Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи магістра

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Гібридний метод управління ризиками»

Виконавець: студентка ІІ курсу, групи КБм-21

_____ **Ольга АНДРЕЙЧУК**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Володимир НАКОНЕЧНИЙ		
Нормоконтроль	Олена БОГУСЛАВСЬКА		

Київ 2023

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о завідувач кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці КБм-21 (група) Андрейчук Ользі Валентинівні (прізвище ім'я по-батькові)

Тема дипломної роботи Гібридний метод управління ризиками

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес управління ризиками в інформаційній безпеці.
Предмет досліджень	Поєднання методів оцінювання ризиків в рамках процесу забезпечення інформаційної безпеки для вдосконалення методу управління ризиками.
Мета	Розробка гібридного методу управління ризиками.
Вихідні дані для проведення роботи	Методи оцінки ризиків, корпоративний ризик-менеджмент; етапи управління ризиками.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	Представлення вдосконаленого процесу управління ризиками за рахунок розроблення гібридного методу, який базується на перевагах відомих методів оцінки ризиків та поєднує їх для ефективної обробки та отримання чітких результатів.
Практична цінність	Розробка гібридного методу управління ризиками та оцінка його ефективності задля покращення процесів зменшення та пом'якшення ризиків та їх наслідків.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Розробка плану для досягнення мети роботи	24.10.2022 – 23.01.2023
Аналіз літературних джерел	24.01.2023 – 14.02.2023
Розробка гібридного методу управління ризиками та оцінка його ефективності	15.02.2023 – 24.04.2023
Оформлення і друк пояснювальної записки	25.04.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	Зменшення ризиків та пом'якшення наслідків.
Соціальний ефект	Підвищення ефективності процесу управління ризиками для організацій різного розміру та типу власності.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Володимир НАКОНЕЧНИЙ _____

(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Ольга АНДРІЙЧУК

(підпис) (прізвище, ініціали)

Дата видачі завдання: 24.10.2022 р.

Термін подання дипломної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Гібридний метод управління ризиками»: 103 сторінок основного тексту, 4 рисунки, 3 таблиці, 2 додатків та 90 літературних джерел.

Об’єкт дослідження – процес управління ризиками в інформаційній безпеці.

Мета роботи – розробка гібридного методу управління ризиками..

Методи дослідження – методи наукової абстракції, індукція, дедукція, аналіз наявних рішень, історико-логічний метод та експертна оцінка.

У дипломній роботі досліджено процес управління ризиками, проведений аналіз доступних джерел у сфері інформаційної безпеки для збору інформації та формування класифікації ризиків. Досліджено взаємозв’язок інформаційної безпеки та бізнесу, порівняно інформаційні ризики та бізнес-ризики. Проведено аналіз методів оцінки ризиків для подальшої побудови ефективного алгоритму. Запропоновано гібридний метод управління ризиками за рахунок комбінації методів оцінки ризиків на основі переваг та недоліків кожного із них та проведена якісна оцінка ефективності представленого методу управління ризиками. Описані основні засади запропонованого алгоритму та наведені його переваги і недоліки.

Наукова новизна: представлення вдосконаленого процесу управління ризиками за рахунок розроблення гібридного методу, який базується на перевагах відомих методів оцінки ризиків та поєднує їх для ефективної обробки та отримання чітких результатів. Запропонований метод відрізняється від існуючих тим, що в якості основних алгоритмів оцінки виступають методики CRAMM та Монте-Карло, а інші етапи регулюються згідно з найкращими галузевими практиками в сфері управління ризиками. .

Актуальність теми: процес управління ризиками є нелегким та адаптується під потреби кожної організації, а також містить декілька основних етапів: ідентифікацію інформаційних активів, оцінку ризиків, прийняття рішень на основі оцінки ризиків та

постійного моніторингу, аналіз для забезпечення неперервності як і захисту організації, так і бізнесу. Традиційні методи оцінки ризиків не завжди можуть надати повне уявлення про ризики організації, а постійний мінливий ландшафт кіберзагроз змінюється та поповнюється. Поєднання різних методів оцінки ризиків, таких як кількісні та якісні, може забезпечити більш повне та точне розуміння ризиків організації. Організації можуть краще розуміти ризики, визначати пріоритети стратегій пом'якшення та ефективно розподіляти ресурси.

Ключові слова: інформаційна безпека, управління ризиками, інформаційні ризики, методи оцінки ризиків, корпоративний ризик-менеджмент, .

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ	—	Інформаційна безпека
ІС	—	Інформаційні системи
ОТ	—	Операційні технології
ICS	—	Індустріальні системи управління
SCADA	—	Система диспетчерського контролю, збору даних
ІВ	—	Інтелектуальна власність
ШІ	—	Штучний інтелект
IoT	—	Інтернет речей
GDPR	—	Загальний регламент про захист даних
СУІБ	—	Система управління інформаційною безпекою
CSF	—	Cybersecurity Framework
ITIL	—	Бібліотека інфраструктури інформаційних технологій
PCI DSS	—	Стандарт безпеки даних індустрії платіжних карток
DevOps	—	Development & Operations
FINRA	—	Управління з регулювання фінансової індустрії
CIS	—	Центр інтернет-безпеки
РНБО	—	Рада національної безпеки та оборони України
НБУ	—	Національний банк України
ДЦКБУ	—	Державний центр кібербезпеки України
ROI	—	Рентабельність інвестицій
COGS	—	Собівартість реалізованої продукції
ROSI	—	Рентабельність інвестицій в безпеку
RMF	—	Система управління ризиками
SCRM	—	Управління ризиками ланцюга постачання
FMEA	—	Метод виявлення та оцінки потенційних ризиків
CSA	—	Самооцінка контролю
CRSA	—	Самооцінка контрольних ризиків

HAZOP	—	Метод для виявлення та оцінки потенційних ризиків та вразливостей, пов'язаних з процесом або системою
FTA	—	Аналіз дерева несправностей
ALE	—	Очікуваний річний збиток
SLE	—	Величина одноразового збитку
ARO	—	Очікувана частота інцидентів, що відбуваються протягом року
QRA	—	Кількісний аналіз ризику
BIA	—	Аналіз впливу на бізнес
QCRA	—	Кількісна оцінка кіберризиків
FAIR	—	Факторний аналіз інформаційних ризиків
CRAMM	—	CCTA Risk Analysis and Management Method
COBRA	—	Consultative, Objective and Bi-functional Risk Analysis
OCTAVE	—	Operationally Critical Threat, Asset and Vulnerability Evaluation

ЗМІСТ

ВСТУП

Актуальність. Процес управління ризиками є нелегким та адаптується під потреби кожної організації, а також містить декілька основних етапів: ідентифікацію інформаційних активів, оцінку ризиків, прийняття рішень на основі оцінки ризиків та постійного моніторингу, аналіз для забезпечення неперервності як і захисту організації, так і бізнесу. Традиційні методи оцінки ризиків не завжди можуть надати повне уявлення про ризики організації, а постійний мінливий ландшафт кіберзагроз змінюється та поповнюється.

Багато українських дослідників, як наприклад, Юдін О. К., Корченко О. Г., Горбенко І., Домарєв В. В, Бучик С. С., Чунарьова А. В. у своїх роботах розкривають проблеми дослідження інформаційної безпеки та деякі з них представляють свої удосконалені методи оцінки інформаційних ризиків [1]. Також цю тему досліджували іноземні вчені: McCumber, J., Thomas R., Wheeler, E., Whitman M. [2 - 8]

Поєднання різних методів оцінки ризиків, таких як кількісні та якісні, може забезпечити більш повне та точне розуміння ризиків організації. Кількісні методи оцінки ризиків передбачають присвоєння їм числових значень, таких як ймовірність виникнення та потенційний вплив, тоді як якісні методи передбачають більш суб'єктивну оцінку ризиків, засновану на експертних судженнях та досвіді фахівців.

Організації можуть краще розуміти ризики, визначати пріоритети стратегій пом'якшення та ефективно розподіляти ресурси.

Крім того, удосконалені методи управління ризиками можуть допомогти організаціям випереджати нові загрози, покращити загальний стан безпеки та захистити свої інформаційні активи.

Більш комплексний підхід до процесу управління ризиками та перегляд методик їх оцінки ризиків може забезпечити кілька переваг для організацій [9]:

1. Більш глибоке розуміння ризиків: комплексний підхід до управління ризиками може допомогти організаціям краще зрозуміти свої ризики як з точки зору ймовірності їх виникнення, так і з точки зору потенційного впливу.

2. Налагоджений процес визначення пріоритетності ризиків: поєднуючи різні методології оцінки ризиків, організації можуть більш ефективно визначати пріоритетність ризиків та відповідно до цього розподіляти ресурси.

3. Більш цілеспрямовані стратегії зменшення ризиків: професійний аналіз ризиків та їхнього впливу на життєдіяльність організації може допомогти розробити вдалі стратегії зменшення ризиків, їх наслідків, покращуючи загальний стан безпеки.

4. Удосконалення процесу комунікації: комплексний підхід до управління ризиками може сприяти комунікації між різними зацікавленими сторонами в організації, включаючи керівництво, IT-персонал та персонал служби безпеки.

5. Більша стійкість: комплексний підхід до управління ризиками може допомогти організаціям стати більш стійкими до нових загроз, забезпечуючи більш точне та сучасне розуміння ризиків і вразливостей.

Таким чином, актуальним науковим завданням, що має теоретичне та практичне значення, є удосконалення процесу забезпечення інформаційної безпеки за рахунок комбінації методів її оцінки.

Метою дипломної роботи є розробка гібридного методу управління ризиками.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

- провести аналіз доступних джерел у сфері інформаційної безпеки;
- зібрати інформацію про процес управління ризиками;
- формалізувати класифікацію ризиків та етапи забезпечення інформаційної безпеки в організаціях;
- дослідити взаємозв’язок інформаційної безпеки та бізнесу;
- порівняти інформаційні ризики та бізнес-ризики;
- провести аналіз методів оцінки ризиків для подальшої їх класифікації;
- розробити гібридний метод управління ризиками за рахунок комбінації існуючих методів оцінки ризиків;
- провести якісну оцінку ефективності представленого методу управління ризиками.

Об’єкт дослідження – процес управління ризиками в інформаційній безпеці.

Предмет дослідження – поєднання методів оцінювання ризиків в рамках процесу забезпечення інформаційної безпеки для вдосконалення методу управління ризиками.

Для вирішення поставлених завдань у дипломній роботі використані такі методи дослідження:

- методи наукової абстракції;
- індукція;
- дедукція;
- аналіз;
- історико-логічний метод;
- експертна оцінка.

Наукова новизна одержаних результатів полягає у представленні вдосконаленого процесу управління ризиками за рахунок розроблення гібридного методу, який базується на перевагах відомих методів оцінки ризиків та поєднує їх для ефективної обробки та отримання чітких результатів. Запропонований метод відрізняється від існуючих тим, що в якості основних алгоритмів оцінки виступають методики CRAMM та Монте-Карло, а інші етапи регулюються згідно з найкращими галузевими практиками в сфері управління ризиками.

Практичною цінністю роботи є розробка гібридного методу управління ризиками та оцінка його ефективності задля покращення процесів зменшення та пом’якшення ризиків та їх наслідків.

Основні наукові положення і результати роботи доповідалися та обговорювалися на V та VI Міжнародних науково-практичних конференціях “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” (Київ, 2022 та 2023).

РОЗДІЛ 1
УПРАВЛІННЯ РИЗИКАМИ В ІБ ТА ВЗАЄМОЗВ'ЯЗОК З БІЗНЕСОМ

Управління ризиками в інформаційній безпеці передбачає виявлення, оцінку та визначення пріоритетів потенційних ризиків та вразливостей, які можуть загрожувати конфіденційності, цілісності та доступності чутливої інформації організації. Це безперервний процес, який допомагає організаціям ефективно управляти цими ризиками та захищати свої інформаційні активи від несанкціонованого доступу, крадіжки, втрати або пошкодження.

Взаємозв'язок між управлінням ризиками в інформаційній безпеці (ІБ) та бізнесом має вирішальне значення, оскільки ризики ІБ можуть мати значний вплив на діяльність, репутацію та фінансовий стан організації. Ефективне управління ризиками дозволяє організаціям захистити свої критичні активи та зменшити потенційні збитки, гарантуючи безперебійну роботу.

Компанії повинні розуміти потенційні ризики та загрози, які існують в їхніх інформаційних системах, і вживати проактивні заходи для управління цими ризиками та їхнього зменшення. Це передбачає створення плану управління ризиками, в якому визначаються потенційні власне ризики та вразливості, їх пріоритетність, а також розробляються стратегії для їх усунення.

План управління ризиками має бути інтегрований у загальну бізнес-стратегію та враховувати унікальні ризики та виклики, характерні для організації. Він також повинен включати політику, процедури реагування на інциденти безпеки, а також навчальні програми для співробітників, щоб вони розуміли свою роль і обов'язки в підтримці належного функціонування ІБ.

Таким чином, управління ризиками в інформаційній безпеці має вирішальне значення для бізнесу, адже захищає конфіденційну інформацію, тобто важливий ресурс компанії, від потенційних загроз та вразливостей.

Ефективне управління ризиками вимагає спільних зусиль між командою з інформаційної безпеки та бізнесом, з акцентом на інтеграцію стратегій управління ризиками в загальну бізнес-стратегію.

За допомогою ефективного управління ризиками інформаційної безпеки підприємства можуть захистити свою конфіденційну інформацію та забезпечити свій подальший успіх. Це включає в себе захист інтелектуальної власності, збереження конфіденційності даних клієнтів і захист репутації від потенційних інцидентів безпеки.

1.1 Управління ризиками в ІБ

Як вже зазначалось раніше, управління ризиками в інформаційній безпеці – це процес виявлення, оцінки та зменшення ризиків, вразливостей, які можуть вплинути на конфіденційну інформацію організації. Це важливий компонент загальної стратегії безпеки будь-якої організації, який передбачає систематичний підхід до виявлення та усунення потенційних загроз.

Нижче наведено ключові етапи управління ризиками в інформаційній безпеці [9]:

a) ідентифікація інформаційних активів: Першим кроком є ідентифікація інформаційних активів організації, включаючи всі типи конфіденційних даних, таких як дані клієнтів, фінансова інформація, інтелектуальна власність та інша конфіденційна інформація;

b) оцінка ризиків: наступним кроком є оцінка ризику, пов'язаного з кожним інформаційним активом. Даний пункт передбачає виявлення потенційних загроз, таких як кібератаки, інсайдерські загрози, фізична крадіжка, а також оцінку ймовірності та потенційного впливу кожного ризику;

c) визначення толерантності до ризику: організація повинна визначити свою толерантність до ризику, тобто рівень ризику, який вона готова прийняти для досягнення своїх бізнес-цілей. Це передбачає зважування потенційної вигоди від прийняття ризику проти потенційних витрат та наслідків інциденту безпеки;

d) впровадження засобів контролю: будь-яке підприємство повинно впровадити засоби контролю безпеки, щоб зменшити ризики, пов'язані з кожним інформаційним активом. Сюди входять технічні засоби контролю, такі як

брандмауери, шифрування, контроль доступу, а також адміністративні засоби, такі як політики безпеки, навчання працівників та процедури реагування на інциденти;

е) моніторинг та аналіз: організація має контролювати стан своєї інформаційної безпеки та регулярно переглядати свою стратегію управління ризиками. Це включає моніторинг нових загроз, вразливостей, оцінку ефективності існуючих засобів контролю та оновлення стратегії управління ризиками за необхідності.

На додаток до кроків, описаних вище, є ще кілька ключових міркувань щодо ефективного управління ризиками в інформаційній безпеці. До них відносяться [9]:

1. Відповідність: багато галузей підпадають під дію регуляторних «правил», які вимагають певних рівнів інформаційної безпеки. Організації повинні забезпечити відповідність своїх стратегій управління ризиками цим вимогам, щоб уникнути юридичних та фінансових санкцій.

2. Ризик третьої сторони: організації повинні враховувати ризики, пов'язані зі сторонніми постачальниками та партнерами, які можуть мати доступ до інформаційних систем. Це включає в себе проведення належної перевірки сторонніх постачальників, забезпечення того, щоб вони відповідали стандартам безпеки організації, а також моніторинг їхнього стану безпеки.

3. Реагування на інциденти: незважаючи на всі зусилля, інциденти безпеки все ще можуть траплятися. Організації повинні мати чітко розроблений план реагування на інциденти, який визначає процедури локалізації та пом'якшення наслідків інциденту, а також комунікації із зацікавленими сторонами, в тому числі клієнтами та регуляторними органами.

4. Передача ризиків: підприємства можуть передати ризик, пов'язаний з інформаційною безпекою, за допомогою страхових полісів, що може допомогти пом'якшити фінансові наслідки інциденту безпеки.

5. Культура безпеки: нарешті, ефективне управління ризиками в інформаційній безпеці вимагає культури обізнаності про безпеку в усій організації. Це включає в себе регулярне навчання співробітників з питань безпеки, фокус на

безпеці в цінностях і цілях організації, а також прихильність до постійного вдосконалення та адаптації до нових загроз і ризиків.

Отже, на думку автора цієї роботи, управління ризиками в інформаційній безпеці є критично важливим компонентом загальної стратегії безпеки будь-якої організації. Воно передбачає системний підхід до виявлення, оцінки та зменшення ризиків для конфіденційної інформації, а також постійний моніторинг та аналіз з метою адаптації до нових загроз та вразливостей.

1.1.1 Класифікація ризиків

У контексті інформаційної безпеки ризик – це ймовірність порушення безпеки або втрати даних, що може призвести до шкоди репутації організації, фінансових втрат або юридичної відповідальності. Це міра потенційної шкоди або впливу, який інцидент безпеки може мати на організацію.

Ризики у сфері безпеки можуть виникати з різних джерел, що є причиною для їх класифікації.

Існує кілька типів ризиків, які можуть загрожувати безпеці інформаційних систем (ІС) [9]. Ось деякі з найпоширеніших типів ризиків в ІС (додаток А):

1. Кібер-ризики: це ризики, пов'язані зі зловмисними атаками хакерів, шкідливим програмним забезпеченням, вірусами або іншими формами кіберзагроз, які можуть порушити конфіденційність, цілісність або доступність інформаційних систем.

2. Фізичні ризики: фізичні загрози, такі як крадіжки, стихійні лиха, пожежі, повені та інші події, які можуть пошкодити або знищити обладнання, програмне забезпечення або дані.

3. Ризики, пов’язані з людським фактором: це ризики, що стосуються людських помилок, недбалості або навмисних дій, які можуть поставити під загрозу безпеку інформаційних систем, наприклад, випадкові витоки даних, атаки соціальної інженерії або інсайдерські загрози.

4. Комплаєнс-ризики: пов'язані з недотриманням правових, регуляторних або галузевих стандартів, які можуть призвести до юридичних або фінансових санкцій, репутаційних збитків або втрати бізнесу.

5. Технологічні ризики: технологічні збої або несправності, які можуть спричинити перебої або збої в роботі інформаційних систем (ІС), наприклад, збої в роботі апаратного чи програмного забезпечення, системні збої або перебої в роботі мережі.

6. Екологічні ризики: тобто фактори навколишнього середовища, такі як перебої в електропостачанні, екстремальні погодні умови або інші типи подій, які можуть вплинути на доступність та цілісність інформаційних систем.

7. Ризики ланцюга постачання: пов'язані з постачальниками та продавцями, які надають товари та послуги організації; можуть включати вразливість апаратних чи програмних компонентів, витік даних третіми сторонами або інші типи ризиків, які можуть вплинути на безпеку ІС організації.

8. Репутаційні ризики: шкода для репутації організації через порушення безпеки або інші типи інцидентів, які можуть підірвати довіру зацікавлених сторін, клієнтів та партнерів.

9. Фінансові ризики: фінансовий вплив інциденту безпеки або інших видів порушень діяльності організації, таких як втрата доходів, перерва в роботі або витрати, пов'язані з реагуванням на інцидент безпеки.

10. Юридичні ризики: юридична відповідальність, судові процеси або примусові заходи, які можуть виникнути внаслідок інциденту безпеки або недотримання законодавчих чи нормативних вимог.

11. Операційні ризики: повсякденна діяльність організації, такі як недостатня кількість персоналу, недостатній рівень підготовки або неадекватні процеси, процедури, які можуть призвести до інцидентів безпеки або інших видів порушень.

12. Стратегічні ризики: пов'язані зі стратегічними цілями та завданнями організації, наприклад, невжиття належних заходів безпеки або неефективне управління ризиками, які можуть вплинути на довгостроковий успіх організації.

13. Ризики операційних технологій (OT): пов'язані із промисловими системами управління (ICS), системами диспетчерського контролю, збору даних (SCADA) та іншими типами систем OT, які керують критично важливою інфраструктурою та операціями. Ризики OT можуть включати вразливості в апаратних або програмних компонентах, людські помилки або навмисні атаки, які можуть порушити або пошкодити промислові операції.

14. Соціальні ризики: стосуються соціальних медіа, онлайн-спільнот або інших типів соціальних мереж, які можуть завдати шкоди репутації організації фішинговими атаками або іншими типами атак соціальної інженерії, які можуть поставити під загрозу безпеку інформаційних систем.

15. Ризики конфіденційності даних: під цю категорію підпадає захист конфіденційних даних, таких як інформація, що дозволяє ідентифікувати особу, дані про стан здоров'я або фінансова інформація. Ризики конфіденційності даних можуть охоплювати також витік або крадіжку персональних даних, несанкціонований доступ до конфіденційної інформації.

16. Ризики інтелектуальної власності: наприклад, йде мова про захист патентів, торгових марок або комерційної таємниці. Ризики інтелектуальної власності (IB) можуть включати крадіжку, порушення або інші види несанкціонованого використання інтелектуальної власності, які можуть вплинути на конкурентну перевагу або фінансовий успіх організації.

17. Геополітичні ризики: це ризики, що пов'язані з політичними, економічними або соціальними умовами в країнах або регіонах, де працює організація. Геополітичні ризики можуть включати кібершпигунство, економічні санкції або інші види геополітичних подій, які можуть вплинути на безпеку інформаційних систем.

18. Ризики нових технологій: нові технології, такі як штучний інтелект (ШІ), блокчейн або Інтернет речей (IoT). Ризики нових технологій можуть включати вразливості в нових технологіях або нові типи кіберзагроз, які використовують ці технології.

Отже, ризики інформаційної безпеки можна класифікувати за різними категоріями залежно від їхньої природи, впливу та джерела. Класифікуючи ризики за категоріями, організації можуть отримати більш повне розуміння ризиків, з якими вони стикаються, та розробити ефективні стратегії управління ризиками для захисту своїх інформаційних активів. Класифікація ризиків ІБ також може допомогти організаціям визначити пріоритети в управлінні ризиками та розподілити ресурси на найбільш важливі сфери.

Хоча розглянуті вище категорії ризиків ІС не є вичерпними, вони надають організаціям основу для виявлення та оцінки ризиків, а також для розробки стратегій управління ризиками, адаптованих до їхніх конкретних потреб.

Розуміючи різні типи ризиків ІС та їх потенційний вплив на організацію, організації можуть приймати обґрунтовані рішення щодо рівня ризику, який вони готові прийняти, та впроваджувати відповідні засоби контролю для зменшення цих ризиків.

1.1.2 Процес управління ризиками

Процес управління ризиками в інформаційній безпеці з'явився як відповідь на зростаючу залежність організацій від інформаційних технологій та зростання кількості загроз виникнення кібератак. На початку розвитку комп'ютерних технологій ризики безпеки були відносно незначними, і ними можна було керувати за допомогою базових заходів, таких як фізична безпека та контроль доступу. Однак з розвитком технологій, зростанням залежності від цифрових даних та систем ландшафт ризиків значно ускладнився.

У 1990-х роках низка гучних кібератак вивела питання інформаційної безпеки в центр уваги громадськості, а організації масово почали усвідомлювати важливість управління ризиками інформаційної безпеки та намагатися побудувати більш структурований і систематичний спосіб. Це призвело до розробки різних систем та стандартів управління ризиками, таких як стандарт ISO/IEC 27001, який забезпечує всеосяжну основу для управління ризиками інформаційної безпеки [9].

Сьогодні процес управління ризиками інформаційної безпеки є невід'ємною частиною загальної стратегії управління ризиками будь-якої організації. Він включає в себе виявлення та оцінку ризиків, розробку стратегій для зменшення цих ризиків, а також впровадження та моніторинг цих стратегій з плином часу. Цей процес постійно розвивається, оскільки з'являються нові загрози, а організації прагнуть бути на крок попереду в управлінні ризиками інформаційної безпеки.

Поява управління ризиками в ІС також була зумовлена зростаючою взаємозалежністю організацій та збільшенням обсягів даних, які генеруються і передаються через різні мережі та системи. Це призвело до появи потреби в координації та співпраці між різними зацікавленими сторонами, в тому числі ІТ-відділами, менеджерами з управління ризиками та вищим керівництвом.

Іншим ключовим фактором, який стимулював розвиток управління ризиками в ІС, є регуляторне середовище. Багато країн і галузей запровадили нормативні акти та стандарти, які вимагають від організацій більш систематичного підходу управління ризиками.

Наприклад, загальний регламент ЄС про захист даних (GDPR) вимагає від організацій впроваджувати відповідні технічні та організаційні заходи для захисту персональних даних від несанкціонованого доступу, втрати або крадіжки [10].

Існує кілька викликів, з якими організації можуть зіткнутися при впровадженні ефективного процесу управління ризиками в інформаційній безпеці. Ось деякі з найпоширеніших проблем [11]:

f) недостатня обізнаність: багато організацій мають обмежену обізнаність про ризики, з якими вони стикаються, і можуть не повністю розуміти важливість управління ними. Це може призвести до браку ресурсів та інвестицій в ініціативи з управління ризиками;

g) обмеженість ресурсів: підприємства можуть мати обмежені ресурси, такі як час, гроші та персонал, які потрібно виділити на діяльність з управління ризиками. Це може ускладнити проведення ретельної оцінки ризиків та впровадження ефективних стратегій їхнього зменшення;

h) зміна ландшафту загроз: ландшафт загроз в інформаційній безпеці постійно розвивається, і регулярно з'являються нові загрози. Компаніям необхідно бути в курсі останніх загроз, вразливостей та відповідно коригувати свої стратегії управління ризиками;

i) опір змінам: впровадження процесу управління ризиками може вимагати змін в організаційній культурі та процесах, що може спровокувати незадоволення з боку працівників, яких влаштовує поточний статус ;

j) відсутність стандартизації: не існує універсального підходу до управління ризиками в інформаційній безпеці, що може стати проблемою для організацій в процесі пошуку стандартизованої системи, яка б відповідала їхнім конкретним потребам, вимогам;

k) складне регуляторне середовище: багато організацій підпадають під дію різних нормативно-правових актів та вимог щодо відповідності, пов'язаних з інформаційною безпекою, що може зробити управління ризиками більш складним для його ефективного впровадження;

l) брак кваліфікованого персоналу: впровадження ефективного процесу управління ризиками вимагає кваліфікований персонал з необхідними знаннями в галузі інформаційної безпеки та управління ризиками. Однак багатьом організаціям важко залучати та утримувати професіоналів через брак таких спеціалістів на ринку;

m) обмежена співпраця: управління ризиками в інформаційній безпеці часто вимагає співпраці між різними відділами та зацікавленими сторонами в організації. Розрізненість та обмеженість комунікації разом з співпрацею можуть перешкоджати ефективному управлінню ризиками.

n) відсутність інтеграції: підприємства можуть мати кілька процесів та інструментів управління ризиками, що є неінтегрованими, це призводить до дублювання зусиль та прогалин у покритті.

o) неповні оцінки ризиків: оцінка ризиків може бути неповною або неадекватною, що призводить до нездатності виявити всі потенційні ризики та вразливості. Це може зробити організації вразливими до кібератак та інших інцидентів, пов'язаних з безпекою.

р) недостатній моніторинг: управління ризиками – це безперервний процес, що потребує постійний моніторинг систем та процесів для виявлення нових ризиків й забезпечення ефективності стратегій їх зниження. Однак багато компаній можуть не мати достатніх можливостей для моніторингу або ресурсів для цього.

Щоб вирішити ці проблеми, організаціям слід визначити управління ризиками як найважливіший компонент загальної стратегії ІБ. Це вимагає інвестицій в ресурси, інструменти та персонал для підтримки зусиль з управління ризиками, а також культури співпраці та постійного вдосконалення. Крім того, організації повинні регулярно переглядати і оновлювати свої процеси та стратегії управління ризиками, щоб забезпечити їхню ефективність й актуальність в умовах еволюції загроз та ризиків.

1.1.3 Міжнародні стандарти, що регулюють управління ризиками

Згідно з підрозділом 1.1.2, неможливо заперечити важливість впровадження системи управління ризиками, яка відповідає міжнародним стандартам та передовим практикам, таким як ISO 27001, NIST Cybersecurity Framework або COBIT.

Міжнародні стандарти надають організаціям основу та керівні принципи для впровадження ефективного управління ризиками в інформаційній безпеці. Ці стандарти та настанови були розроблені такими організаціями, як ISO, NIST та ISACA, і є широко визнаними та прийнятими у всьому світі.

Одним з найбільш визнаних міжнародних стандартів управління інформаційною безпекою є ISO 27001. Цей стандарт забезпечує комплексну основу для управління ризиками інформаційної безпеки та включає набір засобів контролю, які допомагають організаціям протидіяти конкретним загрозам та вразливостям безпеки [9]. ISO 27001 також вимагає від підприємств регулярно проводити оцінку та аналіз ризиків, щоб гарантувати, що їхня система управління інформаційною безпекою залишається ефективною.

ISO 27001 є основою для впровадження системи управління інформаційною безпекою (СУІБ). Стандарт описує системний підхід до управління конфіденційною інформацією компанії, включаючи людей, процеси та IT-системи.

Також цей документ визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення СУІБ. Він забезпечує структуру управління ризиками для інформаційної безпеки, яка дозволяє організаціям виявляти, аналізувати та усувати ризики інформаційної безпеки в систематичний та економічно ефективний спосіб.

Стандарт застосовується до всіх типів організацій, включаючи підприємства, некомерційні організації та державні установи. Він розроблений таким чином, щоб бути гнучким і адаптованим до різних галузей та бізнес-моделей.

ISO 27001 є частиною серії ISO/IEC 27000, яка включає в себе інші суміжні стандарти, такі як ISO 27002 (звід практичних правил контролю інформаційної безпеки) та ISO 27005 (управління ризиками для інформаційної безпеки).

Стандарт ISO 27005 надає настанови щодо проведення оцінки ризиків інформаційної безпеки. Він забезпечує основу для виявлення, оцінювання та управління ризиками інформаційної безпеки в систематичний та послідовний спосіб. Стандарт покликаний допомогти організаціям розробити та впровадити процес управління ризиками, який відповідає їхнім бізнес-цілям та підтримує загальну стратегію інформаційної безпеки [12].

Крім того, стандарт ISO 27005 призначений для використання разом зі стандартом ISO 27001, який забезпечує більш комплексну основу для управління інформаційною безпекою. У той час як ISO 27001 містить настанови щодо загального управління інформаційною безпекою, ISO 27005 зосереджується безпосередньо на процесі оцінювання ризиків.

Стандарт описує шість етапів процесу проведення оцінки ризиків, який включає в себе:

1. Встановлення контексту: передбачає визначення обсягу оцінки ризиків, ідентифікацію активів, що підлягають захисту, та встановлення критеріїв оцінки ризиків.

2. Методологія оцінки ризиків: крок передбачає вибір методології оцінки ризиків, яка відповідає потребам організації.

3. Ідентифікація ризиків: визначення потенційних загроз, вразливостей та впливів на інформаційні активи організації.

4. Аналіз ризиків: оцінка ймовірності та потенційного впливу кожного виявленого ризику.

5. Власне оцінювання ризиків: визначення рівня ризику, пов'язаного з кожним виявленим ризиком, пріоритетності на основі їх значущості.

6. Управління ризиками: вибір та впровадження засобів контролю для пом'якшення або зменшення виявлених ризиків.

NIST Cybersecurity Framework (CSF) – ще один широко визнаний стандарт управління ризиками інформаційної безпеки [13]. Ця система містить набір керівних принципів та найкращих практик для організацій з управління ризиками кібербезпеки, і вона часто використовується організаціями приватного сектору [14].

CSF складається з трьох основних компонентів: ядра, рівнів реалізації та профілів. Ядро містить набір заходів з результатами у сфері кібербезпеки, згрупованих за п'ятьма функціями: ідентифікація, захист, виявлення, реагування та відновлення. Кожна функція поділяється на категорії та підкатегорії, які містять більш конкретні вказівки щодо того, як досягти бажаних результатів [13].

Рівні впровадження надають організаціям можливість оцінити та повідомити про рівень зрілості управління ризиками кібербезпеки. Існує чотири рівні: частковий, ризик-орієнтований, повторюваний та адаптивний.

Компонент "Профілі" дозволяє організаціям створювати індивідуальний набір вимог до кібербезпеки на основі їхніх конкретних потреб, толерантності до ризиків та бізнес-цілей.

CSF стала широко визнаною основою для управління кібер-ризиками, і її часто використовують як посилання або базу для інших структур, нормативних актів. Гнучкий та адаптивний характер стандарту дозволяє організаціям адаптувати свої програми з кібербезпеки до унікальних потреб, дотримуючись при цьому найкращих галузевих практик.

COBIT – це фреймворк, розроблений ISACA, який надає керівні принципи для управління IT, включаючи управління ризиками. Цей фреймворк включає набір найкращих практик для управління IT-ризиками та використовується організаціями для забезпечення відповідності IT-систем, процесів їхнім бізнес-цілям. Тобто для побудови здорової взаємозалежності між бізнесом та ІБ є важливим впровадження цього документу в життєдіяльність будь-якої організації [15].

COBIT складається з п'яти основних компонентів:

I. Структура: надає огляд структури COBIT, її компонентів і того, як вони поєднуються між собою.

II. Процеси: описує різні процеси, пов'язані з IT, які необхідно впровадити для досягнення ефективного управління IT.

III. Цілі контролю: Визначає цілі контролю, яких необхідно досягти для забезпечення ефективного управління IT ризиками.

IV. Керівні принципи управління: надає вказівки щодо того, як управляти IT ризиками та забезпечувати відповідність різним стандартам і нормам.

V. Моделі зрілості: моделі зрілості для кожного з процесів COBIT, що дозволяє організаціям оцінити свій поточний рівень зрілості та визначити сфери для вдосконалення.

COBIT має бути гнучким і адаптованим до різних організацій та галузей, а також сумісним з іншими стандартами і фреймворками, такими як ISO 27001 та бібліотека інфраструктури інформаційних технологій (ITIL). Зосередженість на управлінні ризиками робить його корисним інструментом для організацій, які прагнуть керувати своїми IT-системами та активами у спосіб, що відповідає їхнім загальним бізнес-цілям.

Також важливо згадати стандарт безпеки даних індустрії платіжних карток (PCI DSS) та бібліотеку інфраструктури інформаційних технологій для управління IT-послугами.

Стандарт безпеки даних індустрії платіжних карток – це набір стандартів безпеки, покликаних гарантувати, що всі компанії, які приймають, обробляють, зберігають або передають інформацію про кредитні картки, підтримують безпечне

середовище. Стандарт був розроблений Радою зі стандартів безпеки індустрії платіжних карток (PCI SSC), яка є глобальним форумом, створеним найбільшими компаніями-виробниками кредитних карток, такими як Visa, Mastercard, American Express і Discover [16].

PCI-DSS складається з 12 вимог, які об'єднані в шість категорій, як показано нижче [16]:

1. Побудова та підтримка безпечної мережі та систем.

a) встановити та підтримувати конфігурації брандмауера для захисту даних власників карток;

b) не використовувати системні паролі та інші параметри безпеки, надані постачальником за замовчуванням.

2. Захист даних власників карток.

а) захист збережених даних власників;

б) шифрування даних про власників через відкриті загальнодоступні мережі.

3. Підтримка програм управління вразливостями.

а) захист систем від шкідливого програмного забезпечення та регулярні оновлення антивірусного ПЗ.

б) розробка та підтримка безпечних систем та додатків.

3. Впровадження суворих заходів контролю доступу.

а) обмеження доступу до даних кардхолдерів за принципом службової необхідності;

б) ідентифікація та автентифікація доступу до компонентів системи.

4. Регулярний контроль та тестування мережі.

а) відстеження та контроль всього доступу до мережевих ресурсів та даних;

б) регулярне тестування систем та процесів безпеки.

5. Підтримка політики інформаційної безпеки.

Організації, які обробляють інформацію про кредитні картки, повинні відповідати стандарту PCI DSS. Його недотримання може призвести до штрафів, обмежень або навіть до втрати можливості обробляти платежі за кредитними картками.

ITIL організована навколо низки процесів, які покликані допомогти організаціям ефективно та результативно надавати IT-послуги та керувати ними. Ці процеси охоплюють все: від управління інцидентами та проблемами до управління змінами та рівнем обслуговування [17].

Однією з ключових переваг ITIL є те, що вона забезпечує спільну мову та структуру для управління IT-послугами, що може допомогти організаціям покращити комунікацію та співпрацю між IT-командами та іншими частинами бізнесу.

ITIL також підкреслює важливість постійного вдосконалення, з акцентом на регулярному перегляді та вдосконаленні процесів, щоб забезпечити їх відповідність бізнес-цілям та завданням.

Хоча в деяких колах ITIL критикують за надмірну директивність та бюрократичність, багато організацій визнали його корисним інструментом для покращення надання IT-послуг та приведення IT у відповідність до потреб бізнесу. В останні роки ITIL також еволюціонував, щоб відобразити мінливі тенденції в наданні IT-послуг, з більшим акцентом на гнучких методологіях та development & operations (DevOps).

Впроваджуючи ці міжнародні стандарти та найкращі практики, підприємства можуть забезпечити відповідність своїх процесів управління ризиками світовим стандартам та підвищити загальний рівень інформаційної безпеки.

На додаток до міжнародних стандартів та передових підходів, згаданих вище, існує також кілька галузевих систем управління ризиками інформаційної безпеки. Наприклад, управління з регулювання фінансової індустрії (FINRA) розробило набір засобів контролю кібербезпеки для фінансової індустрії [18], а центр інтернет-безпеки (CIS) надав набір засобів контролю спеціально для безпеки хмарних технологій [19].

1.1.4 Нормативна база регулювання процесу управління ризиками в Україні

Нормативно-правова база управління ризиками інформаційної безпеки в Україні в першу чергу регулюється Законом України "Про захист інформації" ("Закон про захист інформації") [20], який встановлює правові засади захисту конфіденційної інформації та персональних даних.

Рада національної безпеки та оборони України (РНБО) відповідає за нагляд за дотриманням Закону про захист інформації та за створення нормативно-правової бази для управління ризиками інформаційної безпеки в країні. РНБО видала низку нормативно-правових актів та інструкцій, які містять рекомендації щодо управління ризиками інформаційної безпеки, зокрема Положення про порядок віднесення інформації до категорії конфіденційної та Положення про порядок забезпечення захисту інформації [21, 22].

Окрім нормативно-правових актів РНБО, на українські компанії також можуть поширюватися вимоги щодо управління ризиками інформаційної безпеки, передбачені іншими законами та нормативно-правовими актами, такими як Закон "Про кібербезпеку" [23] та Закон "Про електронні комунікації"[24].

Національний банк України (НБУ) також відповідає за нагляд за дотриманням правил інформаційної безпеки у фінансовому секторі. НБУ видав низку нормативно-правових актів та інструкцій, які містять рекомендації щодо управління ризиками інформаційної безпеки для банків та фінансових установ, зокрема Положення про безпеку інформаційно-телекомунікаційних систем банків та Інструкцію про порядок виявлення підозрілих операцій [25, 26]

На додаток до нормативної бази, встановленої РНБО та НБУ, існують також міжнародні стандарти та рамки управління ризиками інформаційної безпеки, які українські компанії можуть прийняти, наприклад, ISO/IEC 27001:2022 та NIST Cybersecurity Framework.

З метою подальшого зміцнення нормативно-правової бази в Україні за останні роки уряд ухвалив низку нових законів та підзаконних актів. Наприклад, у 2020 році було прийнято Закон "Про електронні довірчі послуги", який має на меті створити

правову основу для електронних підписів, печаток та позначок часу, а також електронних послуг рекомендованої доставки [27].

Уряд також створив Державний центр кібербезпеки України (ДЦКБУ), який відповідає за координацію та реалізацію стратегії кібербезпеки країни. ДЦКБ тісно співпрацює з іншими державними установами, а також з приватним сектором для виявлення та пом'якшення кіберзагроз.

Крім того, уряд започаткував ініціативи, спрямовані на підвищення обізнаності та освіти з питань кібербезпеки серед широкої громадськості та бізнесу. Наприклад, щорічно в жовтні проводиться Національний місяць обізнаності з питань кібербезпеки з метою донесення інформації про ризики та найкращі практики кібербезпеки.

Загалом, нормативно-правова база для управління ризиками інформаційної безпеки в Україні постійно розвивається, щоб йти в ногу з мінливим ландшафтом загроз. Для компаній, що працюють в Україні, важливо бути в курсі останніх законів, нормативних актів і передових практик, пов'язаних з управлінням ризиками інформаційної безпеки, щоб забезпечити дотримання вимог законодавства, захистити свої активи та репутацію.

1.2 Інформаційна безпека та бізнес

Інформаційна безпека є важливим аспектом сучасного бізнесу. Оскільки організації продовжують впроваджувати нові технології для підтримки своєї діяльності, вони наражаються на різні ризики, які можуть скомпрометувати їхні інформаційні активи. Тому для бізнесу важливо впроваджувати ефективні практики інформаційної безпеки, щоб забезпечити конфіденційність, цілісність та доступність своїх даних.

Інформаційна безпека охоплює цілий ряд заходів, включаючи оцінку ризиків, аналіз загроз, управління вразливостями та реагування на інциденти. Оцінка ризиків є важливим кроком в управлінні інформаційною безпекою, оскільки вона допомагає компаніям виявляти потенційні загрози та вразливості, які можуть вплинути на їхні

інформаційні активи. Аналіз загроз передбачає розуміння природи ризиків, з якими стикається організація, в той час як управління вразливостями передбачає впровадження заходів для запобігання або зменшення цих ризиків. Реагування на інциденти – це процес реагування на інциденти безпеки, включаючи їх виявлення, локалізацію та мінімізацію наслідків.

Ефективні практики інформаційної безпеки вимагають залучення всіх зацікавлених сторін в організації. Підприємствам недостатньо покладатися на свої IT-відділи у впровадженні заходів безпеки. Всі співробітники, від генерального директора до рядового персоналу, повинні знати про ризики і про свою роль в управлінні цими ризиками. Крім того, компанії повинні дотримуватися відповідних законів та нормативних актів, пов'язаних з інформаційною безпекою, таких як Загальний регламент ЄС про захист даних та стандарт ISO/IEC 27001.

Інформаційна безпека та бізнес тісно пов'язані між собою. Інформація є критично важливим активом для бізнесу, а безпека цієї інформації має вирішальне значення для успіху та виживання організації. Без належних заходів інформаційної безпеки компанії ризикують втратити конфіденційні дані, зазнати фінансових збитків та зашкодити своїй репутації.

1.2.1 Поняття бізнесу в IT-компаніях

Концепція бізнесу в IT-компаніях зосереджена на наданні технологічних рішень для задоволення потреб клієнтів та отримання прибутку. IT-компанії працюють на висококонкурентному ринку, і їхній успіх безпосередньо пов'язаний зі здатністю надавати високоякісні послуги та рішення, які відповідають потребам клієнтів.

Щоб досягти цього, IT-компанії повинні застосовувати бізнес-орієнтований підхід до своєї діяльності. Це передбачає розуміння потреб та очікувань клієнтів, визначення ринкових тенденцій та можливостей, а також розробку та надання технологічних рішень, які відповідають цим потребам.

Ефективне управління бізнесом в ІТ-компаніях вимагає широкого спектру навичок, включаючи управління проектами, продажі та маркетинг, фінансовий менеджмент і стратегічне планування. ІТ-компанії також повинні приділяти значну увагу інноваціям, дослідженням та розробкам, щоб випереджати конкурентів і надавати клієнтам найсучасніші рішення.

Крім того, ІТ-компанії повинні приділяти значну увагу інформаційній безпеці, щоб захистити дані своїх клієнтів, зберегти їхню довіру. Інформаційна безпека має бути інтегрована в усі аспекти діяльності компанії, від проектування та розробки технологічних рішень до управління внутрішніми системами та процесами.

Також ІТ-компанії повинні розвивати сильну корпоративну культуру, яка заохочує інновації, співпрацю та безперервне навчання. Це включає в себе інвестиції в навчання та розвиток співробітників, просування культури прозорості та відкритого спілкування, а також виховання почуття причетності та відповідальності серед працівників.

Отже, концепція бізнесу в ІТ-компаніях зосереджена на наданні технологічних рішень, які задовольняють потреби клієнтів та приносять прибуток. Ефективне управління бізнесом в ІТ-компаніях вимагає широкого спектру навичок, включаючи управління проектами, продажі та маркетинг, фінансовий менеджмент та стратегічне планування. Крім того, ІТ-компанії повинні приділяти значну увагу інформаційній безпеці, культивувати сильну корпоративну культуру, заохочувати інновації та співпрацю між співробітниками.

1.2.2 Взаємозв'язок бізнесу та ІБ

Важливо розуміти, що інформаційна безпека – це не лише технічні питання, а й питання бізнесу. Для того, щоб ефективно управляти ризиками інформаційної безпеки, організації повинні розуміти взаємозв'язок між інформаційною безпекою та їхніми бізнес-цілями. Це включає в себе визначення критично важливих інформаційних активів, які необхідні для діяльності організації, розуміння

потенційного впливу інцидентів інформаційної безпеки на ці активи та розробку стратегій для зменшення цих ризиків.

Ефективне управління інформаційною безпекою може надати бізнесу конкурентну перевагу. Клієнти та партнери все частіше вимагають від організацій, з якими вони працюють, суворих заходів безпеки, та компанії, які можуть продемонструвати свою прихильність до безпеки, мають більше шансів на успіх на ринку. Крім того, інформаційна безпека може допомогти бізнесу відповідати нормативним вимогам, уникнути дорогих штрафів і санкцій.

Інформаційна безпека також відіграє важливу роль у забезпеченні бізнес-операцій. Оскільки підприємства продовжують впроваджувати нові технології, такі як хмарні обчислення та мобільні пристрої, вони повинні забезпечити безпеку своїх інформаційних активів. Заходи інформаційної безпеки можуть допомогти бізнесу зберегти конфіденційність, цілісність і доступність своїх даних, що дасть змогу впевнено здійснювати бізнес-операції.

Більше того, ризики інформаційної безпеки не обмежуються лише ІТ-відділом. Бізнес-рішення, такі як аутсорсинг або партнерство зі сторонніми постачальниками, також можуть наражати організації на ризики безпеки. Тому компанії повинні застосовувати цілісний підхід до управління інформаційною безпекою, залучаючи всі зацікавлені сторони в організації і розглядаючи ризики та переваги бізнес-рішень з точки зору безпеки.

Бізнес-лідери повинні усвідомлювати потенційні ризики, пов'язані з їхньою діяльністю, та надавати чіткі вказівки щодо вимог до безпеки інформаційних активів. Фахівці з ІБ, у свою чергу, повинні гарантувати, що їхні засоби контролю та процеси безпеки відповідають потребам бізнесу, а також ефективно впроваджуються та підтримуються.

Отже, інформаційна безпека є критично важливою для бізнесу для захисту своїх інформаційних активів, збереження довіри клієнтів, дотримання регуляторних вимог та здійснення бізнес-операцій. Ефективне управління інформаційною безпекою вимагає цілісного підходу, залучення всіх зацікавлених сторін в організації та врахування ризиків, переваг бізнес-рішень з точки зору безпеки. Таким чином, бізнес

може забезпечити високий рівень захищеності інформаційних активів та зосередитися на досягненні власних стратегічних цілей.

1.2.3 ROI та ROSI

ROI, або рентабельність інвестицій, – це фінансовий показник, який використовується для оцінки прибутковості інвестицій. Він вимірює величину прибутку від інвестиції по відношенню до її вартості. ROI виражається у відсотках і розраховується шляхом ділення чистого прибутку від інвестиції на її початкову вартість [28].

Розрахунок рентабельності інвестицій є важливим інструментом для бізнесу; слугує для визначення вартості інвестицій та прийняття обґрунтованих рішень про те, куди спрямовувати ресурси. Позитивне значення ROI означає, що інвестиції принесли більше доходу, ніж їхня вартість, тоді як негативне значення ROI вказує на те, що інвестиції виявилися збитковими.

ROI – це універсальний показник, який можна використовувати для оцінки інвестицій у різних сферах, таких як маркетинг, дослідження та розробки, інфраструктура. Загалом, інвестиції з високим показником рентабельності інвестицій вважаються більш привабливими, ніж інвестиції з низьким показником рентабельності інвестицій, оскільки вони приносять більший прибуток порівняно з їхньою вартістю.

Однак важливо зазначити, що показник рентабельності інвестицій має певні обмеження. Наприклад, він не враховує вартість грошей у часі, тобто майбутні грошові потоки не дисконтуються до їхньої теперішньої вартості. Крім того, ROI не враховує інші фактори, які можуть вплинути на прибутковість інвестицій, такі як інфляція, податки та ризики [28].

Незважаючи на ці обмеження, ROI залишається корисним інструментом для бізнесу при оцінці прибутковості інвестицій та прийняття обґрунтованих рішень щодо розподілу ресурсів. Розраховуючи рентабельність інвестицій, бізнес може

визначити можливості для зростання та інвестування, уникаючи при цьому інвестицій, які навряд чи принесуть позитивний прибуток.

Показник ROI також можна використовувати для вимірювання ефективності бізнес-стратегій та ініціатив. За допомогою цього показника бізнес може оцінити, які стратегії приносять найбільшу віддачу, і відповідно до цього скоригувати свій підхід. Це може допомогти оптимізувати діяльність та максимізувати прибутковість.

Окрім оцінки фінансової ефективності інвестицій та стратегій, ROI також можна використовувати для оцінки ефективності роботи окремих співробітників або команд. Наприклад, відстежуючи рентабельність інвестицій у відділ продажів, компанії можуть оцінити ефективність стратегій продажів та визначити сфери для вдосконалення.

Нижче наведений приклад того, як можна розрахувати рентабельність інвестицій.

Припустимо, що бізнес інвестує $50 000 у маркетингову кампанію для збільшення продажів. Після кампанії бізнес отримує додатково $100 000 доходу від продажів. Собівартість реалізованої продукції (COGS), пов'язана з додатковими продажами, становить $30 000, що включає витрати на матеріали, робочу силу та інші витрати, безпосередньо пов'язані з продажами.

Рентабельність інвестицій для цієї маркетингової кампанії розраховується наступним чином [28]:

ROI = (Прибуток від інвестицій - Витрати на інвестиції) / Витрати на інвестиції (1.1)

ROI = (($100,000 - $30,000) - $50,000) / $50,000 = 0,4

РЕНТАБЕЛЬНІСТЬ ІНВЕСТИЦІЙ = 0,4 × 100% = 40%

У цьому прикладі рентабельність інвестицій у маркетингову кампанію становить 40%, що свідчить про позитивну фінансову віддачу від інвестицій.

Цей розрахунок може допомогти бізнесу оцінити ефективність маркетингової кампанії та прийняти обґрунтовані рішення щодо майбутніх інвестицій у маркетинг або інші сфери бізнесу.

Загалом, рентабельність інвестицій є цінним показником, який може дати уявлення про фінансову ефективність інвестицій, стратегій та окремих працівників. Однак важливо використовувати ROI в поєднанні з іншими показниками та враховувати обмеження цього показника, щоб приймати обґрунтовані рішення щодо розподілу ресурсів та бізнес-стратегії.

ROSI (Return on Security Investment) – це фінансовий показник, який використовується для оцінки ефективності та результативності інвестицій в інформаційну безпеку. Він схожий на ROI, але фокусується саме на впливі інвестицій у безпеку на загальні фінансові показники бізнесу [29].

При розрахунку ROSI враховуються витрати, пов'язані з впровадженням та підтримкою заходів безпеки, а також фінансові вигоди, які є результатом цих заходів. Це може включати такі фактори, як зниження ризику витоку даних і кібератак, поліпшення відповідності нормативним вимогам, а також підвищення довіри та лояльності клієнтів.

ROSI також можна використовувати для обґрунтування інвестицій в інформаційну безпеку перед зацікавленими сторонами та особами, які приймають рішення в компанії. Продемонструвавши фінансові вигоди від інвестицій у безпеку з точки зору зниження ризиків та покращення бізнес-результатів, компанії можуть зробити переконливі аргументи на користь інвестицій в інформаційну безпеку.

Однак важливо зазначити, що розрахунок ROSI може бути складним та вимагати участі багатьох відділів та зацікавлених сторін у компанії. Крім того, ROSI слід використовувати в поєднанні з іншими показниками, такими як оцінка ризиків та аудит безпеки, щоб переконатися, що інвестиції в безпеку відповідають загальному профілю ризиків і бізнес-цілям організації.

Розрахунок ROSI може відрізнятися залежно від конкретної інвестиції та її очікуваної прибутковості. Однак, ось приклад того, як можна розрахувати ROSI.

Припустимо, що компанія інвестує $100 000 у нову систему безпеки, яка, як очікується, знизить ризик витоку даних на 50%. Вартість витоку даних для бізнесу оцінюється в $500 000.

До інвестицій щорічний ризик витоку даних розраховується як 500 000 доларів США, помножені на ймовірність витоку даних, скажімо, 10%, що дорівнює 50 000 доларів США.

Після інвестицій щорічний ризик витоку даних знижується до $25 000 (50% від $50 000).

ROSI для цієї інвестиції розраховується наступним чином [29]:

ROSI = (Річна фінансова вигода - Річні інвестиції) / Річні інвестиції (1.2)

ROSI = (($50000 - $25 000) - $100 000)/ $100 000 = -0,75

ROSI = -0,75 × 100% = -75%.

У цьому прикладі ROSI для інвестицій в нову систему безпеки становить -75%, що свідчить про негативну фінансову віддачу від інвестицій. Цей розрахунок може допомогти бізнесу обґрунтувати інвестиції перед зацікавленими сторонами та особами, які приймають рішення, а також дає можливість оцінити ефективність системи безпеки з плином часу.

Отже, ROSI може надати цінну інформацію про фінансову ефективність інвестицій в інформаційну безпеку та допомогти компаніям приймати обґрунтовані рішення щодо розподілу ресурсів та управління ризиками. Однак важливо зазначити, що ROSI – це лише один з багатьох факторів, які слід враховувати при оцінці ефективності інвестицій в інформаційну безпеку. Інші фактори, такі як загальний стан безпеки організації та конкретні ризики і загрози, з якими вона стикається, також повинні бути взяті до уваги.

1.3 Корпоративний ризик-менеджмент

Управління корпоративними ризиками – це процес, за допомогою якого організація виявляє, оцінює та управляє ризиками, що можуть вплинути на її здатність досягати своїх цілей. Корпоративні ризики можуть виникати з різних джерел, включаючи економічні, фінансові, операційні, юридичні, регуляторні,

репутаційні та стратегічні фактори. Ефективне управління корпоративними ризиками передбачає створення системи управління ризиками та впровадження політик і процедур для систематичного та скоординованого управління ризиками.

Основні етапи корпоративного управління ризиками включають [30]:

- ідентифікацію ризиків: визначення потенційних ризиків, які можуть вплинути на цілі, діяльність або репутацію організації;
- оцінку ризиків: оцінка ймовірності та потенційного впливу ідентифікованих ризиків, а також визначення їхньої пріоритетності на основі їхньої значущості;
- пом'якшення ризиків: розробка та впровадження стратегій зниження ризиків для зменшення ймовірності та/або впливу ідентифікованих ризиків;
- моніторинг ризиків: моніторинг ефективності стратегій мінімізації ризиків та виявлення нових ризиків у міру їх виникнення;
- звітування про ризики: інформування про діяльність та результати управління ризиками зацікавлених сторін, зокрема вищого керівництва, ради директорів та зовнішніх сторін, таких як інвестори та регуляторні органи.

Для впровадження ефективної корпоративної програми управління ризиками організаціям необхідно створити систему управління ризиками, яка визначає ролі та обов'язки, ідентифікує процеси та інструменти управління ризиками, а також забезпечує керівництво для діяльності з управління ризиками. Система управління ризиками повинна бути адаптована до конкретних потреб, розміру та складності організації.

Крім того, організації повинні розробити політику та процедури управління ризиками, які надають чіткі вказівки щодо того, як виявляти, оцінювати, зменшувати та контролювати ризики. Ці політики та процедури повинні бути доведені до відома всіх працівників та зацікавлених сторін, щоб гарантувати, що кожен розуміє свою роль та обов'язки в управлінні ризиками.

Управління ризиками має бути безперервним процесом, інтегрованим у загальний процес управління та прийняття рішень в організації. Це має бути безперервний цикл виявлення, оцінки, пом'якшення та моніторингу ризиків, а також адаптації до змін у внутрішньому та зовнішньому середовищі організації.

Крім того, управління ризиками має бути інтегроване з іншими бізнес-процесами, такими як стратегічне планування, управління ефективністю та внутрішній контроль. Така інтеграція може допомогти забезпечити врахування ризиків у всіх процесах прийняття рішень, а також узгодження апетиту організації до ризику з її стратегічними цілями.

Нарешті, організації повинні регулярно переглядати та оновлювати свою програму управління ризиками, щоб забезпечити її ефективність та актуальність. Цей перегляд має включати оцінку ефективності стратегій зменшення ризиків та виявлення нових ризиків і нових загроз.

Таким чином, ефективне корпоративне управління ризиками має вирішальне значення для досягнення організаціями своїх цілей та процвітання в динамічному, невизначеному середовищі. Створивши структуру, політику та процедури управління ризиками, інтегрувавши управління ризиками з іншими бізнес-процесами, а також регулярно переглядаючи та оновлюючи програму управління ризиками, організації можуть підвищити свою загальну ефективність та стійкість.

1.3.1 Корпоративні ризики

Корпоративні ризики – це потенційні загрози, з якими компанія чи організація може зіткнутися у своїй діяльності, фінансах, репутації чи дотриманні законодавства. Ці ризики можуть виникати з різних джерел, включаючи економічні, правові, політичні, соціальні, технологічні, екологічні та операційні фактори [30].

Інформаційні ризики та корпоративні ризики є спорідненими поняттями, але мають деякі важливі спільні риси та відмінності.

Схожість закладається в наведених нижче фактах.

Як інформаційні, так і корпоративні ризики можуть мати негативний вплив на діяльність компанії, її репутацію та фінансові показники.

Обидва типи ризиків потребують постійного моніторингу та оцінки для виявлення потенційних загроз і вразливостей.

Також вони потребують стратегії управління ризиками, яка визначає пріоритети запобігання, виявлення та реагування.

Також варто згадати і наявні відмінності між цими поняттями.

Сфера застосування. Інформаційні ризики в першу чергу стосуються безпеки та конфіденційності даних та інформаційно-технологічних систем, тоді як корпоративні ризики можуть охоплювати ширший спектр ризиків, включаючи фінансові, юридичні, операційні та репутаційні ризики.

Спрямованість. Інформаційні ризики зазвичай зосереджені на захисті даних і систем від зовнішніх та внутрішніх загроз, тоді як корпоративні ризики зосереджені на управлінні ризиками в масштабах всієї організації та різних зацікавлених сторін.

Власність. Інформаційні ризики часто належать та керуються IT-відділами або іншими технічними командами, тоді як корпоративні ризики, як правило, – вищим керівництвом або радою директорів.

Наслідки. Наслідки інформаційних ризиків часто пов’язані з витоком даних, крадіжкою конфіденційної інформації або простоєм системи, тоді як наслідки корпоративних ризиків можуть бути ширшими та містити в собі фінансові втрати, юридичні зобов’язання та шкоду репутації.

Таким чином, хоча інформаційні ризики та корпоративні ризики мають певну схожість, вони є різними поняттями, які вимагають різних підходів до управління ризиками. Компаніям необхідно розробити комплексну стратегію управління ризиками, яка враховує обидва типи ризиків, щоб забезпечити постійний захист своїх активів, операцій та репутації.

1.3.2 Інформаційні ризики та бізнес-ризики

Інформаційні ризики та бізнес-ризики тісно пов’язані між собою, оскільки інформація є критично важливим активом для більшості підприємств, і нездатність захистити її може мати значні наслідки для організації. Інформаційні ризики – це потенційні загрози конфіденційності, цілісності та доступності інформації, такі як витік даних, кібератаки або людські помилки. Бізнес-ризики – це потенційні загрози

здатності організації досягати своїх цілей, такі як фінансові втрати, шкода репутації, юридичні зобов’язання або операційні перебої.

Інформаційні ризики можуть впливати на бізнес-ризики кількома способами [31]. Наприклад:

1. Фінансові втрати: витік даних або кібератака можуть призвести до значних фінансових втрат для компанії, таких як витрати, пов’язані з усуненням наслідків, судові витрати та регуляторні штрафи. Це може вплинути на фінансові показники організації та її здатність досягати своїх цілей.

2. Репутаційні збитки: витік даних або наслідки кібератак можуть також зашкодити репутації компанії, що може вплинути на її відносини з клієнтами, партнерами та іншими зацікавленими сторонами. Пошкодження репутації може призвести до втрати бізнесу, зменшення частки ринку та зниження доходів.

3. Юридичні зобов’язання: порушення або інші інциденти інформаційної безпеки можуть призвести до юридичних зобов’язань для компанії, таких як позови від постраждалих осіб або регуляторні штрафи. Ці зобов’язання можуть також вплинути на фінансові показники організації та її здатність досягати своїх цілей.

4. Операційні перебої: інформаційні ризики також можуть призвести до операційних збоїв, наприклад, до простою системи або втрати критично важливих даних. Такі перебої можуть вплинути на здатність організації надавати продукти або послуги клієнтам, що може вплинути на її фінансові показники та репутацію.

5. Невигідне конкурентне становище: інформаційні ризики можуть поставити компанію в невигідне конкурентне становище, ставлячи під загрозу її здатність захищати конфіденційну інформацію та комерційну таємницю. Це може призвести до втрати конкурентних переваг, зменшення частки ринку та зниження доходів.

6. Комплаєнс-порушення: інформаційні ризики також можуть призвести до порушень комплаєнсу, наприклад, недотримання правил захисту даних або галузевих стандартів. Порушення комплаєнсу може призвести до юридичних зобов’язань, репутаційних збитків та втрати бізнесу.

7. Продуктивність працівників: інформаційні ризики також можуть впливати на продуктивність працівників, спричиняючи простої системи, низьку швидкість мережі або інші проблеми, пов’язані з IT. Це може призвести до зниження продуктивності, пропущених дедлайнів і зменшення доходів.

8. Стратегічні ризики: інформаційні ризики також можуть створювати стратегічні ризики для компанії, впливаючи на її здатність виконувати свої стратегічні цілі. Наприклад, якщо компанія не в змозі захистити свої критичні інформаційні активи, вона не зможе впроваджувати інновації або використовувати нові ринкові можливості, що може вплинути на її довгострокове зростання та стійкість.

9. Довіра клієнтів: також може бути вплив на довіру та лояльність клієнтів. Якщо компанія не може захистити конфіденційну інформацію своїх клієнтів, вона може втратити їхню довіру та лояльність, що може вплинути на її доходи та репутацію.

10. Ризики в ланцюжку поставок: інформаційні ризики також можуть створювати ризики для ланцюга постачання, впливаючи на безпеку партнерів та постачальників компанії. Якщо постачальника або партнера скомпрометовано, це може призвести до витоку даних або інших інцидентів з інформаційною безпекою, які можуть вплинути на діяльність компанії та її доходи.

Аналізуючи інформацію вище, варто розуміти, що бізнес-ризики також можуть мати значний вплив на інформаційні ризики, оскільки вони взаємопов’язані. Коли компанія зіштовхується з бізнес-ризиком, це може збільшити ймовірність або серйозність інформаційних ризиків. Нижче наведено декілька прикладів.

Фінансовий тиск на компанію може збільшити ймовірність інформаційних ризиків, таких як шахрайство або крадіжка даних. Наприклад, якщо компанія стикається з фінансовими труднощами, її співробітники можуть бути схильні до шахрайських дій для отримання доходу або бонусів.

Плинність кадрів може збільшити ризик витоку інформації, особливо коли працівники звільняються з доступом до конфіденційної інформації. Це може

призвести до витоку даних або інших інцидентів безпеки, особливо якщо працівник, який звільняється, незадоволений після співпраці.

Об’єднання або поглинання компаній можуть створювати значні інформаційні ризики, особливо якщо компанія-покупець не проводить ретельної юридичної перевірки. Це може призвести до придбання вразливих ІТ-систем або витоку даних, про які не було повідомлено під час процесу поглинання.

Організаційні зміни, такі як реструктуризація або скорочення штату, можуть збільшити ризик витоку інформації через плутанину або невпевненість серед працівників. Це може призвести до помилок або прогалин у протоколах безпеки, або зловмисних дій працівників, які відчувають загрозу від змін.

Ринкова конкуренція може збільшити ризик витоку інформації, особливо якщо компанія бере участь в агресивному маркетингу або цінових війнах. Це може призвести до того, що компанії будуть ігнорувати інформаційну безпеку або вдаватимуться до неетичної поведінки, щоб отримати перевагу над конкурентами.

Таким чином, взаємозв’язок між бізнес-ризиками та інформаційними ризиками є складним та багатогранним, а ефективне управління ризиками вимагає комплексного підходу, що враховує обидва типи ризиків. Надаючи пріоритет інформаційній безпеці та конфіденційності у своїй загальній стратегії управління ризиками, компанії можуть захистити свої активи, зміцнити репутацію та досягти своїх бізнес-цілей.

Висновки за розділом 1

Управління ризиками є критично важливим аспектом інформаційних систем, який допомагає виявляти, оцінювати та визначати пріоритети ризиків для інформаційних активів організації. Ефективне управління ризиками в ІС передбачає розробку стратегій для зменшення ризиків, а також постійний моніторинг та оновлення цих стратегій для забезпечення їхньої ефективності.

Класифікація ризиків передбачає розподіл ризиків за категоріями на основі їхньої ймовірності та впливу. Цей процес допомагає організаціям визначати

пріоритети в управлінні ризиками, зосереджуючись на найбільш значущих ризиках у першу чергу.

Процес управління ризиками, як правило, включає виявлення ризиків, оцінку їхньої ймовірності та впливу, розробку стратегій для їхнього пом'якшення, впровадження цих стратегій, а також постійний моніторинг та оновлення їх за необхідності.

Міжнародні стандарти, такі як ISO 27001 та NIST SP 800-53, містять настанови та найкращі практики, яких організації можуть дотримуватися при впровадженні процесів управління ризиками інформаційної безпеки. Ці стандарти визначають системний підхід до управління ризиками, що включає оцінку ризиків, обробку ризиків та постійний моніторинг.

В Україні нормативно-правова база управління ризиками інформаційної безпеки знаходиться під наглядом Державної служби спеціального зв'язку та захисту інформації. Агентство встановлює правила та стандарти інформаційної безпеки в державному та приватному секторах, щоб забезпечити ефективне управління організаціями ризиками інформаційної безпеки.

Дотримання міжнародних стандартів та національних норм є важливим для забезпечення ефективності стратегій управління ризиками інформаційної безпеки та захисту конфіденційних даних від кіберзагроз.

Бізнес в IT-компаніях передбачає застосування бізнес-принципів до технологічного сектору. Він включає в себе такі види діяльності, як управління проектами, стратегічне планування та фінансовий менеджмент, спрямовані на досягнення бізнес-цілей за допомогою використання технологій.

Бізнес та ІС тісно пов'язані між собою, причому інформаційні системи відіграють вирішальну роль у забезпеченні та підтримці бізнес-операцій. Ефективне управління ІС має важливе значення для досягнення бізнес-цілей, а успіх будь-якої організації залежить від інтеграції бізнес-стратегій та стратегій ІС.

ROI (Return on Investment) і ROSI (Return on Security Investment) – це показники, які використовуються для оцінки ефективності інвестицій в інформаційну безпеку.

ROI вимірює фінансову віддачу від інвестицій, в той час як ROSI оцінює цінність інвестицій в безпеку з точки зору зниження ризиків.

Управління корпоративними ризиками передбачає виявлення та оцінку ризиків, які можуть вплинути на діяльність організації, а також розробку стратегій для їх пом’якшення. Цей процес допомагає організаціям мінімізувати вплив ризиків на їхні бізнес-цілі та покращити загальну ефективність.

Взаємозв’язок між інформаційними та бізнес-ризиками тісно пов’язаний, а ефективне управління ризиками вимагає комплексного підходу, який враховує обидва типи ризиків.

Інформаційні ризики, такі як витік даних та кібератаки, можуть мати значний вплив на здатність організації досягати своїх бізнес-цілей, наприклад, втрата репутації, фінансові збитки та юридичні зобов’язання.

Бізнес-ризики, такі як волатильність ринку, дотримання нормативних вимог або стихійні лиха, також можуть впливати на інформаційні активи організації та її здатність здійснювати бізнес-операції.

Тому ефективне управління ризиками вимагає комплексного підходу, який враховує як інформаційні, так і бізнес-ризики. Організації повинні виявляти та оцінювати ризики, які можуть вплинути на їхні інформаційні активи та бізнес-цілі, а також розробляти стратегії для зменшення цих ризиків.

РОЗДІЛ 2
МЕТОДИ ОЦІНКИ РИЗИКІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Оцінка ризиків – це важливий процес в інформаційній безпеці, який передбачає виявлення потенційних ризиків та вразливостей для активів, даних і систем організації, а також оцінку ймовірності та потенційного впливу цих ризиків.

Мета оцінки ризиків – допомогти організаціям визначити пріоритети своїх зусиль у сфері безпеки та ефективно розподілити ресурси для пом'якшення найбільш значущих ризиків.

Процес оцінки ризиків, як правило, складається з наступних етапів [32]:

1. Ідентифікація активів. Першим кроком в оцінці ризиків є визначення активів організації, тобто дані, системи, додатки та інфраструктура.

2. Визначення загроз:. Наступним кроком є визначення потенційних загроз для активів організації, таких як шкідливе програмне забезпечення, фішингові атаки або внутрішні загрози.

3. Оцінка вразливостей. Третій крок – оцінка вразливостей або слабких місць в активах організації, які можуть бути використані виявленими загрозами.

4. Аналіз ризиків. Четвертий етап – аналіз ймовірності та потенційного впливу виявлених ризиків на основі таких, як правило, факторів: ймовірність виникнення загрози та серйозність вразливості.

5. Визначення пріоритетності ризиків. На цьому етапі визначається пріоритетність ризиків на основі їхньої ймовірності та потенційного впливу, щоб допомогти організації зосередити свої зусилля та ресурси у сфері безпеки на найбільш значущих ризиках.

6. Розробка стратегії зменшення ризиків. Останнім кроком є розробка стратегій зменшення ризиків, спрямованих на усунення виявлених ризиків. Це може включати впровадження засобів контролю безпеки, таких як брандмауери чи антивірусне програмне забезпечення, або впровадження політик та процедур для мінімізації ризику людських помилок чи внутрішніх загроз.

Загалом, оцінка ризиків – це безперервний процес, який вимагає постійного моніторингу та оновлення, оскільки ландшафт загроз, а також активи та системи організації з часом змінюються. Проводячи регулярну оцінку ризиків та впроваджуючи відповідні стратегії зменшення ризиків, організації можуть посилити свою безпеку та захистити свої активи та дані від кіберзагроз.

Цей розділ присвячений розгляду відомих методів, що регулюють процес оцінки ризиків.

2.1 Класифікація методів оцінки ризиків

В інформаційній безпеці існує кілька методів оцінки ризиків, які можна використовувати для виявлення, аналізу та оцінки потенційних ризиків, вразливостей для активів, даних і систем організації. Ці методи можна умовно поділити на такі категорії [33]:

1. Якісні методи оцінки ризиків – передбачають використання суб'єктивних суджень для оцінки та визначення пріоритетності ризиків на основі їхньої ймовірності та потенційного впливу на організацію. Якісна оцінка використовує такі шкали, як низький, середній або високий для ранжування ризиків. Цей метод часто використовується, коли є обмежена кількість даних або коли потенційні ризики важко оцінити кількісно.

2. Кількісні методи оцінки ризиків – присвоєння числових значень ймовірності та впливу ідентифікованих ризиків, щоб розрахувати бал ризику або ймовірність настання. Кількісна оцінка ризиків використовує статистичні та математичні моделі для оцінки ризиків. Ці методи часто використовуються, коли є велика кількість даних, та потенційні ризики можна оцінити кількісно.

3. Методи оцінки ризиків на основі активів – відповідають за виявлення та оцінку ризиків, пов'язаних з критично важливими активами організації, такими як дані, системи, додатки та інфраструктура. Оцінка ризиків на основі активів дозволяє організаціям визначати пріоритети у сфері безпеки та ефективніше розподіляти ресурси.

4. Методи оцінки ризиків на основі загроз – передбачають виявлення та аналіз потенційних загроз для активів, систем організації. Оцінка ризиків на основі загроз слугує для розробки відповідних контрзаходів для запобігання або пом'якшення наслідків порушення безпеки.

5. Методи оцінки ризиків на основі сценаріїв – основними цілями таких методів є створення гіпотетичних сценаріїв та оцінку потенційних ризиків, вразливостей, пов'язаних з кожним сценарієм. Оцінка ризиків на основі сценаріїв може допомогти організаціям визначити пріоритети своїх потреб у сфері безпеки на основі найбільш ймовірних та впливових ризиків.

6. Методи оцінки ризиків на основі контролю: передбачається оцінка ефективності існуючих засобів контролю безпеки та визначення областей, де можуть знадобитися додаткові засоби контролю. Оцінка ризиків на основі засобів контролю може допомогти організаціям переконатися, що їхні засоби контролю безпеки є належними та ефективними у зменшенні виявлених ризиків.

7. Методи оцінки ризиків на основі відповідності вимогам – оцінка відповідності організації нормативним і галузевим стандартам, пов'язаним з інформаційною безпекою. Оцінка ризиків на основі комплаєнсу може допомогти організаціям виявити прогалини в їх дотриманні та вжити відповідних заходів для усунення цих прогалин.

При оцінці ризиків варто звернути увагу також на декілька суміжних процесів, а саме [33]:

- аналіз впливу на бізнес (Business Impact Analysis, BIA): аналіз потенційного впливу порушення безпеки на бізнес-операції організації, включаючи фінансові, репутаційні та юридичні наслідки. BIA може допомогти організаціям визначити пріоритети у сфері безпеки та ефективніше розподіляти ресурси на основі найбільш значущих бізнес-ризиків;

- аналіз дерева атак: розбиття потенційного сценарію атаки на низку кроків або подій, а також визначення вразливостей, способів пом'якшення наслідків, пов'язаних з кожним кроком. Аналіз дерева атак може допомогти організаціям

виявити найбільш критичні вразливості та розробити відповідні контрзаходи для запобігання або пом'якшення наслідків атаки;

- тестування на проникнення: імітація атаки на системи та мережі організації для виявлення вразливостей та оцінки ефективності існуючих засобів контролю безпеки. Тестування на проникнення може допомогти організаціям виявити та визначити пріоритетність ризиків безпеки та розробити відповідні контрзаходи для їх зменшення;
- система управління ризиками (RMF): структурований підхід до управління ризиками протягом усього життєвого циклу розробки системи. RMF включає шість етапів: категоризація, відбір, реалізація, оцінка, авторизація та моніторинг. RMF може допомогти організаціям більш ефективно управляти ризиками та гарантувати, що їхні засоби контролю безпеки є належними та ефективними для пом'якшення виявлених ризиків [34];
- управління ризиками ланцюга постачання (SCRM): виявлення та оцінка потенційних ризиків, пов'язаних з постачальниками, продавцями та партнерами організації. SCRM може допомогти організаціям виявити та зменшити ризики ланцюга постачання, які можуть вплинути на їхню власну безпеку [35].

Організації можуть використовувати один або декілька з цих методів оцінки ризиків для виявлення, аналізу та оцінки потенційних ризиків або вразливостей безпеки, а також для розробки відповідних контрзаходів для зменшення цих ризиків. Вибір методу оцінки ризиків буде залежати від конкретних потреб, цілей та толерантності до ризиків організації.

2.1.1 Якісні методи оцінки ризиків

Якісна оцінка ризиків – це метод аналізу ризиків, який передбачає суб'єктивне судження експертів або зацікавлених сторін для виявлення та визначення пріоритетності потенційних ризиків на основі їхньої ймовірності та потенційного впливу. На відміну від кількісної оцінки ризиків, якісна оцінка ризиків не використовує числові значення для оцінки ризиків, а натомість покладається на якісні

шкали, такі як низький, середній або високий, для ранжування ризиків за ступенем їхньої серйозності.

Якісні методи оцінки ризиків можна використовувати, коли є обмежена кількість даних або коли потенційні ризики важко оцінити кількісно. Цей метод може бути використаний для визначення найбільш значущих ризиків, які потребують негайної уваги, а також для більш ефективного визначення пріоритетів у сфері безпеки та розподілу ресурсів.

Деякі з найпоширеніших процесів або методів, що використовують якісну оцінку ризиків:

1. Мозковий штурм: групова дискусія для виявлення потенційних ризиків та вразливостей, пов'язаних з активами, даними, системами організації. Цей метод використовується для генерування широкого спектру ідей та поглядів від зацікавлених сторін та експертів.

2. Метод Дельфі: проведення серії опитувань або анкетування для збору та узагальнення думок експертів щодо потенційних ризиків, їхньої ймовірності та впливу. Цей метод може допомогти досягти консенсусу серед експертів та зменшити упередженість [36].

3. Рейтинг ризиків: використання якісних шкал для оцінки ризиків на основі їхньої ймовірності та потенційного впливу. Рейтинг ризиків визначає пріоритетність ризиків та допомагає більш ефективно розподілити ресурси.

4. SWOT-аналіз: визначення сильних та слабких сторін, можливостей і загроз організації. Цей метод виявляє потенційні ризики та вразливості, які можуть вплинути на стан безпеки організації [37].

5. Експертна оцінка: пошук думок та поглядів експертів у певній галузі, зацікавлених сторін і професіоналів галузі для виявлення та оцінки потенційних ризиків. Цей метод може бути особливо корисним при оцінці нових загроз або ризиків, пов'язаних з новими технологіями.

6. Аналіз сценаріїв: створення гіпотетичних сценаріїв або ситуацій та аналіз потенційних ризиків, впливів, пов'язаних з кожним сценарієм. Цей метод

використовується для виявлення ризиків, які, можливо, не розглядалися раніше, та для оцінки потенційного впливу порушення безпеки або інциденту.

7. FMEA (Failure Mode and Effects Analysis): структурований метод, який використовується для виявлення та оцінки потенційних ризиків, вразливостей, пов'язаних з продуктом, процесом або системою. Метод включає в себе визначення режимів відмов та аналіз потенційних наслідків кожного режиму відмови [38].

8. Самооцінка контролю (CSA): CSA – це процес, який використовується для оцінки внутрішнього контролю організації та виявлення потенційних ризиків, вразливостей. Метод передбачає проведення самооцінки контролів та визначення сфер, де контролі можуть бути покращені або посилені [39].

9. Аналіз контрольних списків: створення переліку потенційних ризиків, вразливостей та оцінка кожного ризику на основі набору критеріїв або стандартів. Цей метод корисний для виявлення та визначення пріоритетності ризиків, а також для розробки відповідних контрзаходів на основі заздалегідь визначених критеріїв.

10. Самооцінка контрольних ризиків (CRSA): CRSA – це процес, який використовується для оцінки системи внутрішнього контролю організації та виявлення потенційних ризиків та вразливостей, пов'язаних з нею. Метод передбачає проведення самооцінки контролів та визначення сфер, де контролі можуть бути покращені або посилені [40].

11. HAZOP (Hazard and Operability Study): HAZOP – це структурований метод, який використовується для виявлення та оцінки потенційних ризиків та вразливостей, пов'язаних з процесом або системою. Метод передбачає розбиття процесу або системи на менші компоненти та аналіз потенційних небезпек, операційних проблем, пов'язаних з кожним компонентом [41].

12. Матриця ризиків: графічний інструмент, який використовується для оцінки потенційних ризиків та вразливостей на основі їхньої ймовірності та впливу. Метод передбачає присвоєння якісного балу кожному ризику на основі заздалегідь визначеної шкали та нанесення балів на матрицю. Матриця ризиків може допомогти ідентифікувати та визначити пріоритетність ризиків, а також розробити відповідні контрзаходи на основі серйозності ризиків [42].

13. Аналіз дерева несправностей (FTA): FTA – це метод, який використовується для виявлення та оцінки потенційних ризиків та вразливостей, пов'язаних з системою або процесом. Метод передбачає створення діаграми, яка показує послідовність подій, що можуть призвести до певного збою або інциденту.

Отже, якісні методи ґрунтуються на суб'єктивних судженнях, експертних оцінках та інших якісних критеріях для оцінки ймовірності та впливу різних ризиків. Якісні методи оцінки ризиків особливо корисні при роботі зі складними системами або процесами, де існує обмежена кількість даних або невизначеність щодо ризиків, пов'язаних з ними [43].

Хоча якісні методи оцінки ризиків можуть не надавати стільки деталей, як кількісні методи, вони можуть бути ефективним інструментом для виявлення та оцінки ризиків в економічно ефективний та результативний спосіб.

2.1.2 Кількісні методи оцінки ризиків

Кількісні методи оцінки ризиків – це більш об'єктивний і заснований на даних підхід до оцінки потенційних ризиків та вразливостей в інформаційній безпеці. Ці методи використовують статистичний аналіз та математичні моделі для вимірювання ймовірності та впливу різних ризиків.

Нижче наведені поширені процеси або методи, що використовують кількісну оцінку ризиків:

1. Очікуваний річний збиток (Annualized Loss Expectancy, ALE): використовується для розрахунку очікуваних збитків від потенційного ризику протягом одного року. Формула ALE – це добуток річної частоти виникнення (ARO) та очікуваної величини одноразового збитку (SLE). ARO – це очікувана частота інцидентів, що відбуваються протягом року, а SLE –це очікувані збитки від одного інциденту [44].

2. Кількісний аналіз ризику (QRA): використовується для розрахунку ймовірності та серйозності потенційного ризику. Процес передбачає виявлення

потенційних ризиків, аналіз ймовірності та впливу кожного ризику, а також присвоєння кожному ризику числового значення на основі його критичності [45].

3. Аналіз Монте-Карло: метод моделювання, який використовується для оцінки ймовірності та впливу потенційних ризиків. Потрібен для створення моделі системи або процесу, що аналізується, моделювання потенційних сценаріїв та аналіз результатів моделювання [46].

4. Тестування на введення відмов: метод, який використовується для виявлення потенційних ризиків та вразливостей шляхом навмисного введення несправностей або помилок в систему або процес. Тестування являє собою моделювання потенційних сценаріїв та аналіз результатів для виявлення потенційних ризиків.

5. Оцінка вразливостей: використовується для виявлення та вимірювання потенційних вразливостей в системі або процесі. Процес передбачає аналіз системи або процесу для виявлення потенційних вразливостей, присвоєння числового значення кожній вразливості на основі її критичності та розробку відповідних контрзаходів на основі числових значень, присвоєних кожній вразливості.

6. Моделювання загроз: виявлення потенційних загроз та вразливостей в системі або процесі.

7. Аналіз впливу на бізнес (BIA): BIA – оцінка потенційного впливу ризику на бізнес-операції організації. Метод передбачає аналіз потенційних наслідків ризику, присвоєння числового значення кожному наслідку залежно від його критичності та розробку відповідних контрзаходів на основі числових значень, присвоєних кожному наслідку [47].

8. Кількісна оцінка кіберризиків (QCRA): оцінка потенційних кіберризиків для організації на основі аналітики, заснованої на даних. Метод передбачає аналіз даних з різних джерел, таких як мережеві журнали, журнали додатків, поведінка користувачів, для виявлення потенційних вразливостей та загроз [48].

9. Баєсова мережа або модель: імовірнісний метод, який використовується для оцінки потенційних ризиків та вразливостей в системі або процесі. Метод передбачає створення моделі системи або процесу, присвоєння ймовірностей різним

подіям та результатам, аналіз результатів моделі для виявлення потенційних ризиків і вразливостей [49].

10. Формула ризику: використання математичної формули для розрахунку потенційного ризику інциденту безпеки на основі ймовірності та наслідків інциденту. Формулу можна налаштувати відповідно до конкретних потреб організації.

Кількісні методи можуть дати чітке уявлення про потенційні фінансові наслідки інциденту безпеки, що може допомогти організаціям визначити пріоритети своїх зусиль у сфері безпеки та відповідно розподілити ресурси.

Однак точність методів кількісної оцінки ризиків залежить від якості використовуваних даних, а для збору, аналізу та інтерпретації даних організаціям потрібні необхідні ресурси та експертиза. Складність цих методів може вимагати використання комбінації кількісних та якісних методів оцінки ризиків, щоб отримати комплексне уявлення про ризики для безпеки компанії.

Отже, кількісні методи оцінки ризиків можуть бути корисним інструментом для організацій при оцінці ризиків їхньої безпеки та розробки відповідних контрзаходів.

2.2 Відомі методи оцінки ризиків

Існує багато відомих методів оцінки ризиків в інформаційній безпеці, які організації можуть використовувати для оцінки своїх ризиків та розробки відповідних контрзаходів. Ці методи варіюються від якісних до кількісних та передбачають різні підходи до оцінки ризиків, включаючи визначення активів, загроз, вразливостей і потенційних наслідків. Вибір методу оцінки ризиків залежить від конкретних потреб організації та рівня ризику, який вона готова прийняти. У зв'язку з цим організаціям важливо вибрати відповідний метод оцінки ризиків, який відповідає їхнім цілям і завданням.

2.2.1 Метод оцінки ризиків NIST 800-30

Метод оцінки ризиків NIST 800-30 - це комплексний метод до оцінки ризиків інформаційної безпеки, який широко використовується в галузі. Він забезпечує структурований та систематичний підхід до виявлення, оцінки і визначення пріоритетів ризиків інформаційної безпеки в організації.

Метод оцінки ризиків за стандартом NIST 800-30 складається з дев'яти етапів [14]. Ось більш детальне пояснення кожного кроку:

1. Характеристика системи. Першим кроком є ідентифікація системи та її меж. Це передбачає визначення функцій системи, активів, потоків даних та взаємозв'язків з іншими системами.

2. Ідентифікація загроз. Другий крок – визначення потенційних загроз для системи, розгляд різноманітних факторів, включаючи архітектуру системи, типи даних, які вона містить, і потенційні мотиви зловмисників.

3. Виявлення вразливостей. Третім кроком є виявлення вразливостей системи, тобто аналіз технічних та процедурних засобів контролю системи для виявлення слабких місць, які можуть бути використані зловмисниками.

4. Аналіз засобів контролю. Четвертий крок полягає в оцінці ефективності існуючих засобів контролю для зменшення виявлених ризиків. Будується оцінка адекватності існуючих засобів контролю та виявлення будь-яких прогалин, які необхідно усунути.

5. Визначення ймовірності. П'ятий крок – визначення ймовірності успішної реалізації атаки, аналіз загроз і вразливостей, виявлених на другому та третьому кроках, для оцінки ймовірності успішної реалізації атаки.

6. Аналіз наслідків. Шостий крок – оцінка потенційного впливу успішної атаки. Передбачається розгляд наслідків успішної атаки, таких як втрата даних, простій системи та фінансові втрати.

7. Визначення ризиків. Сьомий крок – визначення рівня ризику, пов'язаного з системою. Для цього необхідно об'єднати інформацію, отриману на попередніх етапах, щоб оцінити ймовірність успішної атаки та потенційні наслідки такої атаки.

8. Рекомендації з контролю. Восьмий крок – розробка та впровадження стратегій для зменшення виявлених ризиків, а також вибір відповідних засобів контролю для усунення виявлених вразливостей та зменшення ймовірності успішної атаки.

9. Документування результатів. Останнім кроком є документування результатів оцінки ризиків. Сюди входить документування результатів, висновків та рекомендацій оцінки, а також будь-яких рішень, прийнятих щодо впровадження стратегій зменшення ризиків.

На рисунку 2.1 показано алгоритм методики управління ризиками NIST 800-30.

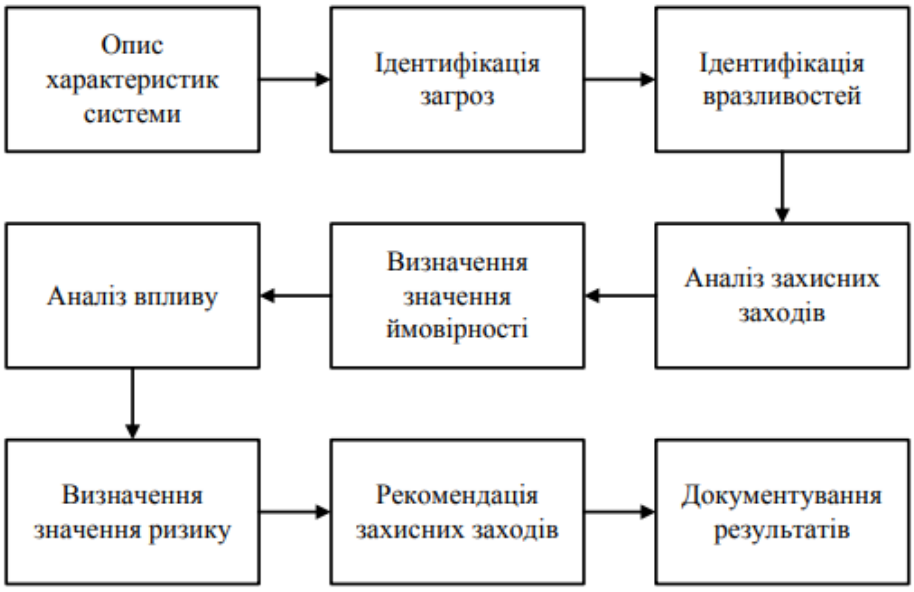

Рисунок 2.1 – Алгоритм методики управління ризиками NIST 800-30

У процесі аналізу ризику збирається інформація та ідентифікуються загрози, тобто визначаються джерела їх виникнення, причини та основні дії.

В рамках оцінки ризиків NIST 800-30 визначаються такі рівні ймовірності:

- високий «В»;
- середній «С»;
- низький «Н».

Аналіз впливу також обробляє події, пов'язані з втратою К, Ц і Д. Величина впливу визначається за шкалою:

- висока (В);

- середня (С);

- низька (Н).

Для визначення ризику використовується матриця РР: «В»; «С»; «Н».

Однією з ключових особливостей методу NIST 800-30 є його орієнтація на систему управління ризиками, яка підкреслює, що постійне управління ризиками є невід'ємною частиною загальної програми інформаційної безпеки організації.

Метод надає вказівки щодо того, як створити структуру управління ризиками та як використовувати цю структуру для виявлення, оцінки та управління ризиками для інформаційних систем.

На додаток до дев'ятикрокового процесу, описаного вище, метод NIST 800-30 також надає вказівки щодо інтеграції управління ризиками в загальну програму інформаційної безпеки організації. Сюди входять вказівки про те, як визначити ролі та обов'язки з управління ризиками, як розробити політику і процедури управління ризиками, а також як повідомити про результати управління ризиками ключовим зацікавленим сторонам.

Іншим важливим аспектом методу NIST 800-30 є його акцент на підході до інформаційної безпеки, заснованому на оцінці ризиків. Це означає, що організації повинні визначати пріоритети своїх зусиль з інформаційної безпеки на основі рівня ризику, пов'язаного з кожною системою або активом. Метод містить вказівки щодо того, як використовувати оцінки ризиків для визначення пріоритетів у сфері безпеки та як ефективно розподіляти ресурси для зменшення виявлених ризиків.

Загалом, метод оцінки ризиків NIST 800-30 є усталеним і широко використовуваним підходом до виявлення та управління ризиками для інформаційних систем. Його всеосяжні рамки та підхід, заснований на оцінці ризиків, роблять його цінним інструментом для організацій, які прагнуть створити надійну і ефективну програму інформаційної безпеки.

2.2.2 Метод оцінки ризиків FAIR

Метод оцінки ризиків FAIR (Factor Analysis of Information Risk – факторний аналіз інформаційних ризиків) – це система кількісної оцінки ризиків, яка покликана допомогти організаціям зрозуміти та проаналізувати ризики інформаційної безпеки у фінансовому вимірі. FAIR був розроблений некомерційною організацією Open Group і широко використовується фахівцями з інформаційної безпеки [50].

Метод оцінки ризиків FAIR складається з шести кроків [50]:

1. Визначення масштабу: визначення активів, загроз та зацікавлених сторін, які необхідно враховувати при оцінці ризиків.
2. Ідентифікація ризиків: визначення сценаріїв, в яких агент загрози може використати вразливість, щоб завдати шкоди активам.
3. Оцінка частоти та збитків: ймовірна частота та величина збитків, які можуть бути спричинені виявленими сценаріями ризиків.
4. Оцінка ризиків: оцінка ризиків за допомогою комбінації кількісних та якісних методів, а також визначення ризиків, які потребують подальшого аналізу та управління.
5. Управління ризиками: розробка та впровадження планів управління ризиками, які знижують ризик до прийнятного рівня.
6. Інформування про ризики: доведення результатів оцінки ризиків до відома зацікавлених сторін, а також забезпечення розуміння та дотримання політики, процедур управління ризиками організації.

Метод оцінки ризиків FAIR використовує низку різних методів та інструментів для кількісної оцінки ризиків, зокрема:

- сценарії ризику: описи подій, які можуть призвести до збитків, включаючи активи, які можуть постраждати, агенти загроз, які можуть використати вразливості, та потенційні наслідки;
- частота подій, що можуть призвести до збитків: ймовірність того, що подія, яка може призвести до збитків, відбудеться протягом певного періоду часу;

- величина збитків: розмір збитків, які можуть виникнути, якщо реалізується сценарій ризику;
- частота виникнення загрози: ймовірність того, що подія загрози відбудеться протягом певного періоду часу;
- вразливість: слабкість або прогалина в засобах контролю безпеки, якою може скористатися агент загрози;

Використовуючи комбінацію цих методів, метод оцінки ризиків FAIR надає організаціям всебічне розуміння ризиків інформаційної безпеки та дозволяє їм приймати обґрунтовані рішення про те, як управляти цими ризиками в економічно ефективний спосіб.

Метод оцінки ризиків FAIR набув популярності в останні роки завдяки своїй здатності надавати кількісну оцінку ризиків, що дозволяє організаціям більш ефективно визначати пріоритети своїх інвестицій і ресурсів у сфері безпеки. FAIR також відомий своїм акцентом на комунікації та співпраці, а також здатністю подолати розрив між технічними та бізнес особами, які приймають рішення.

Однією з ключових переваг методу оцінки ризиків FAIR є те, що він забезпечує спільну мову та структуру для обговорення та аналізу ризиків між різними відділами та зацікавленими сторонами в організації. Це може допомогти покращити комунікацію та співпрацю, а також гарантувати, що всі знаходяться на одній стороні, коли справа доходить до управління ризиками.

Ще однією перевагою методу оцінки ризиків FAIR є те, що його можна легко налаштувати та пристосувати до конкретних потреб різних організацій та галузей. Така гнучкість дозволяє організаціям адаптувати систему до власних унікальних вимог до управління ризиками, а також включати в процес власні інструменти та методології оцінки ризиків.

Однак у методу оцінки ризиків FAIR є й певні потенційні недоліки. Одним з основних критичних зауважень до системи є те, що вона може бути складною і важкою для впровадження, особливо для організацій, які не мають необхідного досвіду або ресурсів. Крім того, метод оцінки ризиків FAIR значною мірою покладається на точні дані та припущення, які може бути важко отримати на практиці.

2.2.3 Метод оцінки ризиків CRAMM

CRAMM (CCTA Risk Analysis and Management Method) – це методологія оцінки ризиків, розроблена UK Government's Central Computer and Telecommunications Agency (CCTA) у 1980-х роках. Метод допомагає організаціям оцінити ризики для своїх інформаційних систем та розробити відповідні заходи безпеки [51].

CRAMM – це комплексна методологія, яка охоплює всі аспекти оцінки ризиків, від ідентифікації активів до обробки та управління ризиками. В її основі лежить концепція аналізу ризиків, яка передбачає виявлення та аналіз ризиків, з якими стикається організація, а також вжиття заходів для їх зменшення або управління ними.

Метод оцінки ризиків CRAMM складається з трьох етапів:

1. Підготовка. На цьому етапі визначається обсяг оцінки, визначаються необхідні ресурси та формується команда з проведення оцінки. До складу команди можуть входити технічні експерти, бізнес-аналітики та фахівці з управління ризиками.

2. Аналіз ризиків. На другому етапі команда з проведення оцінки робить детальний аналіз інформаційних систем організації, включаючи апаратне та програмне забезпечення, дані та людей. Це передбачає виявлення та оцінку потенційних загроз, вразливостей та наслідків. Для збору інформації та оцінки ризиків команда може використовувати низку інструментів та методів, таких як інтерв'ю, опитування та технічні оцінки.

3. Управління ризиками. На третьому етапі команда з проведення оцінки розробляє та впроваджує плани управління ризиками. Це передбачає визначення пріоритетності ризиків на основі їхньої серйозності та ймовірності, а також розробку стратегій для їхнього пом'якшення або управління ними. Команда може також розробити політику, процедури та засоби контролю для запобігання або зменшення ймовірності виникнення ризиків у майбутньому.

Однією з ключових переваг CRAMM є комплексний підхід до оцінки ризиків. Визначаючи та аналізуючи всі аспекти інформаційних систем організації, включаючи

обладнання, програмне забезпечення, дані та людей, він надає повну картину ризиків, якими необхідно управляти. Це дозволяє організаціям розробляти ефективні стратегії управління ризиками, які враховують усі потенційні загрози.

Ще однією сильною стороною CRAMM є його фокус на управлінні ризиками. Замість того, щоб просто ідентифікувати ризики, він забезпечує основу для розробки та впровадження планів управління ризиками. Це гарантує, що організації можуть вжити конкретних заходів для пом'якшення або управління ризиками, з якими вони стикаються, а не просто документувати їх.

Одним із потенційних недоліків CRAMM є його складність. Оскільки це комплексна методологія, її впровадження може зайняти багато часу та ресурсів. Це може ускладнити її ефективне використання невеликими організаціями або організаціями з обмеженими ресурсами.

Ще одним потенційним недоліком є потреба в експертах-оцінювачах. Оскільки CRAMM передбачає детальний аналіз інформаційних систем організації, він потребує експертів зі спеціалізованими знаннями та досвідом. Це може бути проблемою для організацій, які не мають власних експертів або ресурсів для найму зовнішніх консультантів.

Загалом, CRAMM – це добре відпрацьована і широко використовувана методологія оцінки ризиків, яка може бути ефективною для організацій усіх розмірів і галузей. Її комплексний підхід і зосередженість на управлінні ризиками роблять її потужним інструментом для виявлення та управління ризиками для інформаційних систем. Однак складність і вимоги до ресурсів можуть зробити його більш придатним для більших і складніших організацій.

2.2.4 Метод оцінки ризиків Risk Watch

Risk Watch – це метод оцінки ризиків, який покликаний допомогти організаціям виявляти та управляти ризиками, пов'язаними з їхніми інформаційними системами [52]. Він був розроблений компанією Risk Watch та базується на найкращих галузевих практиках і стандартах, таких як ISO 27001 і NIST 800-30.

Метод Risk Watch складається з чотирьох етапів: планування і підготовка, збір даних, аналіз ризиків, звітність та подальші дії. На кожному етапі здійснюються конкретні заходи для забезпечення комплексного та систематичного підходу до оцінки ризиків.

Однією з ключових особливостей методу Risk Watch є використання системи оцінки ризиків, яка враховує ймовірність та вплив потенційних ризиків. Система бальної оцінки дозволяє організаціям визначати пріоритетність ризиків та розробляти відповідні стратегії управління ними.

На додаток до оцінки ризиків, Risk Watch також надає інструменти та послуги з управління ризиками, комплаєнс-менеджменту та управління інцидентами. Ці інструменти та послуги покликані допомогти організаціям впроваджувати ефективні програми управління ризиками та дотримуватися відповідних норм і стандартів.

Переваги методу Risk Watch:

- комплексний підхід: метод Risk Watch охоплює всі аспекти оцінки та управління ризиками, від планування та підготовки до звітності та подальших дій;
- кращі галузеві практики: Risk Watch базується на найкращих галузевих практиках та стандартах, таких як ISO 27001 і NIST 800-30, що означає, що він відповідає визнаним і широко використовуваним системам.;
- система оцінки ризиків: Risk Watch використовує систему оцінки ризиків, яка дозволяє організаціям визначати пріоритетність ризиків на основі їхньої ймовірності та впливу, що полегшує розробку відповідних стратегій управління ризиками.
- зручні інструменти: Risk Watch надає зручні інструменти та сервіси для оцінки та управління ризиками, що полегшує організаціям впровадження та підтримку ефективних програм управління ризиками.

Недоліками Risk Watch є:

- вартість: вартість впровадження та підтримки методу Risk Watch може бути високою для деяких організацій, особливо невеликих;

- складність: комплексний характер методу Risk Watch може зробити його занадто складним для деяких організацій, особливо тих, що мають обмежені ресурси і досвід в управлінні ризиками;
- значні витрати часу: Метод Risk Watch може бути трудомістким у впровадженні та підтримці, вимагаючи значних витрат часу і ресурсів;
- відсутність кастомізації: Метод Risk Watch може бути недостатньо адаптованим для деяких організацій, оскільки він є стандартизованим підходом, який може не відповідати унікальним потребам усіх організацій.

Загалом, метод Risk Watch – це комплексний та ефективний підхід до оцінки та управління ризиками, який може допомогти організаціям проактивно виявляти та усувати потенційні ризики для своїх інформаційних систем.

2.2.5 Метод оцінки ризиків COBRA

COBRA (Consultative, Objective and Bi-functional Risk Analysis – консультативний, об'єктивний і біфункціональний аналіз ризиків), складається з низки інструментів аналізу ризиків, консультацій та огляду безпеки [53]. Вони були розроблені в основному у зв'язку з визнанням мінливого характеру IT та безпеки, а також вимог, що висуваються бізнесом до цих сфер.

Першою такою підводною течією змін було зростаюче визнання того, що IT-безпека є питанням бізнесу. Очікувалося і очікується, що перевірка безпеки та рішення пов’язані з бізнесом, з економічно обґрунтованими рішеннями та рекомендаціями. Іншою проблемою, яка здебільшого виникала наприкінці 90-х років, є пошук багатьма організаціями кращої і більш помітної віддачі від своїх бюджетів на безпеку. Щоб досягти цього, багато організацій застосовують нові підходи до традиційних обмежень, пов'язаних з нестачею досвіду, часу та фінансів.

COBRA та її методологія за замовчуванням розвивалися дуже швидко, щоб вирішити ці проблеми належним чином.

Вона була розроблена у тісній співпраці з однією з найбільших світових фінансових установ та після багаторічних досліджень. Було визнано, що бізнес-

користувачі повинні бути залучені з самого початку. Це має низку переваг і формує весь огляд.

Крім того було запропоновано ряд інших радикальних змін. Результатом інструмент аналізу ризиків, який буде відповідати найсуворішим вимогам, повністю задовольняючи мінливі вимоги, що висуваються до команди безпеки або аудиту.

Процес оцінки ризиків за допомогою COBRA є надзвичайно гнучким. Підтримується значна кількість підходів. Однак, процес за замовчуванням зазвичай складається з трьох етапів [53]:

- створення опитувальника;
- вивчення ризиків;
- формування звіту.

На першому етапі, шляхом вибору або генерації модулів, створюється базова анкета відповідно до середовища та вимог користувача.

Другий етап – це процес опитування. Відповіді на запитання консультанта з ризиків надаються відповідним персоналом, а інформація надійно зберігається. На третьому етапі проводиться оцінка ризиків та виставляються "бали" за окремими категоріями ризику, надаються індивідуальні рекомендації та пропонуються рішення, а також пояснюються потенційні наслідки для бізнесу.

Кожен з цих етапів управляється відповідним компонентом системи: конструктор опитувальників, аналізатор ризиків та генератор звітів.

Однією з ключових переваг програмного забезпечення COBRA є те, що його можна налаштувати, а це означає, що організації можуть пристосувати інструмент до своїх конкретних потреб. Крім того, COBRA надає користувачам вичерпний звіт, в якому описуються виявлені ризики та рекомендовані способи їх усунення.

Однак одним з потенційних недоліків COBRA є те, що вона може не підходити для організацій зі складним ризиковим середовищем або з великою кількістю активів. Крім того, програмне забезпечення вимагає певного навчання для ефективного використання, що може бути бар'єром для деяких організацій.

2.2.6 Метод оцінки ризиків OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) – це методологія оцінки ризиків, розроблена Інститутом інженерії програмного забезпечення (SEI) Університету Карнегі-Меллона [54].

Метод OCTAVE покликаний допомогти організаціям ідентифікувати та управляти ризиками для критично важливих активів, таких як інтелектуальна власність, комерційна таємниця та дані клієнтів. Він особливо корисний для організацій, які працюють з конфіденційними даними, таких як фінансові установи, заклади охорони здоров'я та урядові установи.

OCTAVE включає три різні версії: OCTAVE Allegro, OCTAVE D* та OCTAVE-S.

OCTAVE Allegro – це спрощена версія методології OCTAVE, призначена для малих та середніх організацій. Вона зосереджена на виявленні та визначенні пріоритетності ризиків для критично важливих активів, а також на розробці стратегій зменшення ризиків. OCTAVE Allegro розроблений таким чином, щоб бути простим у використанні та швидко давати результати.

OCTAVE D* – це більш повна версія методології OCTAVE, призначена для великих організацій з більш складним інформаційно-технологічним середовищем. Вона включає більш детальну оцінку технічних та організаційних ризиків, а також забезпечує більш ретельний аналіз стратегій зменшення ризиків.

OCTAVE-S – це версія методології OCTAVE, спеціально розроблена для управління ризиками в ланцюгах поставок. Вона зосереджена на виявленні та управлінні ризиками для критично важливих активів ланцюга поставок, таких як продавці, постачальники та аутсорсингові послуги.

Методологія OCTAVE складається з трьох етапів:

1. Початковий етап передбачає визначення обсягу та цілей оцінки ризиків, відбір групи з оцінки та визначення активів, що підлягають оцінці.

2. Етап оцінки передбачає виявлення та визначення пріоритетності загроз, вразливостей та ризиків для критично важливих активів. Цей етап включає як

технічні, так і організаційні оцінки, такі як інтерв'ю з ключовим персоналом, аналіз документації та сканування вразливостей.

3. Етап зменшення ризиків передбачає розробку стратегій зменшення ризиків та впровадження засобів контролю для зниження виявлених ризиків до прийнятного рівня. Цей етап включає розробку політик, процедур і технічних засобів контролю, а також постійний моніторинг та оцінку ефективності засобів контролю.

Методологія OCTAVE має низку переваг, серед яких комплексний підхід до оцінки ризиків, зосередженість на критично важливих активах і здатність виявляти як технічні, так і організаційні ризики. Однак вона може бути трудомісткою та вимагати багато ресурсів, особливо для великих організацій.

Крім того, результати оцінки ризиків можуть бути складними і потребувати експертної інтерпретації.

OCTAVE – це гнучкий метод, який можна адаптувати до потреб різних організацій. Він забезпечує основу для систематичного виявлення та усунення ризиків інформаційної безпеки і може бути використаний як основа для розробки комплексної програми інформаційної безпеки.

2.3 Порівняльна характеристика визначених методів оцінки ризиків

Порівняльний аналіз методів оцінки ризиків проводився автором цієї роботи з урахуванням таких факторів:

- відповідність стандартам ISO 2700x;
- оцінка захищеності;
- швидкодія;
- облік послідовності контрзаходів при розрахунку ризиків;
- визначення рівня ризиків для різних моделей ІТС;
- можливість завдання власних контрзаходів;
- оцінка аналізу ризиків;
- наявність ліцензії;
- зручність інтерфейсу;

- необхідність спеціальної підготовки для роботи з засобами;

- складність визначення ризику;

- оперативність визначення ризику.

При порівняльному аналізі методів оцінки ризиків [55], були визначені найбільш поширені недоліки, до яких відносять:

1. Складність отримання даних.

2. Постійне оновлення програмного забезпечення.

3. Величезна витрата часу на аналіз, що може бути повільною реакцію на ризики.

Як згадувалось раніше, кількісні методи оцінки ризиків є неточними та ненадійними з декількох причин, зокрема процес збору даних є складним, а інформаційні системи можуть мінятися через постійне вдосконалення програмного та апаратного забезпечення. Варто також згадати, що витрати часу для аналізу є досить великими.

Нижче наведений порівняльний аналіз основних методів оцінки ризиків (таблиця 2.1).

Таблиця 2.1

Порівняльний аналіз FAIR, NIST 800-30, CRAMM, Risk Watch, COBRA, OCTAVE

Критерії порівняння	FAIR	NIST	CRAMM	Risk Watch	COBRA	OCTAVE
Відповідність стандартам ISO 2700x	+	+	+	+	+	+
Оцінка захищеності	+	+	+	+	+	+
Швидкодія	-	-	+	-	+	+
Облік послідовності контрзаходів при розрахунку ризиків	+	+	+	-	+	-

Продовження таблиці 2.1

Критерії порівняння	FAIR	NIST	CRAMM	Risk Watch	COBRA	OCTAVE
Визначення рівня ризиків для різних моделей ІТС	-	-	+	-	+	-
Можливість завдання власних контрзаходів	-	-	+	+	+	-
Оцінка аналізу ризиків	Кількісна	Змішана	Змішана	Кількісна	Якісна	Якісна
Наявність ліцензії	+	+	+	+	+	+
Зручність інтерфейсу	Зручний	Не зручний	Не зручний	Не зручний	Зручний	Зручний
Необхідність спеціальної підготовки для роботи з засобами	+	+	+	+	-	-
Складність визначення ризику	Складна	Не дуже складна	Складна	Складна	Не дуже складна	Не складна
Оперативність визначення ризику	-	-	+	-	+	+

Найпростішими та ефективними методиками оцінки ризиків, згідно з таблицею 2.1, можна вважати CRAMM та COBRA.

2.3.1 Переваги та недоліки кожного методу

Для подальшої побудови гібридного методу управління ризиками є необхідність також вказати основні переваги та недоліки кожного вище згаданого методу для вибірки найбільш простих та ефективних методик (таблиця 2.2).

Таблиця 2.2

Переваги та недоліки кожного методу оцінки ризиків

Метод оцінки	Переваги	Недоліки
FAIR	- Комплексний аналіз - Висока ефективність - Точний підхід - Акцент на комунікації та співпраці - Легке налаштування	- Для великих підприємств - Вимагає певний рівень технічних знань - Багато часу на впровадження - Орієнтованість лише на точні дані та припущення
NIST	- Детальний опис можливих ризиків інформаційних активів - Для підприємств різного розміру - Гнучкість - Галузевий стандарт	- Довготривалий процес аналізу - Деякі функції не автоматизовано - Всеосяжний характер методу може зробити його складним у впровадженні - Відсутність адаптованості та інтеграції з іншими методами

Продовження таблиці 2.2

Метод оцінки	Переваги	Недоліки
CRAMM	- Детальне визначення існуючих ризиків - Ефективність використання - Комплексний підхід - Фокус на управлінні ризиками	- Важкість у розумінні - Робота тільки з існуючими інформаційними активами - Вимагає значних ресурсів для впровадження - Потреба в експертах-оцінювачах
Risk Watch	- Простота впровадження та експлуатації - Комплексний підхід - Кращі галузеві практики - Зручність інструменту	- Аналіз ризиків лише на програмно-технічному рівні - Може не підходити для складних організацій - Вартість - Значні витрати часу на впровадження та підтримку - Складність - Відсутність кастомізації
COBRA	Загальна база знань про загрози та вразливості - Базовий рівень безпеки - Структурований підхід - Вичерпний звіт, в якому описуються виявлені ризики та рекомендовані способи їх усунення - Легко адаптувати до конкретних потреб	- Рівні ризиків не визначаються - Не підходить організаціям, які потребують більш комплексного підходу - Не підходить для організацій зі складним ризиковим середовищем або з великою кількістю активів - Потребує навчання персоналу для ефективного користування

Продовження таблиці 2.2

Метод оцінки	- Переваги	Недоліки
OCTAVE	- Комплексний підхід до оцінки ризиків - Зосередженість на критично важливих активах - Здатність виявляти як технічні, так і організаційні ризики	- Трудомісткий метод, особливо для великих організацій

Таким чином, вибір методу оцінки ризиків залежить від конкретних потреб, ресурсів та досвіду організації. Хоча кожен метод має свої переваги та недоліки, мета полягає в тому, щоб вибрати той, який найкраще відповідає потребам організації в управлінні ризиками.

Висновки за розділом 2

Отже, існує багато методів оцінки ризиків, які організації можуть використовувати для оцінки ризиків для своїх активів та вжиття відповідних заходів для їхнього зменшення. Якісні методи оцінки ризиків, такі як NIST 800-30, FAIR і CRAMM, покладаються на суб'єктивні судження для оцінки ризиків на основі таких критеріїв, як ймовірність, вплив та критичність. Кількісні методи оцінки ризиків, такі як Risk Watch та COBRA, використовують методи, засновані на даних, для аналізу ризиків на основі таких факторів, як ймовірність, частота і очікувані збитки.

Кожен метод оцінки ризиків має свої переваги та недоліки, і організації повинні вибрати метод, який найкраще відповідає їхнім потребам і ресурсам. Важливо також зазначити, що оцінка ризиків – це безперервний процес, який потребує постійного моніторингу та оновлення, щоб зберегти власну ефективність.

Загалом, добре спланована і проведена оцінка ризиків може допомогти організаціям приймати обґрунтовані рішення для зменшення ризиків та захисту своїх активів.

Кожен з розглянутих методів оцінки ризиків (NIST, FAIR, CRAMM, Risk Watch, COBRA та OCTAVE) має свої унікальні переваги та недоліки. Вибір методу буде залежати від конкретних потреб, ресурсів та досвіду організації.

Деякі методи, такі як NIST та CRAMM, є більш комплексними та структурованими, надають детальний аналіз ризиків та основу для управління ними. Однак це також може зробити їх складними та трудомісткими у впровадженні, тобто дані методи вимагають значних ресурсів.

Інші методи, такі як FAIR та Risk Watch, більше зосереджені на кількісному аналізі, забезпечуючи більш точний підхід до оцінки ризиків. Ці методи вимагають певного рівня технічних знань та можуть зайняти багато часу для впровадження.

Обираючи метод оцінки ризиків, організації повинні ретельно зважити свої потреби в управлінні ризиками та ресурси. Важливо також зазначити, що хоча ці методи забезпечують основу для оцінки та управління ризиками, вони не є універсальним рішенням. Є необхідність адаптувати підхід до управління ризиками до конкретних потреб кожної компанії, підтримувати постійну оцінку та коригувати процес управління ризиками за необхідності.

Проведений порівняльний аналіз слугує основою для побудови гібридного методу управління ризиками у розділі 3.

РОЗДІЛ 3
ГІБРИДНИЙ МЕТОД УПРАВЛІННЯ РИЗИКАМИ

Гібридний метод управління ризиками може поєднувати в собі два і більше підходів до управління ризиками в проекті або організації. Основними причинами створення гібридного методу управління ризиками є:

1. Підвищення ефективності. Поєднуючи кілька методів управління ризиками, гібридний підхід може забезпечити більш комплексне управління ризиками, яке краще відповідає конкретним потребам організації або проекту. Це може призвести до більш ефективного процесу управління ризиками та кращих результатів у зменшенні ризиків.

2. Гнучкість. Різні ризики можуть вимагати різних типів підходів до управління. Гібридний підхід забезпечує більшу гнучкість для адаптації процесу управління ризиками до конкретних ризиків та обставин конкретного проекту або організації.

3. Економічна ефективність. Гібридний підхід може бути більш економічно ефективним, ніж використання одного підходу, оскільки він може зменшити дублювання зусиль та ресурсів. Наприклад, деякі ризики можуть вимагати кількісного аналізу ризиків, тоді як для обробки інших достатньо лише якісної оцінки. Використовуючи гібридний підхід, ресурси можна ефективніше розподіляти на ризики, які потребують більш поглибленого аналізу.

4. Покращення інформування про ризики. Гібридний підхід може покращити інформування про ризики, надаючи різні точки зору на ризики та управління ними. Це може допомогти зацікавленим сторонам краще зрозуміти ризики та способи управління ними, що може призвести до прийняття більш обґрунтованих рішень.

5. Краща ідентифікація ризиків. Використовуючи комбінацію методів управління ризиками, гібридний підхід дозволить виявити ризики, які можуть бути пропущені при використанні одного підходу.

3.1 Учасники процесу управління

Учасниками процесу управління ризиками в рамках гібридного методу є:

1. Менеджер з інформаційної безпеки: відповідає за управління програмою інформаційної безпеки в організації. В його зону відповідальності входять виявлення та зменшення інформаційних ризиків, розробка політик та процедур, а також впровадження засобів контролю для захисту інформаційних активів.

2. IT-персонал: відіграє важливу роль у впровадженні та підтримці технічних засобів контролю, які захищають інформаційні активи, – управління брандмауерами, впровадження систем виявлення та запобігання вторгнення, а також управління контролем доступу користувачів.

3. Власники даних: відповідають за управління конкретними наборами даних в організації та забезпечення належного контролю для захисту конфіденційності, цілісності та доступності даних.

4. Відділи комплаєнсу та юридичний відділ: відповідають за дотриманням організацією чинних законів та нормативних актів, пов'язаних з інформаційною безпекою та конфіденційністю. Вони також можуть відповідати за виконання договірних вимог, пов'язаних з інформаційною безпекою.

5. Власники бізнесу/керівництво: власники бізнесу або керівництво відповідають за визначення загальної стратегії управління ризиками в організації. Основною функцією зазначених вище учасників процесу є виділення достатніх ресурсів на діяльність з управління інформаційними ризиками, а також за те, щоб політики та процедури управління інформаційними ризиками дотримувалися в усій організації.

6. Корпоративне управління ризиками: може бути задіяне у виявленні та зменшенні інформаційних ризиків, які можуть вплинути на організацію в цілому. Це може включати оцінку ризиків, пов'язаних з репутацією, дотриманням законодавства та фінансовими показниками.

7. Зовнішні консультанти: можуть залучатися для надання експертизи в конкретних сферах управління інформаційними ризиками, таких як кібербезпека,

комплаєнс або оцінка ризиків. Вони можуть надати цінну інформацію та рекомендації менеджеру з інформаційної безпеки та вищому керівництву, допомагаючи виявити потенційні ризики та розробити ефективні стратегії їх зниження.

8. Співробітники: працівники також є важливими учасниками процесу управління інформаційними ризиками. Вони несуть відповідальність за дотримання політик та процедур інформаційної безпеки, а також за повідомлення про потенційні інциденти безпеки, вразливості своїм керівникам або команді з інформаційної безпеки.

9. Сторонні постачальники: особливо, якщо вони мають доступ до інформаційних активів організації. Організація повинна забезпечити належну перевірку сторонніх постачальників та наявність у них належних засобів контролю безпеки для захисту інформаційних активів організації.

10. Підрозділи аудиту та управління ризиками: команди аудиту та управління ризиками відповідають за оцінку ефективності програми управління інформаційними ризиками організації. Вони можуть проводити оцінку ризиків, аудит та перевірку відповідності, щоб виявити прогалини в практиці управління інформаційними ризиками в організації та рекомендувати вдосконалення.

11. Група реагування на інциденти: команда реагування на інциденти відповідає за управління та реагування на інциденти безпеки, коли вони виникають. Це включає в себе розслідування інциденту, локалізацію наслідків і реалізацію заходів з виправлення ситуації, щоб запобігти виникненню подібних інцидентів у майбутньому.

Варто зазначити, що власниками інформаційних ризиків є спеціалісти інформаційної безпеки, на стратегічні або операційні цілі яких відбувається безпосередній вплив.

Ефективне управління інформаційними ризиками вимагає співпраці та координації між усіма зацікавленими сторонами, а також прагнення до постійного вдосконалення практик управління інформаційними ризиками. Конкретні ролі та обов'язки кожного учасника можуть відрізнятися залежно від структури організації,

галузі та профілю ризику, але всі учасники відіграють важливу роль у захисті конфіденційності, цілісності та доступності інформаційних активів.

3.2 Розділення ризиків за фактором впливу на процеси

За фактором впливу на процеси ризики можна розділити на три основні категорії [56]:

- стратегічні ризики: ризики, які потенційно можуть суттєво вплинути на здатність організації досягати своїх стратегічних цілей, часто пов'язані із зовнішніми факторами, такими як зміни на ринку, конкуренція або регулювання; прикладами стратегічних ризиків є вихід на новий ринок, розробка нового продукту, послуги або значні інвестиції в нову технологію;
- операційні ризики: ризики, які виникають у процесі повсякденної діяльності організації, часто пов'язані з внутрішніми процесами, системами та людьми; прикладами операційних ризиків є шахрайство, збої в роботі ІТ, перебої в ланцюжку поставок і помилки співробітників;
- фінансові ризики: ризики, які виникають унаслідок фінансової діяльності організації, часто пов'язані з волатильністю ринку, кредитним ризиком або ризиком ліквідності; прикладами фінансових ризиків є валютний ризик, ризик процентної ставки та кредитний ризик.

Важливо зазначити, що ці категорії ризиків не є взаємовиключними, і багато ризиків можуть належати до більш ніж однієї категорії. Наприклад, кібератака на ІТ-системи компанії може бути як операційним, так і фінансовим ризиком, залежно від характеру та серйозності атаки. Поділяючи ризики на ці категорії, організації можуть краще зрозуміти типи ризиків, з якими вони стикаються, і розробити відповідні стратегії управління ризиками для їх зменшення.

Операційними або іншими ризиками бізнес-сторона може нехтувати, якщо вони перешкоджають бізнес-цілям організації. В контексті даної роботи таке нехтування регулюється поняттям рівень толерантності компанії до ризиків.

Також для збереження часу спеціалістів та коштів з боку бізнесу є пропозиція нехтувати ризиками з меншим рівнем критичності для організації та очевидним рішенням.

Критичні ризики обов'язково реєструються як корпоративні, за допомогою процесу корпоративного ризик-менеджменту.

Від рівня толерантності та критичності залежить подальший аналіз ризиків в наступних етапах гібридного методу.

Структурований підхід до управління ризиками та налагоджена комунікація між учасниками даного процесу збільшать ефективність протидії та запобігання загрозам, а також зменшать витрати часу на обробку ризиків за фактором толерантності і критичності.

3.3 Схематичне представлення гібридного методу управління ризиками

Увесь процес обробки ризиків в першу чергу регулюється двома міжнародними стандартами: ISO 31000, який описує процес управління корпоративними ризиками, та ISO/IEC 27005, що стосується саме управління ризиками в інформаційній безпеці.

Ризики обробляються, охоплюючи бізнес-сторону та основні засади інформаційної безпеки.

Рисунок 3.1 відображає організаційний етап гібридного методу управління ризиками, що охоплює процес збору даних для їх подальшого аналізу. Подвійні лінії означають паралельність кроків або групування даних.

Ідентифікація активів організації покладена на метод оцінки ризиків OCTAVE, оскільки зосередженість саме на критично важливих активах є його перевагою над іншими методами оцінки ризиків (згідно з таблицею 2.2).

При проведенні оцінки ризиків за методологією OCTAVE активи ідентифікуються та класифікуються на основі наступних критеріїв [54]:

1. Матеріальні активи: фізичні предмети, які мають цінність для організації, такі як будівлі, обладнання та інвентар.

2. Нематеріальні активи: нефізичні об'єкти, які мають цінність для організації, такі як інтелектуальна власність, дані про клієнтів та бізнес-процеси.

3. Інформаційні активи: активи, які складаються з даних або інформації, що мають цінність для організації, наприклад, фінансові дані, списки клієнтів та комерційні таємниці.

4. Активи, що стосуються персоналу: включають знання, навички та досвід працівників, а також їхню здатність виконувати критичні функції в організації.

5. Активи інфраструктури: IT-системи, мережі або інші технологічні компоненти інфраструктури організації.

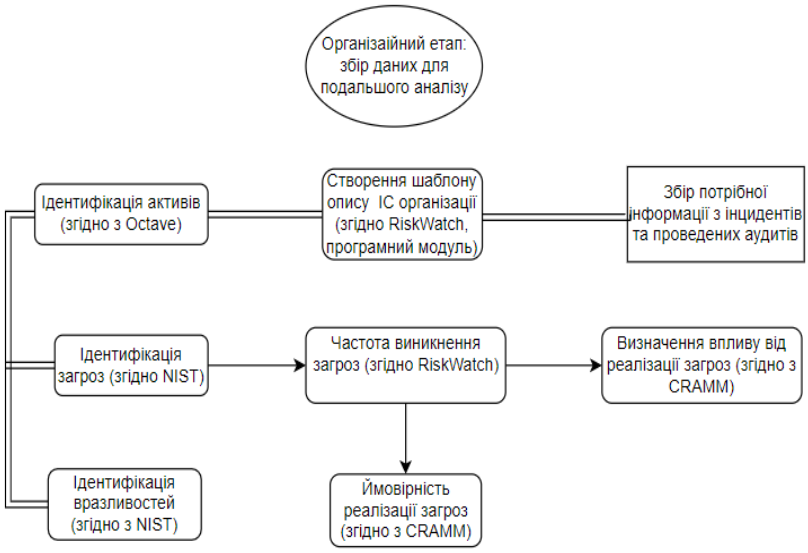

Рисунок 3.1 – Перший етап гібридного методу управління ризиками

Після ідентифікації та класифікації активів OCTAVE рекомендує організаціям оцінити критичність кожного активу, щоб визначити необхідний рівень захисту та управління ризиками. Це передбачає оцінку потенційного впливу втрати або компрометації кожного активу на місію, цілі та завдання організації. Завдяки алгоритму OCTAVE, організації можуть розробити більш ефективні стратегії управління ризиками та більш ефективно розставити пріоритети щодо своїх ресурсів.

Щодо ідентифікації загроз, NIST виділяє п'ять категорій, які організації повинні враховувати при розробці комплексної програми управління ризиками:

1. Природні ризики: стихійні лиха, такі як повені, землетруси, урагани та лісові пожежі. Вони можуть завдати фізичної шкоди об'єктам та порушити роботу.

2. Ризики людського фактору: спричинені людськими діями, такими як крадіжки, вандалізм чи саботаж. Вони також можуть включати ненавмисні дії, такі як помилки або нещасні випадки.

3. Екологічні: ці загрози спричинені екологічними факторами, такими як відключення електроенергії, розливи хімічних речовин або інші екологічні небезпеки.

4. Кіберзагрози: спричинені зловмисним або несанкціонованим доступом до комп'ютерних систем або мереж, включаючи віруси, хробаки та інші види шкідливого програмного забезпечення.

5. Ризики ланцюгу постачання: виникають через вразливості в ланцюгу постачання, включаючи компрометацію апаратних або програмних компонентів, або нездатність сторонніх постачальників надавати товари або послуги, як очікувалося.

Методологія NIST рекомендує організаціям враховувати всі п'ять категорій загроз при розробці своїх програм управління ризиками. Це включає визначення потенційного впливу кожного типу загроз на діяльність, репутацію та фінансову стабільність організації.

Ідентифікація вразливостей також відбувається згідно з методом NIST 800-30, оскільки ця методологія універсальна та комплексна і підходить для організацій будь-якого розміру.

Використовується шаблон опису інформаційних систем організації згідно з методом Risk Watch, що включає пункти, наведені нижче:

a. Назва інформаційної системи.

b. Власник інформаційної системи.

c. Призначення інформаційної системи.

d. Опис інформаційної системи.

e. Масштаб інформаційної системи (сфера застосування інформаційної системи, включаючи будь-які зовнішні системи, які взаємодіють з нею).

Впровадження даного кроку на організаційному етапі гібридного методу дозволить структурувати дані про інформаційні системи, що в свою чергу зменшить витрати часу при подальшій обробці ризиків конкретної ІС.

Згідно з методом Risk Watch, задається частота виникнення кожної з виділених загроз, ступінь уразливості та цінність ресурсів (активів), на підставі чого розраховується ефективність впровадження засобів захисту інформації. За аналогією з ПЗ COBRA в методі Risk Watch (для спрощення введення та обробки даних) множини запитів тематичного опитувальника ініціюються за допомогою вибору даних з набору варіантів, наприклад, конкретні числові значення (0, 1 – «ніколи», 2, 3 – «рідко», 4, 5, 6 – «іноді»; 7, 8 – «звичайно»; 9, 10 – «завжди») або «ні», «не знаю».

Метод CRAMM оцінює ймовірність реалізації загрози за шкалою від 1 до 5, де 1 означає найнижчу ймовірність, а 5 – найвищу. Рейтинг ймовірності визначається шляхом оцінки низки факторів, таких як ймовірність виникнення, простота використання, вплив на бізнес та наявність контрзаходів.

За методом CRAMM вплив загрози зазвичай оцінюється з точки зору потенційних наслідків або шкоди, які можуть виникнути, якщо загроза буде реалізована. Це може включати як матеріальні, так і нематеріальні наслідки, такі як фінансові збитки, шкода репутації або юридичні та регуляторні санкції.

Для визначення впливу загрози в методі CRAMM, як правило, враховується ряд факторів, включаючи критичність активу або системи, що знаходяться під загрозою, потенційні наслідки інциденту і вплив на бізнес-операції. Оцінка впливу зазвичай проводиться за шкалою від 1 до 5, де 1 означає найнижчий вплив, а 5 – найвищий.

Пріоритетним кроком в алгоритмі є збір даних з інцидентів та результатів аудитів, оскільки ця інформація відображає поточний стан організації в цілому.

На другому етапі гібридного методу управління ризиками відбувається аналіз ризиків, який враховує дані, що були зібрані попередньо (рис. 3.2).

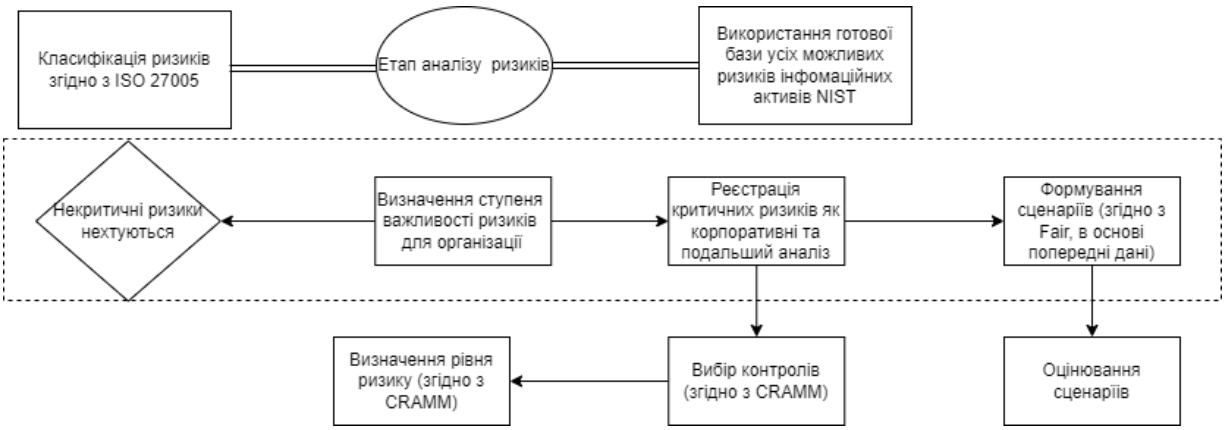

Рисунок 3.2 – Другий етап гібридного методу управління ризиками

Для збереження часу спеціалістів та коштів з боку бізнесу автор цієї роботи пропонує не обробляти ризики з меншим рівнем критичності для організації та очевидним рішенням.

Деякі ризики можуть нехтуватися через низький рівень толерантності компанії до них, основна причина – досягнення бізнес-цілей, що є пріоритетом.

Обробка ризику з високим ступенем важливості полягає в поєднанні якісних та кількісних методів оцінки ризиків, а також вимагає реєстрації в базі корпоративних ризиків, оскільки критичний інформаційний ризик має вплив на безперервність бізнесу та роботу інформаційних систем.

У стандарті ISO 27005 класифікація ризиків є ключовою частиною процесу оцінки ризиків і передбачає розподіл ризиків за категоріями на основі їхнього потенційного впливу та ймовірності.

Стандарт ISO 27005 визначає чотири рівні ризику на основі поєднання ймовірності та впливу:

1. Дуже низький ризик: малоймовірні або мають незначний вплив на організацію.
2. Низький ризик: можливі, але малоймовірні або мають незначний вплив на організацію.
3. Середній рівень ризику: можуть відбутися або мають значний вплив на організацію.

4. Високий ризик: напевно відбудуться або мають серйозний вплив на організацію.

Класифікація рівнів ризику є суб'єктивною та може відрізнятися в різних організаціях залежно від багатьох факторів, наприклад від рівня толерантності до нього. Проте, ISO 27005 забезпечує основу, яку організації можуть використовувати для послідовної та ефективної класифікації своїх ризиків.

Саме ця класифікація використовується в алгоритмі управління ризиками, а також перегукується з готовим переліком усіх можливих ризиків інформаційних активів NIST. Процес обробки можна полегшити, беручи до уваги можливі ризики згідно з NIST та надаючи йому певного рівня ризику на базі ISO 27005 під час аналізу на другому етапі гібридного методу управління ризиками.

Сценарії ризиків у методі FAIR передбачають розробку наративу або історії, яка описує, як конкретна подія загрози може вплинути на інформаційні активи організації. Опис зазвичай включає таку інформацію, як причина події, характер події, потенційний вплив і ймовірність настання події.

Сценарії забезпечують структурований спосіб аналізу та оцінки потенційних ризиків для активів організації. Розробляючи сценарії, які ілюструють, як загроза може проявитися та вплинути на активи, фахівці з управління ризиками можуть краще зрозуміти ймовірність та потенційний вплив ризику.

Крім того, використовуючи кількісний підхід для оцінки ймовірної частоти і величини ризику, сценарії ризиків FAIR дозволяють організаціям приймати обґрунтовані рішення щодо управління ризиками. Це допомагає організаціям визначати пріоритетність своїх ресурсів і зосереджуватися на найбільш значущих ризиках для своїх активів, що в кінцевому підсумку знижує загальну схильність до ризиків.

В свою чергу, сценарії ризику оцінюються шляхом визначення ймовірної частоти та ймовірного розміру збитків або впливу. Це робиться шляхом присвоєння значень різним факторам, які впливають на сценарій ризику, таким як частота загрозливих подій, вразливість і потенційний розмір збитків.

Частота загрозливих подій вираховується на основі історичних даних, експертних оцінок або іншої відповідної інформації. Вразливість визначається шляхом аналізу засобів контролю безпеки, що застосовуються для запобігання або пом'якшення наслідків загрозливих подій. Потенційний розмір збитків оцінюється з урахуванням залучених активів, потенційного впливу на організацію та будь-яких зовнішніх факторів, які можуть погіршити ситуацію.

Якісна оцінка ризиків в представленому методі управління ризиками покладається на метод CRAMM, оскільки він простий для реалізації цієї мети, а також містить комплексний підхід до усього процесу управління.

Метод CRAMM також відповідає за вибір контролів, оскільки містить усі необхідні етапи для ефективного зменшення ризиків:

1. Ідентифікація існуючих засобів контролю: перегляд існуючих засобів контролю, які вже впроваджені в організації, щоб визначити, чи є вони достатніми для зменшення виявлених ризиків;

2. Нові засоби контролю: якщо в існуючих засобах контролю є прогалини, необхідно визначити нові засоби контролю для усунення виявлених ризиків. Це можуть бути технічні, адміністративні або фізичні засоби контролю.

3. Ефективність засобів контролю: ефективність визначених засобів контролю необхідно оцінити, щоб визначити, чи є вони достатніми для пом'якшення виявлених ризиків. Це передбачає оцінку економічної ефективності засобів контролю та визначення того, чи відповідають вони вимогам безпеки організації.

4. Вибір засобів контролю: після оцінки ефективності визначених засобів контролю слід обрати засоби контролю, які найбільше підходять з точки зору зменшення виявлених ризиків. Вибрані засоби контролю повинні бути здійсненними, економічно ефективними та прийнятними для організації.

5. Впровадження засобів контролю: після того, як відповідні засоби контролю визначені, їх слід впровадити в організації. Даний етап відповідає за те, щоб засоби контролю були інтегровані в політику та процедури організації, а також проведення необхідного навчання для працівників.

6. Моніторинг та аналіз засобів контролю: ефективність впроваджених засобів контролю слід регулярно відстежувати та переглядати, щоб переконатися, що вони продовжують забезпечувати необхідний захист інформаційних активів організації. У разі виявлення будь-яких слабких місць слід вжити відповідних заходів для їх усунення.

Рисунок 3.3 ілюструє фінальний етап гібридного методу управління ризиками, що включає в себе результати аналізу, звіти та процеси зменшення ймовірності та наслідків ризиків.

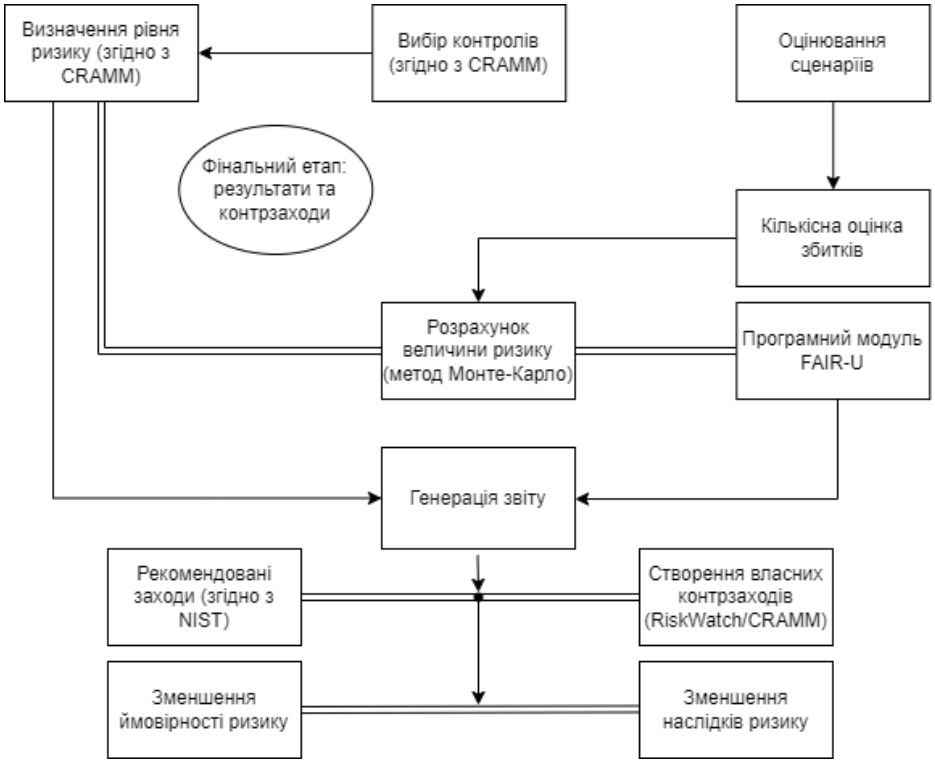

Рисунок 3.3 – Третій етап гібридного методу управління ризиками

Оскільки процес управління має вплив на бізнес та цілі організації, важливим кроком перед формуванням результатів є кількісна оцінка збитків. Організація зможе правильно розподілити ресурси та зосередити свою увагу на більш критичних ризиках.

Моделювання за методом Монте-Карло дозволяє врахувати невизначеність та мінливість результатів проекту при оцінці очікуваної вартості. Це дає більш реалістичну й точну картину ризиків або потенційних прибутків, пов'язаних з

проектом, що може допомогти в прийнятті рішень в процесі управління ризиками [46].

Також ефективним етапом кількісної оцінки ризиків є програмний модуль FAIR-U, оскільки метод FAIR легкий в налаштуванні, а також використовує метод Монте-Карло для моделювання впливу різних сценаріїв ризику та оцінки ймовірності різних результатів. Модуль також включає ряд інструментів і шаблонів для моделювання ризиків, аналізу даних та створення звітів. Результати якісної та кількісної оцінки формують звіт (або відбувається генерація програмним модулем FAIR-U).

Метод NIST надає комплексний набір рекомендованих заходів безпеки, які організації повинні впроваджувати для захисту своєї інформації та інформаційних систем. Ці заходи викладені у Спеціальній публікації NIST 800-53 "Контроль безпеки та конфіденційності для федеральних інформаційних систем та організацій", яка містить каталог засобів контролю безпеки та конфіденційності разом з відповідними інструкціями щодо їх впровадження [57]. Згаданий вище набір заходів стане у нагоді для першого впровадження контролів та є прикладом стандартизованого підходу.

Оскільки потреби та ресурси у кожної організації унікальні, важлива можливість створення власних контрзаходів в рамках процесу. На вибір пропонується зручний, заснований на кращих галузевих практиках, метод Risk Watch, або більш економічно вигідний CRAMM.

Існує кілька підходів до зменшення ймовірності та наслідків ризиків. Один із поширених підходів полягає у впровадженні засобів контролю на основі результатів оцінки ризиків. Контролі можуть бути превентивними, детективними або коригуючими за своєю природою [58].

Превентивний контроль має на меті зменшити ймовірність настання ризику шляхом усунення або зменшення першопричини. Наприклад, впровадження контролю доступу для запобігання несанкціонованому доступу до конфіденційних даних.

Детективні засоби контролю спрямовані на виявлення ризику або його наслідків після того, як він стався. Наприклад, впровадження систем виявлення

вторгнень для оповіщення команд безпеки про будь-які спроби або успішні спроби несанкціонованого доступу.

Коригувальні засоби контролю спрямовані на обмеження впливу ризику, який вже стався. Наприклад, впровадження процедур резервного копіювання та відновлення даних після збою системи або витоку даних.

Інші заходи, які можна вжити для зменшення ймовірності та наслідків ризиків, включають програми навчання та підвищення обізнаності персоналу, регулярну оцінку системи та вразливостей, а також плани реагування на інциденти.

Важливо постійно переглядати та оновлювати процес управління ризиками, щоб гарантувати, що засоби контролю залишаються ефективними, а нові ризики виявляються та усуваються.

3.4 Якісна оцінка ризиків згідно з CRAMM в гібридному методі управління ризиками

Якісна оцінка ризиків є важливою частиною процесу CRAMM, оскільки вона допомагає виявити та оцінити потенційні ризики для інформаційної безпеки [59]. Оцінка рівнів ризику CRAMM має певний алгоритм, приклад якого наведений нижче. Область оцінки: IT-відділ невеликої компанії, що займається розробкою програмного забезпечення.

Крок 1: Визначення активів та ресурсів.

1) IT-інфраструктура (сервери, бази даних, мережеві пристрої тощо).
2) Конфіденційні дані компанії та її клієнтів.
3) Персонал з доступом до IT-інфраструктури.

Крок 2: Визначення загроз:

А) Атаки шкідливих програм.

Б) Фішингові атаки.

В) Інсайдерські загрози.

Г) Перебої в електропостачанні.

Д) Стихійні лиха.

Крок 3: Виявлення вразливостей:

i. Застаріле програмне та апаратне забезпечення.

ii. Слабка політика паролів.

iii. Відсутність контролю доступу.

iv. Відсутність навчання працівників найкращим практикам кібербезпеки.

Крок 4: Оцінка впливу та ймовірності кожного ризику (таблиця 3.1).

Таблиця 3.1

Якісна оцінка ризиків

Ризик	**Оцінка впливу**	**Ймовірність**
Атаки шкідливих програм	Високий	Середня
Фішингові атаки	Середній	Висока
Внутрішні загрози	Високий	Середня
Перебої в електропостачанні	Високий	Низька
Стихійні лиха	Високий	Низька

Крок 5: Визначення пріоритетності ризиків.

На основі оцінок впливу та ймовірності ризики можна класифікувати за пріоритетністю наступним чином:

1. Атаки шкідливих програм.
2. Внутрішні загрози.
3. Стихійні лиха.
4. Фішингові атаки.
5. Перебої в електропостачанні.

Крок 6: Визначення заходів для зменшення ризиків.

Основні заходи:

- встановлення та підтримка актуального антивірусного програмного забезпечення для захисту від атак шкідливих програм.

- впровадження контролю доступу, щоб запобігти несанкціонованому доступу до конфіденційних даних;
- регулярне навчання співробітників найкращим практикам кібербезпеки, щоб зменшити ймовірність внутрішніх загроз;
- резервні копії важливих даних та їхнє збереження в безпечному місці за межами офісу, щоб підготуватися до стихійних лих;
- встановлення та підтримка резервного генератора, щоб підготуватися до перебоїв в електропостачанні.

Крок 7: Впровадження та контроль визначених заходів.

Контроль включає в себе оцінку ефективності даних заходів. Є потреба також в регулярному перегляді та оновленні оцінки ризиків, щоб переконатися в актуальності та ефективності в рамках зменшенні ризиків.

Фактична оцінка ризиків на практиці може містити додаткові кроки або інші методи залежно від особливостей організації.

3.5 Кількісна оцінка ризиків згідно з моделюванням Монте-Карло в гібридному методі управління ризиками

Метод Монте-Карло базується на генерації випадкових значень та великій кількості симуляцій для оцінки ймовірності виникнення ризику та його величини [60]. Для прикладу візьмемо оцінку ризику кібератак на мережу компанії.

Крок 1: Визначення змінних.

1. Кількість спроб вторгнення на мережу за день.
2. Час реакції на вторгнення.
3. Ймовірність того, що вторгнення успішне.
4. Збитки, які можуть виникнути внаслідок кібератаки.

Крок 2: Визначення розподілу ймовірностей для кожної змінної.

Наприклад, кількість спроб вторгнення може мати розподіл Пуассона, час реакції може бути рівномірним розподілом, ймовірність успішного вторгнення може бути біноміальним розподілом, а збитки можуть мати нормальний розподіл.

Крок 3 Монте-Карло симуляція.

За допомогою програмного забезпечення, що реалізує метод Монте-Карло, можна згенерувати випадкові значення для кожної змінної. Наприклад, 10 000 випадкових значень для кожної змінної.

Крок 4: Обчислення ризику.

Для кожного з 10 000 випадкових наборів змінних, можна обчислити ризик шляхом використання формули:

$$Р=Ів*Зв,$$

де Р – ризик;

Ів - ймовірність вторгнення;

Зв - збитки від вторгнення.

Для кожного випадкового набору змінних можна розрахувати ризик та взяти середнє значення ризику з усіх 10 000 випадкових наборів змінних, щоб отримати оцінку загального ризику.

Крок 5: Аналіз результатів

Залежно від отриманого результату, керівництво компанії може приймати рішення щодо підвищення рівня безпеки мережі, наприклад, збільшення кількості захисних заходів або вдосконалення наявних.

Таким чином, метод Монте-Карло може допомогти оцінити ризик у сфері інформаційної безпеки та дозволяє керівництву компанії приймати обґрунтовані рішення щодо поліпшення безпеки мережі.

Однак, результати Монте-Карло симуляції можуть бути залежні від якості визначення змінних та розподілу їх ймовірностей, тому важливо враховувати ці обмеження при використанні цього методу.

3.6 Ефективність гібридного методу

Оскільки запропонований гібридний метод є суто теоретичним, тобто сформованим на базі найкращих галузевих практик, кількісна оцінка його ефективності викликає певні труднощі і виходить за рамки цієї роботи.

Проте, існує алгоритм для узагальнення роботи в рамках необхідних для ефективного функціонування компонентів процесу управління ризиками [55, 61]:

- детальне вивчення гібридного методу: аналіз розробленого методу, щоб переконатися в чіткому розумінні його ключових компонентів, припущень та цілей;
- визначення критеріїв оцінки: є необхідність у визначенні або створенні власних критеріїв, за якими можливо оцінити метод, модель; критерії повинні ґрунтуватися на цілях, які потрібно оцінити, та можуть включати такі фактори, як здатність ідентифікувати або пріоритезувати ризики, масштабованість та ефективність у зменшенні ризиків;
- аналіз зібраних даних за вибраною темою: пошук закономірностей, тенденцій та іншої інформації, яка допоможе зрозуміти, наскільки добре працює розроблений метод;
- порівняння з існуючими методиками: для визначення, як запропонований гібридний метод управління ризиками співвідноситься з іншими моделями;
- коригування методу: на основі результатів аналізу є потреба в коригуванні методу для підвищення його ефективності.

На даному етапі роботи автор методу пропонує такі критерії оцінки ефективності:

1. Відповідність найкращим галузевим практикам.
2. Відповідність міжнародним стандартам.
3. Основа побудови методу.
4. Визначення власника ризиків та відповідальних осіб за процес.
5. Налагодженість комунікації між учасниками процесу.
6. Ідентифікація загроз.
7. Ідентифікація вразливостей.

8. Ідентифікація активів.
9. Якісна оцінка ризиків.
10. Кількісна оцінка ризиків.
11. Обробка результатів.
12. Робота та впровадження контролів.
13. Формування звітів.
14. Зменшення ризиків та пом’якшення їхніх наслідків.
15. Витрати часу на обробку ризиків.
16. Вартість рішення.
17. Зосередженість на критичних ризиках.
18. Структурованість підходу.
19. Можливість автоматизації процесу.
20. Адаптивність методу.
21. Комплексність.
22. Легкість в налаштуванні.
23. Потреба в навчанні персоналу.

Щоб оцінити ефективність гібридного методу управління ризиками, була сформована таблиця з зазначеними критеріями (ДОДАТОК Б).

Враховуючи усі критерії, що вибрані для оцінки ефективності методу, можна вважати, що гібридний метод управління ризиками є ефективним та неперервним процесом, який легко адаптується під потреби організації та є гнучким до вдосконалення.

Важливо зазначити, що хоча оцінка ефективності запропонованого теоретичного методу є не простою задачею і виходить за рамки цієї роботи, проте автор методу ставить за мету його тестування у своїх подальших дослідженнях.

Висновки за розділом 3

Гібридний метод управління ризиками поєднує в собі відомі алгоритми та стратегії для забезпечення комплексного підходу до управління ризиками. Цей підхід

використовує сильні сторони кожного окремого методу, мінімізуючи при цьому їхні недоліки. Використання запропонованого гібридного методу може бути ефективним в управлінні складними ризиками, де одного підходу може бути недостатньо.

У третьому розділі основні засади побудови запропонованого гібридного методу управління ризиками, описано проведення якісної оцінки ризиків згідно з CRAMM та обчислення величини ризику за методом Монте-Карло.

Ідентифікація активів реалізується за допомогою методу OCTAVE.

Запропонований гібридний метод охоплює усі основні етапи управління ризиками та є ефективним з точки зору швидкодії, що забезпечується використанням програмних модулів FAIR-U та нехтуванням ризиками з низькою толерантністю і важливістю.

Однією з переваг використання запропонованого гібридного підходу є те, що він може забезпечити більш цілісний погляд на ризики, дозволяючи організаціям краще зрозуміти потенційний вплив різних ризиків на їхню діяльність. Це, в свою чергу, може допомогти організаціям розробити більш ефективні стратегії пом'якшення та управління ризиками, адаптовані до їхніх конкретних потреб.

Ще однією перевагою запропонованого гібридного методу, автор вважає його гнучкість. Залежно від характеру і складності ризиків, різні методи можна комбінувати і пристосовувати до конкретних потреб. Це означає, що організації можуть адаптувати свої стратегії управління ризиками до конкретної ситуації, а не покладатися на універсальний підхід.

Однак впровадження гібридного підходу вимагає ретельного планування та координації. Організації повинні мати чітке розуміння визначених методів і того, як їх можна ефективно поєднувати. Крім того, важливо мати надійну систему управління ризиками, яка включає в себе чіткі політики, процедури та інструкції з управління ризиками.

ВИСНОВКИ

У дипломній роботі досліджено процес управління ризиками, проведений аналіз доступних джерел у сфері інформаційної безпеки для збору інформації та формування класифікації ризиків.

Досліджено взаємозв'язок інформаційної безпеки та бізнесу, порівняно інформаційні ризики та бізнес-ризики.

Проведено аналіз методів оцінки ризиків для подальшої побудови ефективного алгоритму.

Запропоновано гібридний метод управління ризиками за рахунок комбінації методів оцінки ризиків на основі переваг та недоліків кожного із них та проведена якісна оцінка ефективності представленого методу управління ризиками.

Описані основні засади запропонованого алгоритму та наведені його переваги і недоліки.

Запропонований гібридний метод може охоплювати усі основні етапи управління ризиками та вважається ефективним з точки зору швидкодії, що забезпечується з використанням програмних модулів та нехтуванням ризиків з низькою толерантністю та важливістю.

Перевагами використання гібридного підходу є те, що він може забезпечити більш цілісний погляд на ризики, дозволяючи організаціям краще зрозуміти потенційний вплив різних ризиків на їхню діяльність, а також гнучкість, тобто залежно від характеру та складності ризиків, різні методи можна комбінувати та пристосовувати до конкретних потреб. Організації можуть адаптувати свої стратегії управління ризиками до конкретної ситуації, а не покладатися на універсальний підхід.

Практична цінність поданої роботи полягає в розробці гібридного методу управління ризиками та оцінки його ефективності задля зменшення та пом'якшення ризиків та їх наслідків.

Мету дипломної роботи, а саме розробка гібридного методу управління ризиками, досягнуто, поставлені задачі виконані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 213 с.

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

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

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

5. Talabis, M., Martin, J., & Kennedy, D. (2014). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection;and Data Analysis. Syngress.

6. Andress, J., & Winterfeld, S. (2013). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress.

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

8. Harkins, M. (2014). Managing Risk and Information Security: Protect to Enable. Auerbach Publications.

9. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/54534.html.

10. Офіційний текст Загального регламенту щодо захисту даних (GDPR). – Регламент (ЄС) 2016/679, 2016 р. – Опубліковано в Офіційному журналі Європейського Союзу L 119, 4.5.2016. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

11. Лю, Міньяо. "Key challenges to effective information security risk management practices". International Journal of Business and Management, 2013; 8(24): 1-10.

12. ISO. ISO/IEC 27005:2018 Техніка безпеки інформації. Управління ризиками інформаційної безпеки. – [Чинний від 2018-03-15]. – К.: Держспоживстандарт України, 2018. – 44 с. – Режим доступу: https://www.iso.org/standard/75281.html.

13. National Institute of Standards and Technology. (2018). NIST Cybersecurity Framework: A Risk Management Approach to Cybersecurity. U.S. Department of Commerce.

14. National Institute of Standards and Technology (NIST). Guide for Conducting Risk Assessments. Special Publication 800-30 Rev. 1 [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

15. ISACA. COBIT 2019 Framework: Introduction and Methodology. [Електронний ресурс]. – Режим доступу: https://www.isaca.org/resources/cobit/cobit-2019-introduction-and-methodology.

16. Болеславська І.О. Вимоги стандарту PCI DSS щодо захисту платіжних карток в інтернет-торгівлі. Наукові записки Університету "КРОК". Серія: Юридичні науки. 2018; 2(50): 84-89.

17. ITIL. Service Strategy. [Електронний ресурс]. – Режим доступу: https://www.axelos.com/store/book/itil-service-strategy-pdf.

18. FINRA. Кібербезпека [Електронний ресурс] – Режим доступу: https://www.finra.org/rules-guidance/key-topics/cybersecurity.

19. CIS (Center for Internet Security). (2021). CIS Controls and CIS Benchmarks. [Електронний ресурс] – Режим доступу: https://www.cisecurity.org/controls/.

20. Закон України "Про захист інформації" [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2297-17.

21. Положення про порядок класифікації інформації як конфіденційної [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2332-18.

22. Положення про захист інформації в органах державної влади, органах місцевого самоврядування та підприємствах, установах та організаціях, що належать до сфери управління Міністерства цифрової трансформації України. Наказ Міністерства цифрової трансформації України від 24.04.2020 № 454. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0597-20#Text.

23. Закон України "Про кібербезпеку" [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19.

24. Закон України "Про електронні комунікації" [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1280-19.

25. Положення про безпеку інформаційних та телекомунікаційних систем банків [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/control/uk/publish/article?art_id=34293629&cat_id=34293623.

26. Інструкції щодо процедури виявлення підозрілих операцій [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/control/uk/publish/article?art_id=34293629&cat_id=34293623.

27. Закон України "Про електронні довірчі послуги". Відомості Верховної Ради України, 2015, № 31, ст. 270. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-19#Text.

28. Абрахамс, Д., & Бабіоне, М. (2017). Вимірювання інвестицій в кібербезпеку: підхід до управління ризиками [Електронний ресурс]. – Режим доступу: https://hbr.org/2017/02/measuring-cybersecurity-investments-a-risk-management-approach.

29. Хьюлер, А., & Шмід, М. (2020). Повернення інвестицій у сфері кібербезпеки (ROSI): вплив пріоритезації метрик безпеки. IEEE Transactions on Information Forensics and Security, 15, 3505-3518.

30. ISO/IEC 31000:2018. Risk management – Guidelines. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/65694.html.

31. ISACA. (2019). Enterprise Risk Management: Aligning Risk with Strategy and Performance. ISACA. [Електронний ресурс] – Режим доступу:

https://www.isaca.org/Portals/0/Images/Enterprise-Risk-Management-Aligning-Risk-with-Strategy-and-Performance_tcm1300-413578.pdf.

32. BSI. BS ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/54536.html.

33. Пінкертон К. Л., Олівер Д. С. Управління ризиками: Концепції та рекомендації. 5-те вид. Бінгемтон: Universal-Publishers, 2020. 467 с.

34. National Institute of Standards and Technology (NIST). (2021). Risk Management Framework (RMF). [Електронний ресурс] – Режим доступу: https://www.nist.gov/system/files/documents/2019/04/22/rmf-overview.pdf.

35. US Department of Homeland Security. (2021). Управління ризиками ланцюга постачання. [Електронний ресурс] – Режим доступу: https://www.cisa.gov/supply-chain-risk-management.

36. Wholey, J. S., Hatry, H. P., та Newcomer, K. E. (2010). Handbook of practical program evaluation. (с. 689-721). John Wiley & Sons.

37. Kokemuller, N. (2021). SWOT Analysis Definition and Examples. [Електронний ресурс] – Режим доступу: https://www.thebalancesmb.com/swot-analysis-2947964.

38. Kiritsis, D., & Gao, J. (2016). Failure mode and effects analysis (FMEA): A bibliometric review. International Journal of Production Research, 54(12), 3657-3676.

39. NSSF Uganda. (2019). Risk Echo Issue 5 [Електронний ресурс] – Режим доступу:https://issuu.com/nssfuganda/docs/nssf_risk_echo_issue_5/s/16468108.

40. KPMG. (n.d.). Control and risk self-assessment. [Електронний ресурс] – Режим доступу: https://home.kpmg/cn/en/home/services/advisory/risk-consulting/internal-audit-risk/control-and-risk-self-assessment.html.

41. Abeysinghe, G. (2012). Hazard and operability study (HAZOP): A guide for engineers and process operators. CRC press.

42. O'Connell, T., & Cuthbertson, R. (2013). The matrix risk methodology: Identifying and managing business risk in the 21st century. John Wiley & Sons.

43. Yang, Y., & Zhao, Y. (2017). Fault tree analysis for risk assessment of spacecraft systems. In Proceedings of the 30th Chinese Control and Decision Conference (CCDC) (pp. 4660-4664). IEEE.

44. Liu, P. (2017). Quantitative Information Security Risk Assessment Based on Attack Trees and Loss Distribution Approach. Journal of Information Security, 8(2), 150-159. [Електронний ресурс] – Режим доступу: https://doi.org/10.4236/jis.2017.82012.

45. Liu, B., Liu, W., Wei, W., Li, Z., & Hu, H. (2020). A quantitative risk analysis model for coal mine accidents using Bayesian network and fuzzy logic. Safety Science, 130, 104874. [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.ssci.2020.104874.

46. Liu, L. and Liao, H. (2019). Probabilistic safety assessment of critical infrastructure based on Monte Carlo simulation. International Journal of Critical Infrastructure Protection, 25, 10-20.

47. Kohli, A., & Grover, V. (2008). Business impact analysis in risk management: An exploratory study of best practices. Journal of applied security research, 3(1-2), 97-126.

48. Zhu, Y., Wang, R., & Chen, Y. (2020). Quantitative cyber risk assessment model for industrial control system. Reliability Engineering & System Safety, 193, 106702. [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.ress.2019.106702.

49. Jensen, F. V. (2001). Bayesian networks and decision graphs. Springer Science & Business Media.

50. FAIR Institute. Factor Analysis of Information Risk (FAIR) – The FAIR Standard. [Електронний ресурс]. – Режим доступу: https://www.fairinstitute.org/what-is-fair.

51. ResearchGate. (2022). CRAMM (CCTA Risk Analysis and Management Method) - A Framework for Managing Information System Risks [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/319215870_CRAMM_CCTA_Risk_Analysis_and_Management_Method__A_Framework_for_Managing_Information_System_Risks.

52. The RiskWatch Advantage - Risk Assessment Software". RiskWatch International. [Електронний ресурс] – Режим доступу: https://www.riskwatch.com/risk-assessment-software/.

53. COBRA: Introduction to Security Risk Analysis. Available on [Електронний ресурс]. – Режим доступу: http://www.security-risk-analysis.com/.

54. Методологія OCTAVE для оцінки інформаційних ризиків [Електронний ресурс]. – Режим доступу: http://www.risk24.ru/octave.htm.

55. Бучик С. С. Методика оцінювання інформаційних ризиків в автоматизованій системі / Наукоємні технології № 3 (35), 2017 224 © Бучик С. С., Шалаєв В. О., 2017 С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. — Житомир: ЖВІ ДУТ, 2015. — Вип. 11. — С. 33–43.

56. Olson, D.L., & Wu, D.D. (2010). Enterprise risk management (ERM) and decision making. Journal of Information Systems and Technology Management, 7(1), 1-16.

57. Special Publication 800-53, Revision 5. (2020). Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology (NIST). [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

58. Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security (6th ed.). Boston, MA: Cengage Learning.

59. Мейджор, М. (1995). A Practical Guide to the CRAMM Methodology. McGraw-Hill Book Company.

60. Кравченко, О. М., Трощинський, І. В., & Іванов, О. В. (2022). Застосування методу Монте-Карло для оцінки ризиків в інформаційній безпеці. Наукові записки Тернопільського національного технічного університету імені Івана Пулюя. Серія: Інформаційні технології та комп’ютерна інженерія, 1(88), 45-52.

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

62. Чунарьова А. В. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп’ютеризованих системах / А. В. Чунарьова, І. І. Пархоменко, І. І. Сащук // Вісник Інженерної академії України. — Х. — 2014. — Вип. 2. — С. 138–142.

63. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2014. — Вип. 8 (124).— ISSN 1681–7710. — С. 128–134.

64. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2015. — Вип. 3 (128). — ISSN 1681-7710. — С. 75–79.

65. Державний центр кібербезпеки України (ДЦКБ) [Електронний ресурс]. – Режим доступу: https://scc.gov.ua/.

66. Національний місяць кібербезпеки [Електронний ресурс]. – Режим доступу: https://safeonweb.ua/national-cybersecurity-awareness-month-2020/.

67. Кіберспостереження [Електронний ресурс]. – Режим доступу: https://cyberobserver.com.ua/.

68. Клішевич, О. В. Методи оцінки безпеки інформаційних систем / О. В. Клішевич, В. А. Корчинський. – К.: НДУ ім. О. М. Бекетова, 2018. – 250 с.

69. Мушкет, І. Методи оцінки ризиків кібернападів на інформаційні системи банків / І. М. Мушкет, О. В. Гончаренко, С. О. Ківшар // Електронні технології та системи комп'ютерного моделювання. – 2017. – Т. 47, № 1. – С. 132-140.

70. Петренко, А. В. Методи оцінки ефективності заходів із захисту інформації в інформаційних системах / А. В. Петренко, Ю. В. Столяренко, М. С. Яцко. – К.: IMEI, 2016. – 114 с.

71. Ткаченко, В. А. Методи оцінки надійності криптографічних захистів / В. А. Ткаченко, М. С. Лунц. // Проблеми теорії та методології боротьби зі злочинністю. – 2018. – Т. 40, № 2. – С. 135-142.

72. Методологія аналізу та управління ризиками в інформаційній безпеці: Науково-методичний посібник / За ред. О. М. Саєнка. – К.: НДІЗІТ, 2012. – 244 с.

73. Ахмедов С. Р., Бойко А. В. Анализ методов оценки рисков информационной безопасности компьютерных систем // Международный научный журнал. – 2016. – № 1 (46). – С. 83-86.

74. Трапезников В. Ю. Методы и модели оценки информационной безопасности корпоративных информационных систем // Безопасность бизнеса. – 2015. – № 3. – С. 70-77.

75. Бондаренко А. В., Волошинов С. В., Макарова Л. Н. Оценка эффективности методов защиты информации в компьютерных системах // Молодой ученый. – 2018. – № 9 (189). – С. 137-140.

76. Кікоть О. М. Методи інтелектуального аналізу даних в системах оцінювання ризиків безпеки інформації // Системи обробки інформації. – 2018. – № 9. – С. 67-70.

77. Петров А. М., Рогозин О. В., Хамидулін Р. А. Аналіз методів інформаційної безпеки в електронному урядуванні // Наукові праці ДонНТУ. Серія "Інформатика, кібернетика та обчислювальна техніка". – 2017. – Вип. 1 (32). – С. 107-114.

78. COSO Enterprise Risk Management - Integrating with Strategy and Performance: Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management: Integrating with Strategy and Performance. Hoboken, NJ: John Wiley & Sons.

79. COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). [Електронний ресурс]. – Режим доступу: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

80. ISO 22301:2019 Societal security — Business continuity management systems — Requirements: Державний комітет з питань технічного регулювання та споживчої політики України. (2019). Міжнародний стандарт ISO 22301:2019 “Суспільна безпека. Системи управління континуїтетом бізнесу. Вимоги” [ISO 22301:2019 Societal security — Business continuity management systems — Requirements]. Київ: Інтернорма.

81. National Institute of Standards and Technology (NIST). Guide for Conducting Risk Assessments. Special Publication 800-30 Rev. 1 [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

82. ENISA. Guidelines for SMEs on the security of personal data processing. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/at_download/fullReport.

83. The Open Group Risk Management Standard (O-ORM). [Електронний ресурс]. – Режим доступу: https://publications.opengroup.org/o-orm.

84. SANS Institute. Top 20 Critical Security Controls. [Електронний ресурс]. – Режим доступу: https://www.sans.org/critical-security-controls.

85. ITU-T. X.1051 (02/2018). Overview of risk management framework for information and communication technology (ICT) systems. [Електронний ресурс]. – Режим доступу: https://www.itu.int/rec/T-REC-X.1051-201802-I.

86. Cigital. Software Security Touchpoints, Version 2.0 [Електронний ресурс] – Режим доступу: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/software-security-touchpoints/software-security-touchpoints.pdf.

87. ENISA. Guidelines for SMEs on the security of personal data processing [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

88. Risk Management Society (RIMS). The RIMS Risk Maturity Model [Електронний ресурс]. – Режим доступу: https://www.rims.org/risk-management/rmm/Pages/default.aspx.

89. Наконечний В.С., Андрейчук О.В. Шляхи підвищення ефективності процесу забезпечення інформаційної безпеки за рахунок комбінації існуючих методів оцінки ризиків / V Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”- 28 ЖОВТНЯ 2022, КИЇВ, Україна–С.102-103.

90. Наконечний В.С., Андрейчук О.В. Удосконалення процесу забезпечення інформаційної безпеки за рахунок комбінації методів її оцінки / VI Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”- 27 КВІТНЯ 2023, КИЇВ, Україна–С. 83-86.

ДОДАТОК А

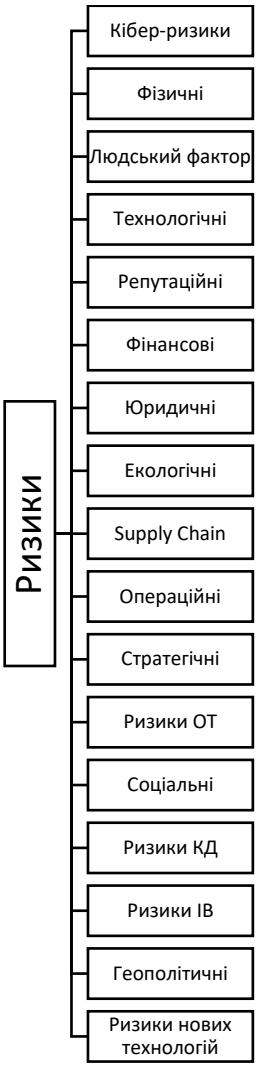

Рисунок 1.1 – Класифікація ризиків в ІБ

ДОДАТОК Б

Відповідність критеріям для оцінки ефективності гібридного методу

Критерій	Відповідність
Відповідність найкращим галузевим практикам	Гібридний метод відповідає найкращим галузевим практикам, а також деякі з них використовує у процесі.
Відповідність міжнародним стандартам	Обробка ризиків регулюється двома міжнародними стандартами: ISO 31000, який описує процес управління корпоративними ризиками, та ISO/IEC 27005, що стосується саме управління ризиками в інформаційній безпеці.
Основа побудови методу	Гібридний метод заснований на перевагах та недоліках методів оцінки ризиків.
Визначення власника ризиків та відповідальних осіб за процес	Власник ризиків – спеціаліст ІБ. Учасники процесу визначені.
Налагодженість комунікації між учасниками процесу	Три сторони, ІБ, бізнес та корпоративний ризик-менеджмент, успішно беруть участь у процесі управління ризиками та приймають спільні рішення.
Ідентифікація загроз	Даний етап дотриманий згідно з методом.
Ідентифікація вразливостей	Даний етап дотриманий згідно з методом.

Продовження таблиці 3.2

Критерій	Відповідність
Ідентифікація активів	Даний етап дотриманий згідно з методом.
Якісна оцінка ризиків	Ризики оцінюються якісно (CRAMM).
Кількісна оцінка ризиків	Ризики оцінюються кількісно (FAIR-U, Монте-Карло).
Обробка результатів	Зібрані дані та аналіз формують результати обробки ризиків.
Робота та впровадження контролів	Вибір та впровадження контролів регулюються методом CRAMM.
Формування звітів	Програмний модуль + робота спеціалістів.
Зменшення ризиків та пом’якшення їхніх наслідків	Дані кроки впроваджені в гібридний метод.
Витрати часу на обробку ризиків	За рахунок відбір ризиків за рівнем толерантності компанії та критичності деяка частка при обробці нехтується, а також певні програмні компоненти за рахунок автоматизації зменшують витрати часу.
Вартість рішення	Відносно недороге рішення за рахунок можливості вибору певних кроків в алгоритмі.
Зосередженість на критичних ризиках	Метод повністю орієнтований на обробку критичних ризиків.
Структурованість підходу	Підхід структурований.

Продовження таблиці 3.2

Критерій	Відповідність
Можливість автоматизації процесу	Частково автоматизований та є можливість удосконалити певні кроки.
Адаптивність методу	Повністю адаптивний.
Комплексність	Комплексно підходить до процесу управління ризиками, розглядаючи усі важливі етапи.