімната відпочинку та туалетна кімната. Приміщення розташоване на першому поверсі бізнес-центру (рис. 3.2).

Передбачається, що в компанії можуть виникати проблеми захисту комерційної інформації, персональних даних співробітників та клієнтів в центрі розробки програмного забезпечення, а також авторської інформації (розроблене програмне забезпечення).

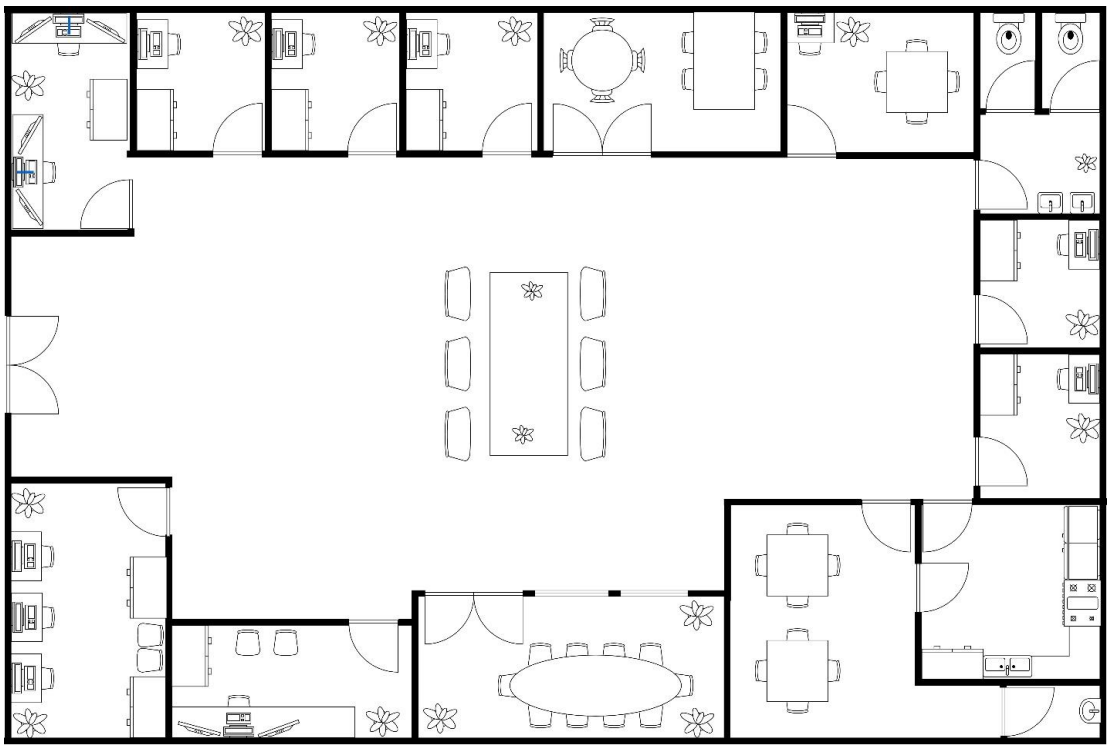


Рисунок 3.2 – Схема приміщення центру розробки програмного забезпечення

Для обробки захищуванної інформації використовується 12 комп'ютерів, які мають доступ до мережі Інтернет. Провідна мережа заснована на оптоволокні, що виключає можливість зняття інформації з кабелю.

Кожному розробнику видаються база знань, яка розташована на хмарному сервісі Notion, доступ до віддалених репозиторіїв з кодом програмного забезпечення.

На об'єкті використовуються наступні заходи щодо захисту інформації.

1. Вікна ретельно герметизовані монтажною піною.
2. Вікна захищені тонувальною плівкою.
3. Двері з використанням ключ-карти.
4. За вхідними дверима розташовані двері-решітка.
5. Система сигналізації.
6. Протипожежна система.

7. Система відеоспостереження.

8. Всі комп’ютери захищені паролем.

9. Використовується ліцензійне ПЗ.

10. На всіх комп’ютерах встановлена антивірусна система, яка оновлюється не рідше ніж раз на місяць.

11. Весь персонал найнятий за договором із застосуванням пункту, що гарантує збереження комерційної таємниці.

Персонал компанії складається з постійного складу:

– керівник;

– 2 менеджери;

– 8 розробників;

– розробник, який виконує функції адміністратора мережі;

– прибиральниця.

Використовуючи програмний продукт CORAS, складемо схему активів (цінної інформації, що підлягає захисту)(рис. 3.3, 3.4):

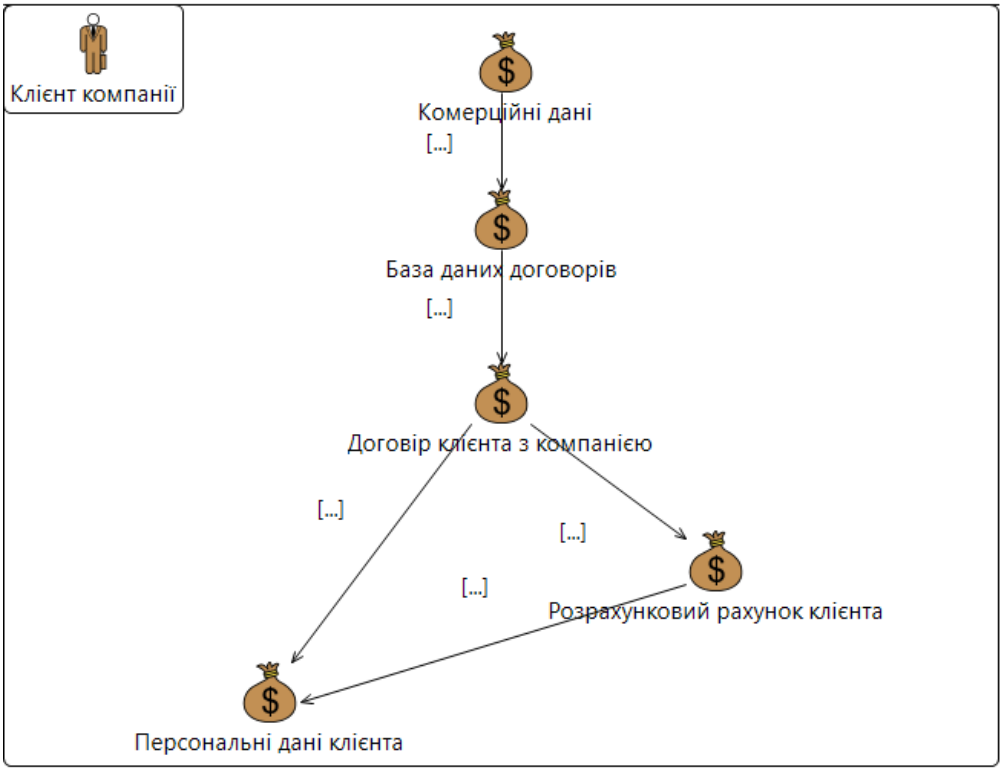


Рисунок 3.3 – Діаграма активів відносно клієнта компанії

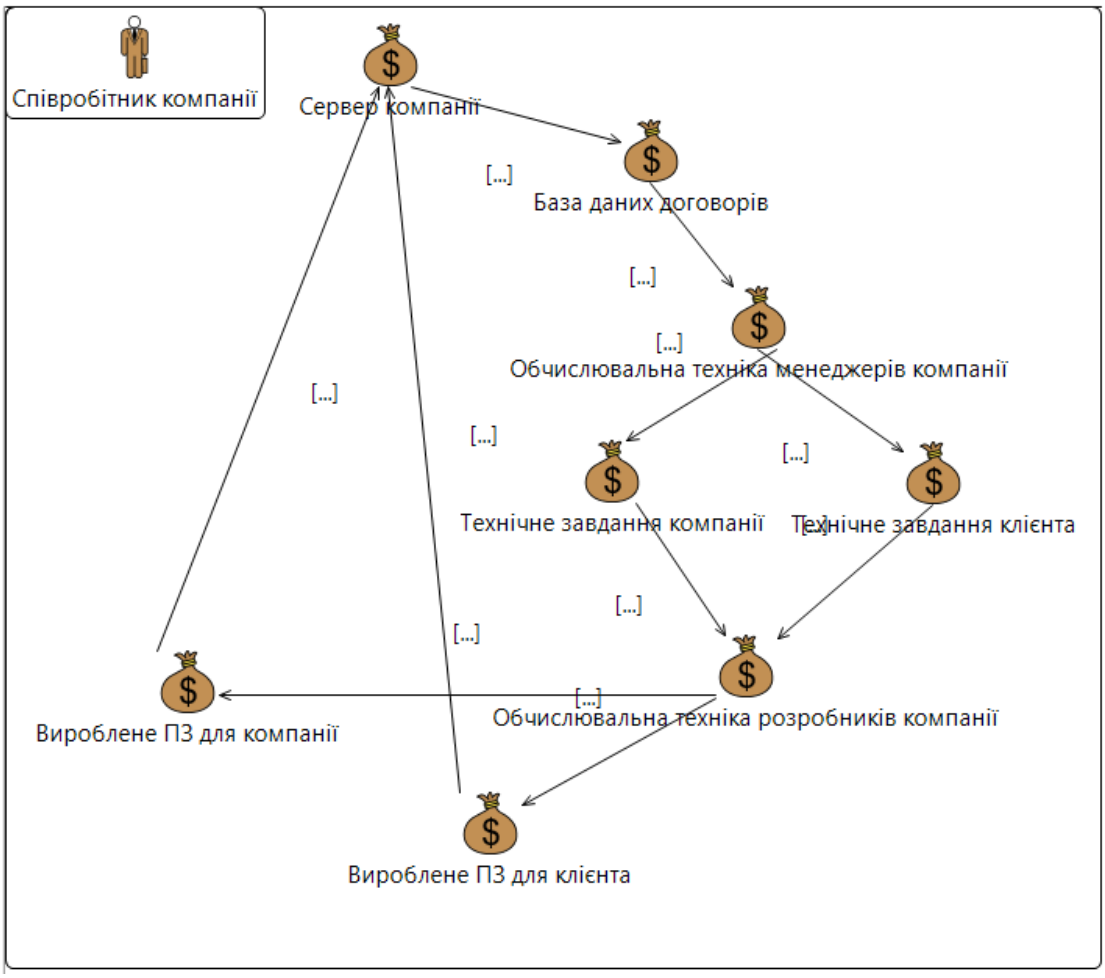


Рисунок 3.4 – Діаграма активів відносно співробітника компанії

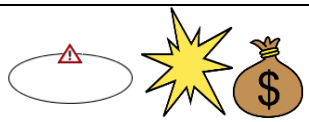
Складемо таблицю 3.2 для повного опису моделі ризиків з використанням інформації щодо захисту об'єкта та матрицю ризиків, в якій стовпці є шкалою наслідків небажаних інцидентів, а рядки – ймовірністю настання даного інциденту, або його частоти (рис. 3.5).

Бажано для кожного активу за кожною шкалою скласти опис: що значить рідко, іноді, регулярно і часто в кількісному відношенні за певний період часу тощо.

Далі в матриці ризиків (рис. 3.5) вносяться дані відповідно до того, який є ризик: прийнятний чи ні.

Завдяки зробленим зв'язкам між активами, можна вказувати вплив на більш загальний актив, якщо даний інцидент можливий для кожного «підактива».

Таблиця 3.2 – Таблиця потенційних ризиків

 Хто / що причина?	 Як? Який інцидент? Чому загрожує?	 Завдяки чому стала можливим - вразливість.
Порушник	Розкрадання інформації з сервера	Відсутність шифрування
	Несанкціоноване копіювання інформації	Помилки в розмежуванні доступу
	Розкрадання апаратури	Можливість доступу до систем відеоспостереження
	Запис мовної інформації	Диктофон
Системні збої	Втрата інформації	Відсутність копії
Вірус, закладні пристрої	Втрата інформації	Помилки користувачів
	Несанкціоноване отримання віддаленого доступу	Відсутність антивірусного ПЗ
Персонал	Установка свого ПЗ	Політика безпеки
	Копіювання інформації на носії	Простий пароль
	Доступ до інформації, що захищається	Помилки адміністратора
	Втрата інформації	Помилки користувача

Підсумком цього етапу є ймовірність і вага наслідків, об'єднаних в матрицю ризиків, за якою стає зрозуміло який ризик є прийнятним, а який ні.

		Шкала наслідків небажаних інцидентів			
		Незначні	Мінімальні	Середні	Катастрофічні
Імовірнісна шкала	Рідко	Прийнятний	Прийнятний	Прийнятний	Неприйнятний
	Іноді	Прийнятний	Прийнятний	Неприйнятний	Неприйнятний
	Регулярно	Прийнятний	Неприйнятний	Неприйнятний	Неприйнятний
	Часто	Неприйнятний	Неприйнятний	Неприйнятний	Неприйнятний

Рисунок 3.5 – Матриця ризиків

Використовуючи таблицю 3.2, будуємо модель загроз з ймовірнісними характеристиками, зображену на рис. 3.6.

Далі, використовуючи вкладку «Generate risk diagram», генеруємо діаграму ризиків з характеристикою наслідків загрози (рис. 3.7).

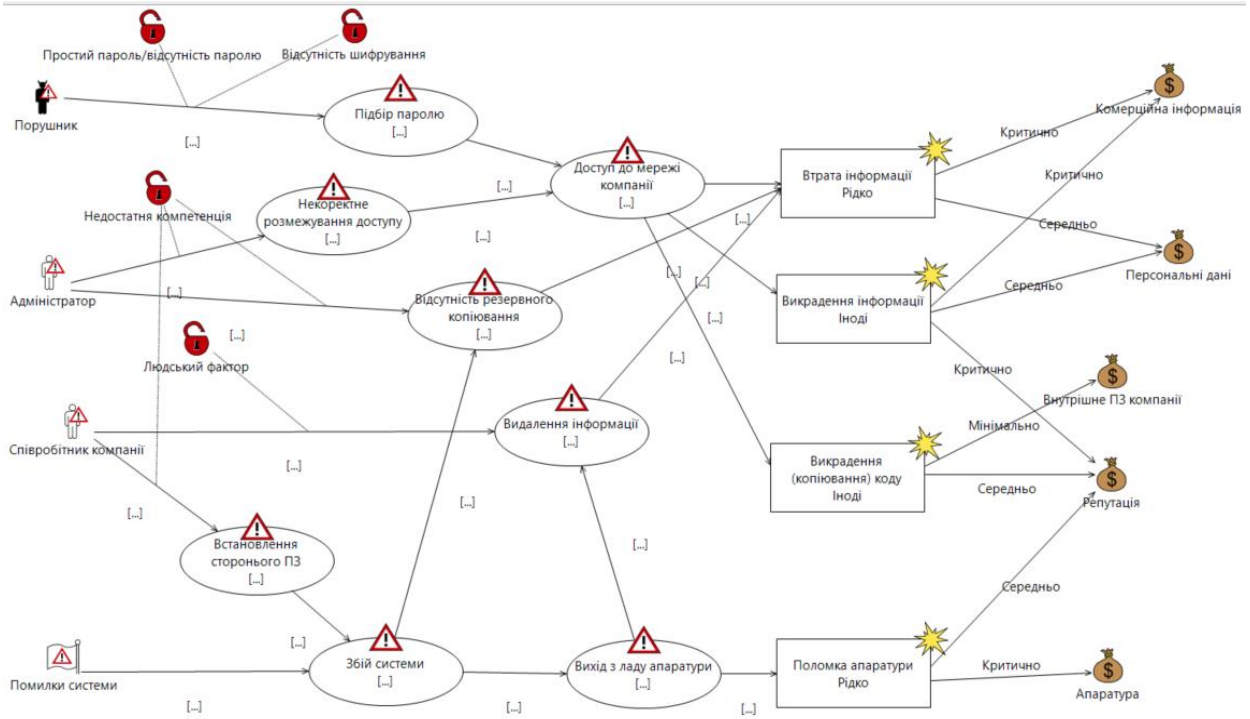


Рисунок 3.6 – Модель загроз з ймовірними характеристиками

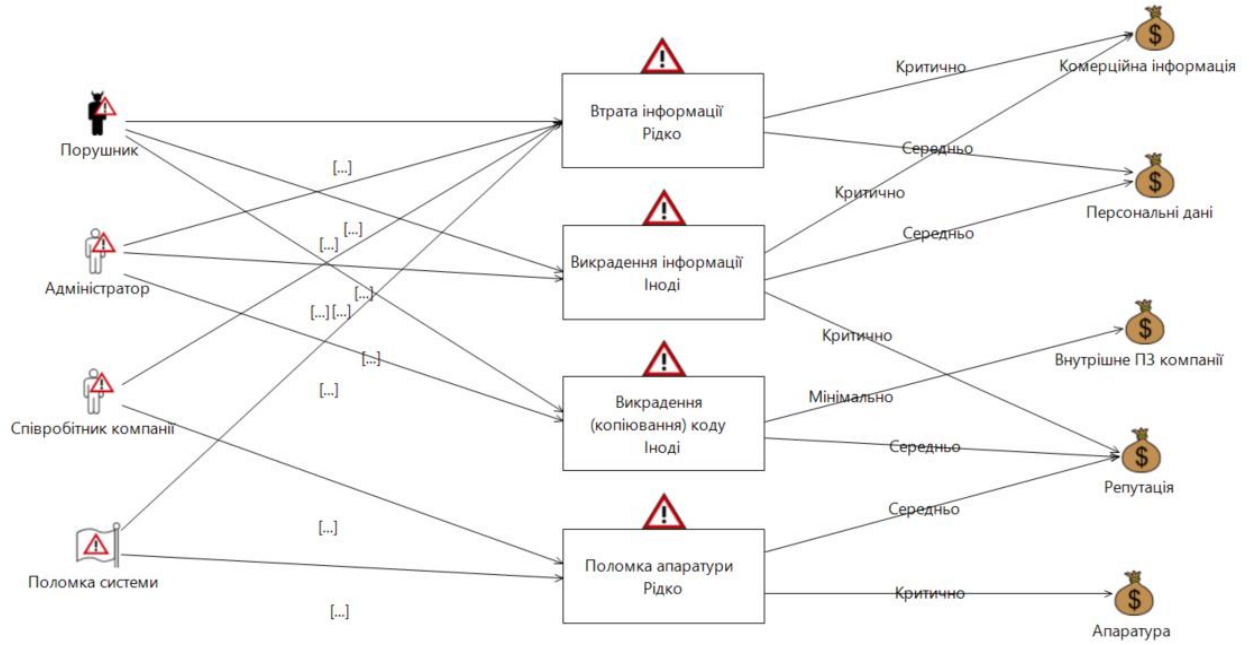


Рисунок 3.7 – Діаграма ризиків з характеристикою наслідків загрози

Відповідно до діаграми ризиків (рис. 3.7) та матриці ризиків (рис. 3.5), заносимо отриману інформацію до матриці ризиків після контрзаходів (рис. 3.8).

		Шкала наслідків небажаних інцидентів			
		Незначні	Мінімальні	Середні	Катастрофічні
Імовірнісна шкала	Рідко			Втрата персональних даних; Поломка апарату-ри з втратою репутації;	Втрата комерційної інформації; Поломка апаратури;
	Іноді		Копіювання коду внутрішнього ПЗ компанії	Викрадення персональних даних; Копіювання коду внутрішнього ПЗ компанії з втратою репутації	Викрадення комерційної інформації; Викрадення інформації з втра-тою репутації;
	Регулярно				
	Часто				

Рисунок 3.8 – Матриця ризиків після додавання контрзаходів

На діаграмі загроз для кожної вразливості ставимо контрзахід (рис. 3.9).

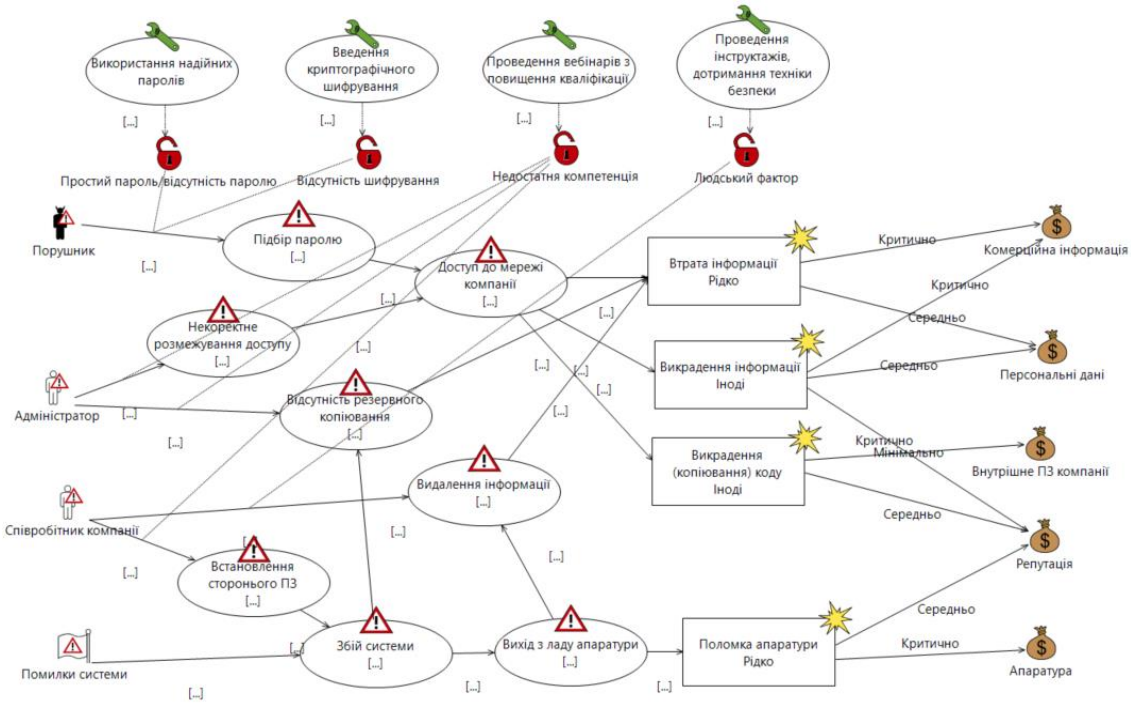


Рисунок 3.9 – Діаграма загроз після додавання контрзаходів

Вносячи правки, відповідно до рис. 3.8, отримаємо наступну діаграму неприйнятних ризиків (рис. 3.10).

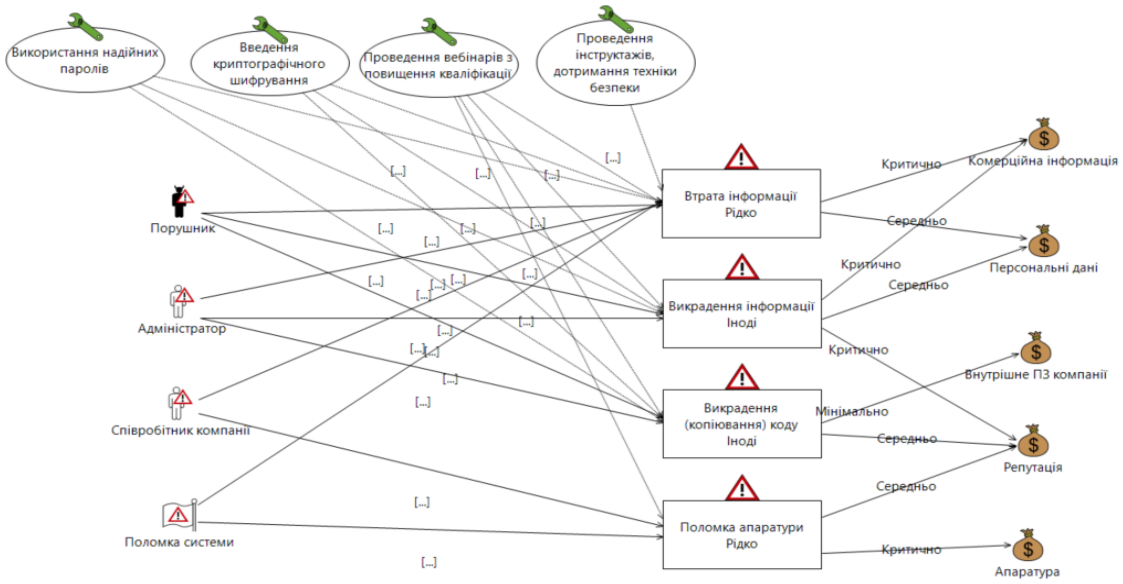


Рисунок 3.10 – Діаграма неприйнятних ризиків

На підставі діаграми неприйнятних ризиків можна запропонувати наступні контрзаходи в порядку впливу на ризики: ведення криптографічного шифрування; використання надійних паролів; проведення вебінарів з підвищення кваліфікацій; проведення інструктажів з дотримання техніки безпеки.

3.3 Висновки до розділу 3

Було промодельовано ризики і загрози інформаційній безпеці в IT-компанії з використанням середовища CORAS. Середовище CORAS дає можливість оцінити ризики на якісному рівні з використанням кольорових матриць ризику.

Процес побудови моделей можна охарактеризувати як зручний, але не для організацій зі значною номенклатурою активів. Для аналізу дії загроз великих компаній, методика CORAS буде громіздкою, а побудовані діаграми – нечитабельними.

ВИСНОВКИ

В магістерській роботі розглянуті базові стандарти в сфері управління та оцінки ризиків інформаційної безпеки, що визначають вимоги до засобів захисту та надають рекомендації щодо використання тих чи інших методів аналізу та обробки ризиків.

Для досягнення поставленої мети, в результаті опрацювання вітчизняної та зарубіжної наукової літератури, були проведені теоретичні та практичні дослідження:

– проведений огляд міжнародних стандартів серії ISO/IEC 2700x, ISO 31000, IEC 31010;

– предметно розглянуті національні стандарти США, Великобританії та Австралії/Нової Зеландії, на основі яких розроблені програмні засоби оцінки ризиків;

– досліджені якісні, кількісні та змішані методи та засоби аналізу та оцінки ризиків інформаційної;

– виконано моделювання процесів управління можливих ризиків IT-компанії в середовищі CORAS.

За результатами проведеного дослідження можна стверджувати, що наявні стандарти управління ризиками надають організаціям ефективні інструменти контролю інформаційної безпеки з метою зменшення ризиків, які можуть вплинути на їх прогрес.

Загальним недоліком всіх розглянутих методів і засобів оцінки ризиків є те, що достовірність отриманих результатів оцінки ризику безпосередньо залежить від суб’єктивних думок експертів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Розробка основи стратегії аналізу ризиків для оцінки впливу в системах управління інформаційної безпеки. URL: https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informaczijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltyngu-chastyna-2/ (дата звернення: 09.09.2023).

2. Єрмошин В. В., Невойт Я. В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем. *Сучасний захист інформації*. 2014. № 3. С. 26 –29.

3. Боровик М. В. Ризик-менеджмент: конспект лекцій для студентів магістратури усіх форм навчання спеціальності 073 – Менеджмент. Харків: ХНУМГ ім. О. М. Бекетова, 2018. 65 с.

4. ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (last accessed: 09.09.2021).

5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en (last accessed: 10.09.2023).

6. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements *(third edition)*. URL: https://www.iso27001security.com/html/27001.html (last accessed: 10.09.2021).

7. A summary of ISO 27001 requirements for information security. URL: https://ictinstitute.nl/iso-27001-requirements-summary/ (last accessed: 09.09.2021).

8. Information security and PDCA (Plan-Do-Check-Act). URL: https://ictinstitute.nl/pdca-plan-do-check-act/ (last accessed: 12.09.2021).

9. How to implement an ISMS using ISO 27001. URL: https://digitaloctopii.com/blog/what-is-isms/how-to-implement-isms-iso-27001/ (last accessed: 12.09.2021).

10. Plan – Do – Check – Act ISO 27001. URL: https://isocouncil.com.au/plan-do-check-act-iso-27001/ (last accessed: 12.09.2021).

11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en (last accessed: 12.09.2023).

12. ISO/IEC 27002:2022 – Information Security Controls. URL: https://blog.ansi.org/iso-iec-27002-2022-information-security-controls/#gref (last accessed: 14.09.2023).

13. Андре Секель Перегляд ISO 27002. Є зміни. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/pereglyad-iso-27002.-e-zmini (дата звернення: 15.09.2023).

14. ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls (third edition). URL: https://www. iso27001security.com/html/27002.html (last accessed: 15.09.2023).

15. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.scribd.com/document/634149413/ISO-IEC-27005-2022-en (last accessed: 18.09.2023).

16. Everything you need to know about ISO 27005: summary, requirements, pros and cons. URL: https://www.c-risk.com/blog/iso-27005 (last accessed: 18.09.2023).

17. ISO/IEC 27005:2022: Main Changes and Implications. URL: https://pecb.com/article/isoiec-270052022-main-changes-and-implications (last accessed: 18.09.2023).

18. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks (*fourth edition*). URL: https://www.iso27001security.com/html/27005.html (last accessed: 20.09.2023).

19. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). [Чинний від 2019-01-01]. URL: https://www.iso.org/obp/ui/ #iso:std:iso:31000:ed-2:v1:en (дата звернення: 20.09.2023).

20. Risk management ISO 31000. URL: https://www.iso.org/files/live/ sites/isoorg/files/store/en/PUB100426.pdf (last accessed: 20.09.2023).

21. IEC 31010:2019 Risk management – Risk assessment techniques. URL: https://www.scribd.com/document/434742728/IEC-31010-2019 (last accessed: 20.09.2023).

22. ISO 31010 and Implementing Risk Assessment Techniques. URL: https://www.linkedin.com/pulse/iso-31010-implementing-risk-assessment-techniques-lazarus-alliance (last accessed: 20.09.2023).

23. An Introduction to IEC 31010. URL: https://www.risksandventures.com/ 2020/02/09/iec31010-introduction/ (last accessed: 21.09.2023).

24. NIST Special Publication 800-series General Information. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information (last accessed: 21.09.2023).

25. NIST Technical Series Publication List. URL: https://pages.nist.gov/ NIST-Tech-Pubs/SP800.html (last accessed: 21.09.2023).

26. NIST Risk Management Framework. URL: https://csrc.nist.gov/ projects/risk-management/about-rmf (last accessed: 21.09.2023).

27. Calder A., Watkins S. IT Governance: A Manager's Guide to Data Security and BS 7799/IS0 17799: 3rd edition. London and Sterling, VA: Kogan Page Business Books, 2005. 272 p.

28. BS 7799-3-2006. URL: https://www.scribd.com/document/96574973/BS-7799-3-2006 (last accessed: 21.09.2023).

29. Revision of BS 7799-3:2017 - Information security management systems - Guidelines for information security risk management. URL: https://standardsdevelopment.bsigroup.com/projects/9023-09086#/section (last accessed: 21.09.2023).

30. AS/NZS 4360:2004. Risk management. URL: http://mkidn.gov.pl/media/docs/pol_obronna/20150309_3-NZ-AUST-2004.pdf (last accessed: 09.09.2023).

31. Ionita D., Hartel PH., Pieters W., Wieringa RJ. Current Established Risk Assessment Methodologies and Tools. URL: https://www.researchgate.net/publication/308887387_Current_Established_Risk_Assessment_Methodologies_and_Tools?channel=doi&linkId=57f4c32608ae91deaa5c3ab1&showFulltext=true (last accessed: 24.09.2023).

32. Причинно-наслідковий діаграма (діаграма Ісікави). URL: https://stud.com.ua/34613/tovaroznavstvo/prichinno_naslidkoviy_diagrama_diagrama_isikavi (дата звернення: 05.10.2023).

33. Застосування ризик орієнтованого підходу для побудови імовірнісних структурно-логічних моделей виникнення та розвитку НС. URL: https://www.shevchenkove.org.ua/person_syte/Lusak/БЖД електронний посібник/ Dokument/Lekzia/Лекція №7.htm (дата звернення: 05.10.2023).

34. Creating a Risk Matrix: 3 Examples. URL: https://www.etq.com/blog/creating-a-risk-matrix-3-examples/ (last accessed: 05.10.2023).

35. Бідюк П.І., Терентьєв О.М., Коновалюк М.М. Байєсівські мережі в технологіях інтелектуального аналізу даних // Вісник Чорноморського державного університету ім. Петра Могили, 2010, с. 6-16.

36. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ: ЦП «Компринт», 2017 – 435 с.

37. System Reliability Theory. URL: https://www.ntnu.edu/ross/books/srt (last accessed: 10.10.2023).

38. A comparative analysis of risk assessment techniques from the risk management perspective. URL: https://www.matec-conferences.org/articles/matecconf/pdf/2019/39/matecconf_mse2019_12003.pdf (last accessed: 12.10.2023).

39. Pandey S. K., Mustafa K. A Comparative Study of Risk Assessment Methodologies for Information Systems. URL: https://www.academia.edu/37068951/A_Comparative_Study_of_Risk_Analysis_Methodologies_for_Information_Security (last accessed: 12.10.2023).

40. 10 Steps to do it yourself CRAMM. URL: https://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm (last accessed: 09.10.2023).

41. A qualitative risk analysis and management tool – CRAMM. URL: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysis-management-tool-cramm/103133 (last accessed: 14.11.2023).

42. When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method. URL: https://www.mdpi.com/2071-1050/15/12/9812 (last accessed: 14.11.2023).

43. Гаркуша В.О. Методичний підхід до оцінки ризиків інформаційної безпеки підприємства. URL: http://pev.kpu.zp.ua/journals/2020/2_19_ukr/17.pdf (дата звернення: 15.11.2023).

44. Microsoft Security Assessment Tool. URL: https://download.microsoft.com/documents/uk/security/msat/Customer_User_Guide.pdf (last accessed: 15.11.2023).

45. Методика RiskWatch. URL: https://stud.com.ua/179802/informatika/metodika_riskwatch (дата звернення: 15.11.2023).

46. Пугин В. Г., Губарева О. Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия. URL: https://cyberleninka.ru/article/n/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya (дата звернення: 15.11.2023).

47. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности. URL: https://cyberleninka.ru/article/n/metodiki-analiza-i-otsenki-riskov-informatsionnoy-bezopasnosti (дата звернення: 20.11.2023).

48. The Coras Method. URL: https://CORAS.sourceforge.net/index.html (last accessed: 20.11.2023).

ДОДАТОК А

Терміни та визначення
(відповідно до ISO/IEC 27000)

автентичність (authenticity) – властивість того, що суб’єкт є тим, за кого/що себе видає;

аналіз ризиків (risk analysis) – процес для розуміння природи ризику та визначення рівня ризику. Аналіз ризику забезпечує основу для оцінки ризику і прийняття рішень щодо обробки ризику;

атака (attack) – спроба знищити, розкрити, змінити, вивести з ладу, викрасти або отримати несанкціонований доступ або несанкціоноване використання активу;

аудит (audit) – систематичний, незалежний і задокументований процес для отримання доказів перевірки та їх об'єктивної оцінки для визначення ступеня дотримання критеріїв аудиту: може бути внутрішній, зовнішній або комбінований аудит;

аутентифікація (authentication) – надання впевненості в тому, що заявлена характеристика суб'єкта є правильною

безперервність інформаційної безпеки (information security continuity) – процеси і процедури забезпечення постійної безпеки інформації;

вище керівництво (top management) – особа або група осіб, які керують і контролюють організацію на найвищому рівні. Вище керівництво (генеральні директори, фінансові директори, інформаційні директори тощо) має право делегувати повноваження та надавати ресурси в межах організації;

власник ризику (risk owner) – фізична чи юридична особа, яка має відповідальність і повноваження керувати ризиком;

вразливість (vulnerability) – слабкість активу або контролю (заходів безпеки), яка може бути використана однією або кількома загрозами;

доступність (availability) – властивість бути доступним і використовуватися на вимогу уповноваженої особи;

загроза (threat) – потенційна причина небажаного інциденту, який може призвести до шкоди системі чи організації;

залишковий ризик (residual risk) – ризик, що залишається після обробки (зменшення) ризику;

засоби обробки інформації (information processing facilities) – будь-яка система обробки інформації, послуга чи інфраструктура або фізичне розташування, у якому вони розміщені;

зіставлення ризику (risk evaluation) – процес порівняння результатів аналізу ризику з критеріями ризику для визначення того, чи є ризик та/або його величина прийнятними чи допустимими;

ідентифікація ризиків (risk identification) – процес пошуку, розпізнавання та опису ризиків. Ідентифікація ризику передбачає ідентифікацію джерел ризику, подій, їх причин та потенційних наслідків. Ідентифікація ризику може включати історичні дані, теоретичний аналіз, експертні думки та потреби зацікавлених сторін;

інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації (також можуть бути

задіяні інші властивості, такі як автентичність, підзвітність, незаперечність та надійність);

інформаційна система (information system) – набір програм, послуг, активів інформаційних технологій або інших компонентів обробки інформації;

інцидент інформаційної безпеки (information security incident) – одна або декілька небажаних або неочікуваних подій інформаційної безпеки, які мають значну ймовірність скомпрометувати бізнес-операції та загрожувати інформаційній безпеці;

керівництво інформаційною безпекою (governance of information security) – система, за допомогою якої діяльність організації у сфері інформаційної безпеки спрямовується та контролюється;

контроль/заходи безпеки (control) – міра, що змінює ризик: засоби контролю включають будь-який процес, політику, пристрій, практику або інші дії, які змінюють ризик;

конфіденційність (confidentiality) – властивість, що інформація не надається або не розкривається неавторизованим особам, організаціям або процесам;

корекція (correction) – дія для усунення виявленої невідповідності;

коригувальні дії (corrective action) – дії для усунення причини невідповідності та запобігання повторенню;

критерії ризику (risk criteria) – технічне завдання, за яким оцінюється значущість ризику. Критерії ризику ґрунтуються на цілях організації та зовнішньому і внутрішньому контексті. Критерії ризику можна отримати зі стандартів, законів, політики та інших вимог;

обробка ризику (risk treatment) – процес для зміни ризику. Обробка ризику може включати:

– уникнення ризику шляхом прийняття рішення не починати або не продовжувати діяльність, яка породжує ризик;

– прийняття або збільшення ризику з метою його подальшого вивчення;

– усунення джерела ризику;

– зміна ймовірності виникнення ризику;

– зміна наслідків;

– розподіл ризику з іншою стороною або сторонами (включаючи контракти та фінансування ризику);

– збереження ризику шляхом усвідомленого вибору.

Методи обробки ризику, які стосуються негативних наслідків, іноді називають «пом’якшенням ризику», «усуненням ризику», «запобіганням ризику» та «зменшенням ризику»;

обговорення ризиків та консультації (risk communication and consultation) – набір безперервних і повторюваних процесів, які організація проводить для надання, обміну або отримання інформації, а також для вступу в діалог із зацікавленими сторонами щодо управління ризиком;

оцінка ризику (risk assessment) – загальний процес ідентифікації ризику, аналізу ризику та оцінки ризику;

перегляд (review) – діяльність, здійснювана для визначення придатності, адекватності та ефективності предмета дослідження для досягнення встановлених цілей;

подія безпеки інформації (information security event) – ідентифікований випадок стану системи, служби чи мережі, що вказує на

можливе порушення політики інформаційної безпеки або збій засобів керування, або раніше невідому ситуацію, яка може мати значення для безпеки;

прийняття ризику (risk acceptance) – інформоване рішення піти на певний ризик. Прийняття ризику може відбуватися без обробки ризику або під час процесу обробки ризику. Прийняті ризики підлягають моніторингу та перегляду;

професіонал системи управління інформаційною безпекою (СУІБ) (information security management system (ISMS) professional) –особа, яка встановлює, впроваджує, підтримує та постійно вдосконалює один або більше процесів системи управління інформаційною безпекою;

процес управління ризиками (risk management process) – систематичне застосування управлінських політик, процедур і практик до діяльності з комунікації, консультування, встановлення контексту та виявлення, аналізу, оцінки, обробки, моніторингу та перегляду ризику;

рівень ризику (level of risk) – величина ризику, виражена в термінах комбінації наслідків та їхньої ймовірності;

ризик (risk) – ефект невизначеності щодо досягнення цілей. У контексті систем управління інформаційною безпекою ризики інформаційної безпеки можна виразити як вплив невизначеності на цілі інформаційної безпеки. Ризик інформаційної безпеки пов’язаний із потенційною можливістю використання загрозами вразливості інформаційного активу або групи інформаційних активів і, таким чином, завдавати шкоди організації.

система управління (management system) – сукупність взаємопов’язаних або взаємодіючих елементів організації для встановлення політики, цілей і процесів для досягнення цих цілей. Елементи системи

включають структуру організації, ролі та обов’язки, планування та функціонування. Сфера застосування системи управління може включати всю організацію, конкретні та визначені функції організації, конкретні та визначені частини організації або одну чи більше функцій у групі організацій.

управління доступом (access control) – засоби для забезпечення авторизації та обмеження доступу до активів відповідно до вимог бізнесу та безпеки;

управління інцидентами інформаційної безпеки (information security incident management) – набір процесів для виявлення, звітування, оцінки, реагування на інциденти інформаційної безпеки, робота з ними та навчання на основі інцидентів інформаційної безпеки;

управління ризиками (risk management) – скоординована діяльність з управління та контролю над організацією щодо ризику;

цілісність (integrity) – властивість точності та повноти;

ціль контролю (control objective) – твердження, що описує, що має бути досягнуто в результаті впровадження заходів контролю.

ДОДАТОК Б

Таблиця Б.1 - Контролі інформаційної безпеки (витяг з ISO/IEC 27001:2022)

5	**Організаційні контролі**	
5.1	Політики інформаційної безпеки	**Заходи безпеки** Політика інформаційної безпеки та тематична політика повинні бути визначені, затверджені керівництвом, опубліковані, доведені до відома та визнані відповідним персоналом і відповідними зацікавленими сторонами, і переглядається через заплановані проміжки часу та, якщо відбуваються значні зміни.
5.2	Ролі інформаційної безпеки та відповідальність	**Заходи безпеки** Ролі інформаційної безпеки та відповідальність мають бути визначені та розподілені відповідно до потреб організації
…	…	…
5.4	Відповідальність керівництва	**Заходи безпеки** Керівництво має вимагати від усього персоналу застосування інформаційної безпеки відповідно до встановленої політики інформаційної безпеки, тематичних політик і процедур організації.
…	…	…
5.19	Інформаційна безпека у відносинах з постачальниками	**Заходи безпеки** Процеси та процедури повинні бути визначені та впроваджені для управління ризиками інформаційної безпеки, пов’язаними з використанням продуктів або послуг постачальника
…	…	…
5.21	Управління інформаційною безпекою в ланцюзі поставок інформаційно-комунікаційних технологій (ІКТ)	**Заходи безпеки** Процеси та процедури повинні бути визначені та впроваджені для управління ризиками інформаційної безпеки, пов’язаними з ланцюгом постачання продуктів і послуг ІКТ.
6	**Контролі персоналу**	
6.1	Відбір	**Заходи безпеки** Перевірка репутації всіх кандидатів на посаду персоналу повинна проводитися до зарахування до організації та на постійній основі з урахуванням чинних законів, нормативних актів та етики, та бути пропорційною вимогам бізнесу, класифікації інформації, до якої потрібно отримати доступ, та передбачувані ризики

Продовження таблиці Б.1

6.2	Умови прийому на роботу	**Заходи безпеки** У трудових договорах повинні бути визначені обов'язки персоналу та організації щодо захисту інформації.
6.3	Інформаційна безпека, освіта та навчання	**Заходи безпеки** Персонал організації та відповідні зацікавлені сторони повинні отримувати належну обізнаність з інформаційною безпекою, освіту та навчання та регулярні оновлення політики організації з інформаційної безпеки, тематичних політик і процедур, відповідно до їх функціональних обов’язків.
…	…	…
7	**Фізичні контролі**	
7.1	Периметри фізичної безпеки	**Заходи безпеки** Периметри безпеки повинні бути визначені та використані для захисту зон, які містять інформацію та інші пов’язані активи.
7.2	Фізичний доступ	**Заходи безпеки** Зони безпеки мають бути захищені відповідними засобами контролю входу та точками доступу.
7.3	Охорона офісів, приміщень та приміщень	**Заходи безпеки** Фізична охорона офісів, приміщень і приміщень має бути спроектована та впроваджена.
…	…	…
8	**Технологічні контролі**	
8.1	Кінцеві пристрої користувачів	**Заходи безпеки** Інформація, яка зберігається на кінцевих пристроях користувача, обробляється ними або доступна через них, має бути захищена.
…	…	…
8.3	Обмеження доступу до інформації	**Заходи безпеки** Доступ до інформації та інших пов’язаних активів має бути обмежено відповідно до встановленої тематичної політики контролю доступу.
8.4	Доступ до вихідного коду	**Заходи безпеки** Необхідно відповідним чином керувати доступом для зчитування та запису вихідного коду, засобів розробки та бібліотек програмного забезпечення.
…	…	…

ДОДАТОК В

Таблиця В.1 - Матриця контролів та значень атрибутів (витяг з таблиці А.1 ISO/IEC 27002:2022)

Ідентифікатор контролю ISO/IEC 27002	**Назва контролю**	**Тип контролю**	**Властивості інформаційної безпеки**	**Концепції кібербезпеки**	**Операційні можливості**	**Домени безпеки**
5.1	Політики інформаційної безпеки	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Ідентифікувати	#Керівництво	# Керівництво_та_Екосистема, #Стійкість
5.2	Ролі інформаційної безпеки та відповідальність	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Ідентифікувати	#Керівництво	# Керівництво_та_Екосистема, #Стійкість
…	…	…	…	…	…	…
5.4	Відповідальність керівництва	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Ідентифікація	#Керівництво	# Керівництво_та_Екосистема
…	…	…	…	…	…	…
5.19	Інформаційна безпека у відносинах з постачальниками	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Ідентифікувати	# Безпека_ взаємовідносин_із_ постачальниками	# Керівництво_та_Екосистема, #Захист
…	…					
5.21	Управління інформаційною безпекою в ланцюзі поставок ІКТ	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Ідентифікувати	# Безпека_ взаємовідносин_із_постачальниками	# Керівництво_та_Екосистема, #Захист
…	…	…	…	…	…	…
6.1	Відбір	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Безпека_ людських_ресурсів	# Керівництво_та_Екосистема
6.2	Умови прийому на роботу	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Безпека_ людських_ресурсів	# Керівництво_та_Екосистема
6.3	Інформаційна безпека, освіта та навчання	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Безпека_ людських_ресурсів	# Керівництво_та_Екосистема
…	…	…	…	…	…	…
7.1	Периметри фізичної безпеки	#Попереджувальний	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Фізична_ безпека	#Захист

Продовження таблиці В.1

7.2	Фізичний доступ	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Фізична_ безпека, # Ідентифікація_та_ управління_доступом	#Захист
7.3	Охорона офісів, приміщень та приміщень	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	# Фізична_ безпека, #Управління_ активами	#Захист
…	…	…	…	…	…	…
8.1	Кінцеві пристрої користувачів	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	#Управління_ активами, #Захист_інфор-мації	#Захист
…	…	…	…	…	…	…
8.3	Обмеження доступу до інформації	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	#Ідентифікація_та_ управління_доступом	#Захист
8.4	Доступ до вихідного коду	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	#Ідентифікація_та_ управління_доступом, #Безпека_додатків, # Безпечне_налаштування	#Захист
8.5	Безпечна автентифікація	#Попереджу-ючий	#Конфіденційність, #Цілісність, #Доступність	#Захищати	#Ідентифікація_та_ управління_доступом	#Захист
…	…	…	…	…	…	…