МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію Завідувач кафедри УІКБ доктор економічних наук, доцент _____ С.В. Легомінова «___»_____20__ р.	До захисту Завідувач кафедри УІКБ доктор економічних наук, доцент _____ С.В. Легомінова «___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

ДОСЛІДЖЕННЯ ПРОЦЕСУ УПРАВЛІННЯ І МЕТОДИК ОЦІНКИ РИЗИКІВ У ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ

СТУДЕНТ: Запорожченко Михайло Михайлович _____

(підпис)

КЕРІВНИК: к.в.н., доцент Якименко Юрій Михайлович _____

(підпис)

НОРМКОНТРОЛЕР: _____ _____

(підпис)

Київ – 2021

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Освітньо-кваліфікаційний рівень - магістр
Галузь знань - «12 Інформаційні технології»
Спеціальність -«125 Кібербезпека»
Спеціалізація - «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
д.е.н.,доцент_____ С.В.Легомінова
(підпис)
"___"_____ 2021 р.

ЗАВДАННЯ
на магістерську атестаційну роботу

Студенту **Запорожченку Михайлу Михайловичу**

1.**Тема роботи** " **Дослідження процесу управління і методик оцінки ризиків у сфері захисту інформації в організації** ", затверджена наказом по університету від "13" жовтня 2020 р. №.230
2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020р.
3. **Вихідні дані до роботи**:
- дослідити вимоги міжнародних та вітчизняних стандарти в галузі ризик-менеджменту,
- проаналізувати методологічні засади оцінки ризиків інформаційної безпеки організації,
- провести дослідження процесів управління і методик оцінки ризиків в організації,
- розробити рекомендації щодо вдосконалення процесів управління і методик оцінки ризиків в організації (для вибраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки).
1. Аналіз основ управління ризиками на методологічному рівні.
2. Аналіз процесу управління ризиками у сфері захисту інформації і їх оцінки в організації.
3. Дослідження процесів управління і методик оцінки ризиків в організації.

5. **Перелік обов'язкових демонстраційних креслень**:
1. Схема управління інформаційними ризиками в організації.
2. Схема алгоритму дій керівництва щодо прийняття рішення в умовах невизначеності ризиків.
3. Таблиця порівнянь існуючих ризиків та можливих інформаційних ризиків в організації.
4. Рекомендації щодо вдосконалення процесів управління і методик оцінки ризиків у сфері захисту інформації в організації (для вибраного прикладу).
6. Презентація доповіді, виконана в Microsoft PowerPoint.

6. **Термін виконання дипломної роботи**:
подання закінченої роботи керівнику 22 грудня 2020 року.

подання роботи на рецензію 23 грудня 2020 року.

7. **Дата видачі завдання** 26.10.2020 року.

Календарний графік

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури.	29.10.2020 р.	
2.	Аналіз та систематизація матеріалу. Вступ	5.11.2020 р.	
3.	Аналіз основ управління ризиками на методологічному рівні.	13.11.2020 р.	
4.	Аналіз процесу управління ризиками у сфері захисту інформації і їх оцінки в організації.	1.12.2020 р.	
5.	Дослідження процесів управління і методик оцінки ризиків в організації.	15.12.2020 р.	
6.	Оформлення та друк пояснювальної записки	25.12.2020 р.	
7.	Отримання відгука та рецензії на роботу	29.12.2020 р.	
8.	Оформлення презентацій	4.01.2021 р.	
10.	Попередній захист на кафедрі	8.01.2021 р.	
11.	Захист в ДЕК	___01.2021 р.	

Керівник _____ Якименко Юрій Михайлович
(підпис) (прізвище, ім'я, по-батькові)

Завдання прийняв для виконання _____ Запорожченко Михайло Михайлович
(підпис) (прізвище, ім'я, по-батькові)

РЕФЕРАТ

Магістерська дипломна робота присвячена дослідженню процесу управління й методик оцінки ризиків в галузі захисту інформації. Робота складається зі вступу, трьох розділів, що містять 18 рисунків, 11 таблиць та 18 формул, висновків та списку використаних джерел, що складає 36 найменувань. Загальний обсяг роботи становить 100 сторінок, серед яких 5 аркушів займає перелік умовних позначень та список використаних джерел.

Об'єктом дослідження є управління і оцінка ризиків інформаційної безпеки організації.

Предметом дослідження є дослідження процесу управління і методик оцінки інформаційних ризиків.

Метою роботи є оцінка ризиків інформаційної безпеки організації, виявлення найбільш критичних з них і визначення способів зменшення їх ступеня. Для цього в роботі використовуються положення міжнародних стандартів та загальновизнані підходи до оцінки ризиків інформаційної безпеки.

Як результат, у роботі проаналізовано підходи та методики оцінки ризиків інформаційної безпеки, досліджено варіації процесу управління ризиками згідно зі стандартами в галузі ризик-менеджменту, проведено оцінку наявних і потенційних ризиків організації, знайдено її сильні сторони та вразливості за допомогою SWOT-аналізу, розроблено план реагування на ризики та надано перелік рекомендацій щодо вдосконалення процесів управління і методик оцінки ризиків у сфері захисту інформації.

Сфера застосування. Матеріали роботи можуть бути використані в процесі створення нової чи аналізі вже існуючої інформаційної системи організації.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНИЙ РИЗИК, РИЗИК-МЕНЕДЖМЕНТ, ОЦІНКА РИЗИКУ, АНАЛІЗ РИЗИКУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СУІБ	Система управління інформаційною безпекою
ІБ	Інформаційна безпека
ОПР	Особа, що приймає рішення
ІС	Інформаційна система
БД	База даних
ПЗ	Програмне забезпечення
ОС	Операційна система
НСД	Несанкціонований доступ
УРІБ	Управління ризиками інформаційної безпеки

ВСТУП

Актуальність дослідження. Функціонування організацій з різних галузей діяльності майже завжди супроводжується ризиком, котрий несе за собою певні наслідки. В умовах зростаючої конкуренції та внаслідок збільшення різноманітних загроз та вразливостей інформаційної безпеки управління ризиками стало важливою складовою будь-якої бізнес-стратегії, оскільки при правильному використанні даний процес надає можливості уникнути несприятливих наслідків, як матеріальних, так і нематеріальних. Проблема полягає в тому, що велика кількість організацій впроваджує управління ризиками як самостійний процес, який функціонує окремо від бізнес-процесів організації. Як наслідок, через неможливість інтегрувати ризик-менеджмент в загальну діяльність організації і недостатність інформації в ризик-менеджерів щодо діяльності інших підрозділів, керівництвом організації приймаються необґрунтовані та недоцільні рішення. Процес управління ризиками описано у міжнародних, національних та вітчизняних стандартах, а також в методиках аналізу й управління ризиками від урядових організацій та приватних компаній.

Ступінь наукової розробки. Питання управління і оцінки ризиків розглядали Атапіна Н.В., Петрова А.В, Рєпін М.М., Файзулаєв Д.Ф., Морозов Б.Б. та інші. У зв’язку з оновленням стандартів в галузі ризик-менеджменту у 2017-2019 рр. деякі змінені аспекти в них не були розглянуті.

Практичне значення одержаних результатів. Застосування матеріалів роботи надасть можливість полегшити розуміння процесу управління ризиками інформаційної безпеки, а також обрати доцільну методику їх оцінки.

Розділ 1 АНАЛІЗ ОСНОВ УПРАВЛІННЯ РИЗИКАМИ НА МЕТОДОЛОГІЧНОМУ РІВНІ

Перед початком дослідження теми роботи необхідно ознайомитися з основними визначеннями в галузі ризик-менеджменту, вимогами стандартів до процесу управління ризиками, а також розглянути методи та критерії, використання яких буде доцільним під час прийняття рішення щодо обробки ризиків.

1.1 Міжнародні та вітчизняні стандарти в галузі ризик-менеджменту

Кожна організація ставить перед собою певні цілі та прагне досягти їх. Однак не можна з впевненістю сказати, що вона зможе отримати очікувані результати, і не можна стверджувати, що зміни у внутрішніх і зовнішніх факторах будуть проходити таким чином, як планувалося. Адже неможливо з абсолютною точністю передбачити, яку саме комбінацію зі всіх можливих станів внутрішнього середовища організації та навколишнього середовища буде реалізовано.

Враховувати та керувати такими факторами для подальшого прийняття рішення дозволяє ризик-менеджмент. У зв’язку з розвитком цього напрямку виникла потреба в систематизації уявлення про сам ризик та процес керування ним. Правила та підходи до управління ризиками були зібрані в стандартах ризик-менеджменту. В широкому сенсі слова стандарт – це модель чи еталон, який приймається за зразок для зіставлення з ним інших подібних об’єктів.

Активна стандартизація в галузі ризик-менеджменту почалась на початку 90-х років XX століття [1]. Серед найбільш відомих міжнародних стандартів виділяють наступні:

- ISO 31000:2018 “Risk management – Guidelines”;

- ISO/IEC 27005:2018 “Information Technology – Security Techniques – Information Security Risk Management”;
- FERMA (Federation of European Risk Management Associations);
- COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission).

Далі розглянемо кожний з них більш детально.

ISO 31000:2018 “Risk management – Guidelines” є одним із трьох стандартів серії ISO 31000. Даний документ був розроблений Технічним комітетом ISO/TC 262 “Risk Management” і вперше опублікований у 2009 році. Він призначений для осіб, які створюють і захищають вартість в організації шляхом управління ризиками, прийняття рішень, постановки і досягнення цілей, а також підвищення продуктивності.

З точки зору структури стандарт розділений на три ключові блоки: принципи, структуру (фреймворк) і процес управління ризиками (рис. 1.1) [2,3]. У порівнянні з першою версією стандарту структура залишається незмінною.

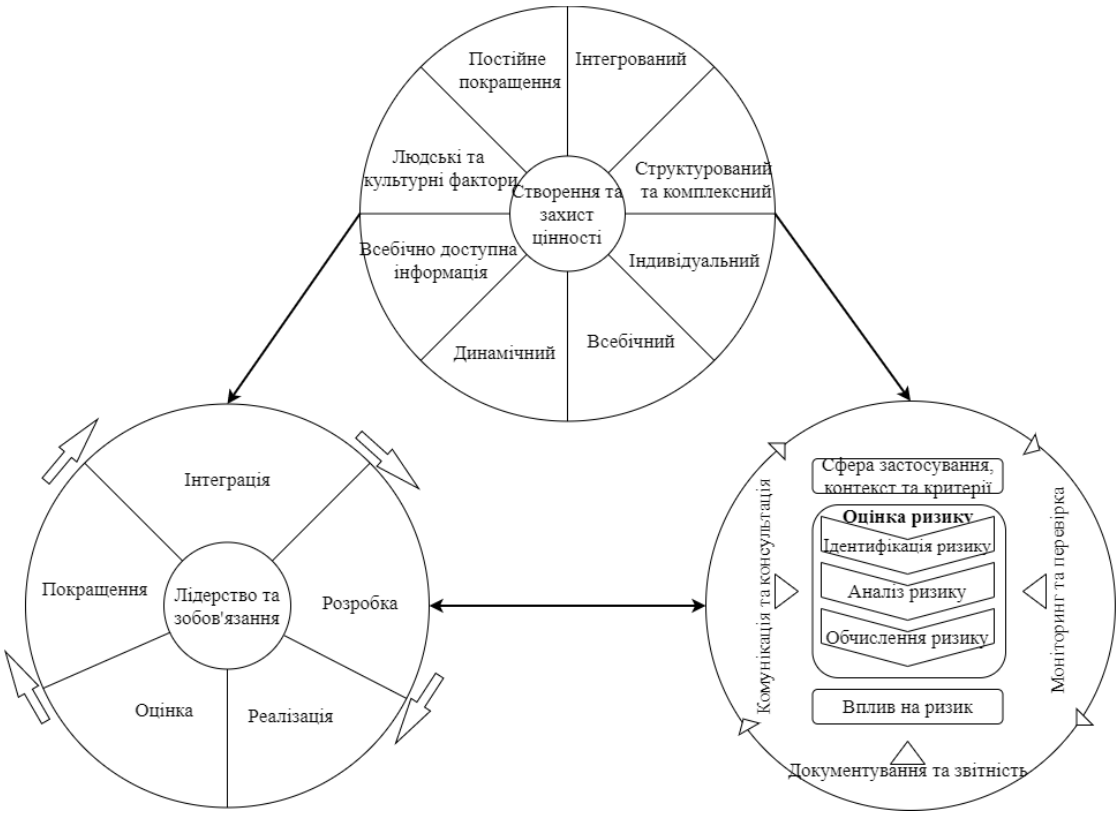

Рис. 1.1. Взаємозв’язок між принципами, структурою і процесом управління ризиками

З точки зору охоплення, згідно зі стандартом, управління ризиками може бути застосовано до будь-якого типу ризиків і організацій, і це каже про те, що даний документ не є вузькоспеціалізованим або галузевим. Стандарт може використовуватись як для окремого процесу, так і для всієї організації в цілому, тобто в нього закладено максимальне можливе охоплення.

Принципи управління ризиками, описані у стандарті, визначають характеристики ефективного та результативного ризик-менеджменту, пояснюючи його призначення, ціль та цінність. Згідно з документом ціллю ризик-менеджменту є створення і захист вартості.

В першій версії стандарту 2009 року було описано 11 принципів. В актуальній версії їх перелік зменшився внаслідок поєднання деяких з них і наразі можна побачити 8 принципів управління ризиками (рис. 1.2) [2,3]. На цих принципах повинен базуватися ризик-менеджмент та вони повинні бути враховані при подальшому створенні структури та процесів ризик-менеджменту організації. За допомогою цих принципів організація зможе керувати впливом невизначеності на її цілі.

Рис. 1.2. Принципи ризик-менеджменту відповідно до ISO 31000

Структура (фреймворк) ризик-менеджменту складається з декількох важливих компонентів (рис. 1.3) [2,3]. Цей блок відповідає на питання “що повинно

змінитися в організації для того, щоб вона змогла враховувати ризики в процесі прийняття рішень у всіх сферах її діяльності?”.

В стандарті стверджується, що ефективність ризик-менеджменту буде залежати від його інтеграції в систему управління та всі види діяльності організації, включаючи процес прийняття рішень. Це означає, що якщо рішення в організації приймаються без системного врахування ризиків, а ризик-менеджмент існує як окремий самостійний процес, то такий процес управління ризиками є неефективним і його необхідно змінювати.

Рис. 1.3. Структура ризик-менеджменту відповідно до ISO 31000

В минулій версії стандарту інтеграція була поверхнево оглянута в принципах управління, в той час як в актуальній версії вона розглянута дуже детально. Можна сказати, що ключовий посил нової версії стандарту – це інтеграція ризик-менеджменту в основні процеси організації та прийняття рішень. Ризик-менеджмент повинен бути невід’ємною частиною цілей організації, корпоративного управління, лідерства та відповідальності, стратегії, задач і діяльності організації та не повинен відокремлюватися від них. Управління ризиками повинно бути задіяне у всіх випадках, коли бізнесу необхідно приймати важливі рішення.

Процес ризик-менеджменту – це певний алгоритм дій, який повинен бути застосований в межах будь-якого бізнес-процесу організації (рис. 1.4) [2,3]. Він передбачає застосування політик, процедур і практик для забезпечення обміну інформацією і консультування, визначення контексту, а також оцінки ризиків, впливу на ризики, моніторингу, аналізу і документування ризиків, ведення звітності по ризикам.

В організації процес управління ризиками може мати множину варіацій, адаптованих під певні цілі, а також внутрішній і зовнішній контекст. Слід також пам’ятати, що процес управління ризиками є ітеративним.

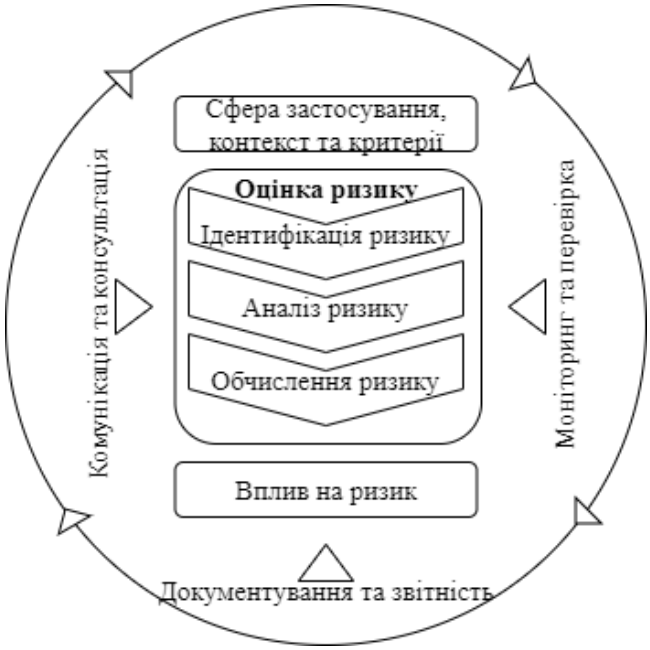

Рис. 1.4. Процес ризик-менеджменту

Основні зміни відносно першого видання включають наступні:

- були переглянуті принципи ризик-менеджменту;
- була підкреслена важливість інтеграції ризик-менеджменту в основні процеси і прийняття рішень;
- була виділена лідерська роль вищого керівництва;
- зроблено акцент на тому, що процес ризик-менеджменту є ітеративним, а не послідовним;
- упорядковано зміст документу з метою досягнення більшою універсальності для застосування стандарту до різноманітних вимог і ситуацій [3].

ISO/TR 31004:2013 “Guidance for the implementation of ISO 31000” [4] – другий стандарт серії ISO 31000, який сприяє ефективному впровадженню ISO 31000 та забезпечує:

- пояснення базових концепцій ISO 31000 з рекомендаціями та прикладами, адаптованими до індивідуальних потреб користувачів;
- структурований підхід до переходу від існуючої практики ризик-менеджменту до ISO 31000 з гнучкою перспективою адаптації до майбутніх змін;
- додаткове керівництво щодо принципів ISO 31000 та основи управління ризиками.

IEC 31010:2019 “Risk management – Risk assessment techniques” [5] був розроблений IEC/TC 56 “Dependability” спільно з ISO/TC 262 “Risk management”. Стандарт доповнює положення ISO 31000.

Даний стандарт фокусується на визначеннях, процесах і виборі методу оцінки ризиків та забезпечує основу для прийняття рішення щодо застосування найбільш доцільного підходу до оцінки конкретних ризиків.

Стандарт надає перелік методів оцінки ризику, таких, як, наприклад, мозковий штурм, метод Делфі, техніка SWIFT, дерево рішень, метод Монте-Карло, методи HAZOP, HACCP, FMEA, FTA тощо.

У стандарті ISO Guide 73:2009 “Risk management – Vocabulary” [6] наведено терміни та визначення понять у сфері керування ризиком. Стандарт був переглянутий у 2016 році, тому дана версія залишається актуальною.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission) – американський стандарт, розроблений Комітетом організацій-спонсорів Комісії Тредвею у 1992 році, був оновлений у 2004 і 2017 році.

Коли вийшла перша версія COSO Enterprise Risk Management 2004 “Integrated Framework” (“Інтегрована модель”), цей документ, можна сказати, був безальтернативним джерелом знань в галузі управління ризиками до публікації стандарту ISO 31000:2009. Він використовувався для впровадження систем

управління ризиками в багатьох організацій як фінансового, так і нефінансового секторів економіки.

На практиці при використанні моделі управління ризиками, запропонованій в COSO ERM 2004 пріоритетним був процес ризик-менеджменту, проте здійснювався він окремо від процесів планування та прийняття управлінських рішень. У зв'язку зі змінами в законодавстві та змінами, пов'язаними з появою нових ризиків, підвищенням їх складності та зростом глобальної конкуренції, виникла необхідність в оновленні документу.

COSO ERM 2017 "Integrating with Strategy and Performance" ("Інтеграція зі стратегією та ефективністю діяльності") являє собою концептуальні основи управління ризиками в організації та надає рекомендації зі створення корпоративної системи управління ризиками.

COSO не позиціонує себе як стандарт, це скоріше підхід до управління ризиками, який описано в даному документі. Фактично це набір рекомендацій.

Структура концепції COSO ERM 2017 складається з 5 елементів, котрі містять в собі 20 принципів управління. Вона наведена в табл. 1.1. [7]

Принципи COSO ERM дають більш точну спрямованість на цільові аудиторії у порівнянні з ISO 31000.

Таблиця 1.1

Структура концепції COSO ERM 2017

Компоненти	Принципи
Управління і культура	Здійснення Радою директорів наглядової функції за управлінням ризиками. Створення операційних структур. Визначення бажаної культури. Демонстрація прихильності основним цінностям. Залучення, розвиток і утримання кваліфікованих спеціалістів.
Стратегія і постановка цілей	Аналіз умов ведення діяльності. Визначення ризик-апетиту. Оцінка стратегічних альтернатив. Формулювання бізнес-цілей.

Продовження табл. 1.1

Структура концепції COSO ERM 2017

Компоненти	Принципи
Ефективність діяльності	Виявлення ризиків. Оцінка впливу ризиків. Пріоритизація ризиків. Реагування на ризик. Комплексний погляд на ризики.
Моніторинг і впровадження змін	Оцінка існуючих вразливостей. Аналіз ризиків і ефективності діяльності. Підвищення ефективності системи управління ризиками.
Інформація, комунікація та звітність	Використання інформації та технологій. Розповсюдження інформації про ризики. Звітність по ризикам, корпоративній культурі й ефективності діяльності.

Якщо розглядати компонент “Ефективність діяльності”, то першочергово організація виявляє ризики на всіх рівнях бізнес-процесів і функцій, пов’язані з досягненням стратегічних та бізнес-цілей, і формує загальну базу даних по ризикам (risk inventory) для подальшого визначення актуальних ризиків.

Після цього ризики оцінюються за впливом і ймовірністю, яка може бути отримана шляхом експертної, кількісної оцінки та частотою реалізації ризику. Оцінка може бути як кількісною, так і якісною. Для подальшої пріоритизації ризиків може бути застосована карта ризиків (heat map) в якості інструменту візуалізації їх істотності.

Пріоритизація проводиться з метою обрати адекватну стратегію з реагування на ризики і обґрунтовано розподілити ресурси, виділені на управління ризиками. Пріоритет ризиків визначається за певними критеріями, наприклад, складність ризику, швидкість впливу ризику, відновлення після реалізації ризику тощо.

У відношенні до ризику можна виділити 5 стратегій: прийняття ризику, ухилення, зниження або добір ризику і його передача. Вибір стратегії ґрунтується

на співвідношенні вигоди і втрат, пріоритизації ризиків, істотності ризику, ризик-апетиті та умовах ведення бізнесу.

Актуальна версія COSO ERM 2017 є більш вдалою в порівнянні зі своїм першим виданням. В моделі COSO ERM 2004 в якості основних виділялися 4 категорії бізнес-цілей: стратегічні, операційні, цілі підготовки звітності та цілі дотримання вимог законодавства, і для їх досягнення створювалася система управління ризиками. Нова версія документу відмовилася від минулої концепції і акцентувала увагу на інтеграції процесу управління ризиками в існуючі процеси, що дозволить встановити нові перспективи в галузі ризик-менеджменту.

Однак у той же час концепція недостатньо детально описує підходи до кількісної оцінки ризиків і альтернативні інструменти візуалізації ризиків.

FERMA (Federation of European Risk Management Associations) – стандарт, розроблений Федерацією Європейських Асоціацій ризик-менеджерів у 2002 році.

В розробці стандарту брали участь організації, які займалися питанням ризик-менеджменту у Великобританії. Це такі організації, як Інститут Ризик-Менеджменту (Institute of Risk Management, IRM), Асоціація Ризик-Менеджменту і Страхування (Association of Insurance and Risk Managers in Industry and Commerce, AIRMIC) та Національний Форум Ризик-Менеджменту в Громадському Секторі (The National Forum for Risk Management in the Public Sector).

В стандарті присутні основні визначення в галузі ризик-менеджменту, на прикладі пояснені ключові зовнішні та внутрішні фактори ризику, описано процес управління ризиками та їх аналізу, ролі та функції Ради директорів і ризик-менеджерів, а також перелік методів ідентифікації та оцінки ризиків. Також наголошується, що процес ризик-менеджменту повинен розвиватися, бути постійним та інтегрованим в загальну культуру організації, прийнятий керівництвом і донесений до співробітників. Процес ризик-менеджменту представлено на рис. 1.5 [8].

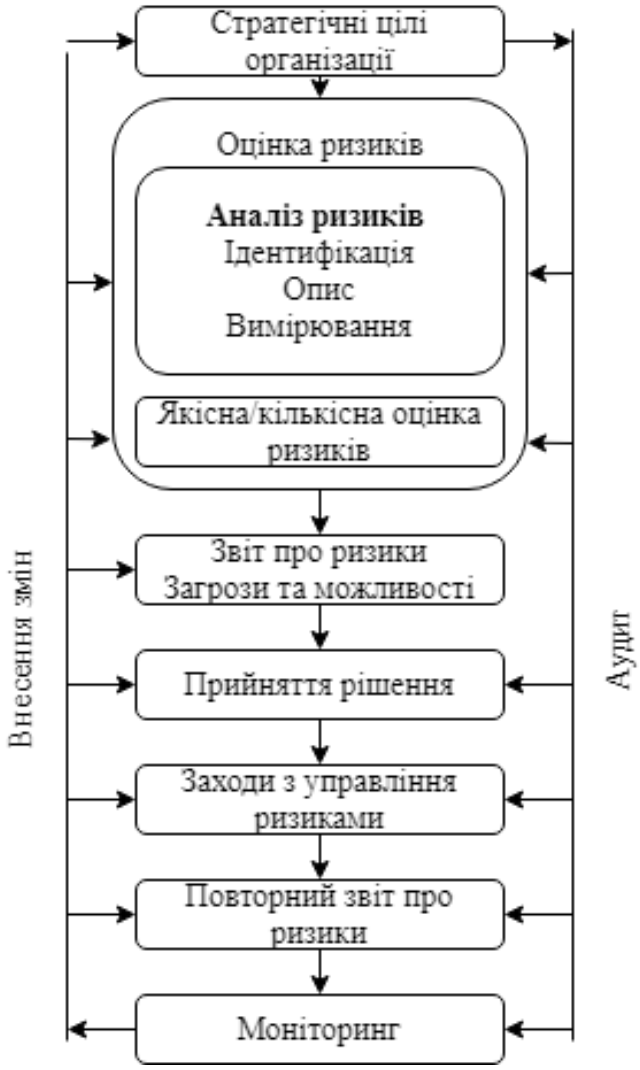

Рис. 1.5. Етапи процесу ризик-менеджменту згідно FERMA

Стандарт ISO/IEC 27005:2018 “Information Technology – Security Techniques – Information Security Risk Management” входить до серії стандартів ISO 27000 і взаємопов’язаний з деякими з них (рис. 1.6).

На відміну від раніше розглянутих документів, ISO/IEC 27005 є більш вузькоспеціалізованим і фокусується саме на ризиках інформаційної безпеки. Він містить детальне керівництво з управління ризиками, яке допоможе задовольнити вимогам, наявним в ISO/IEC 27001.

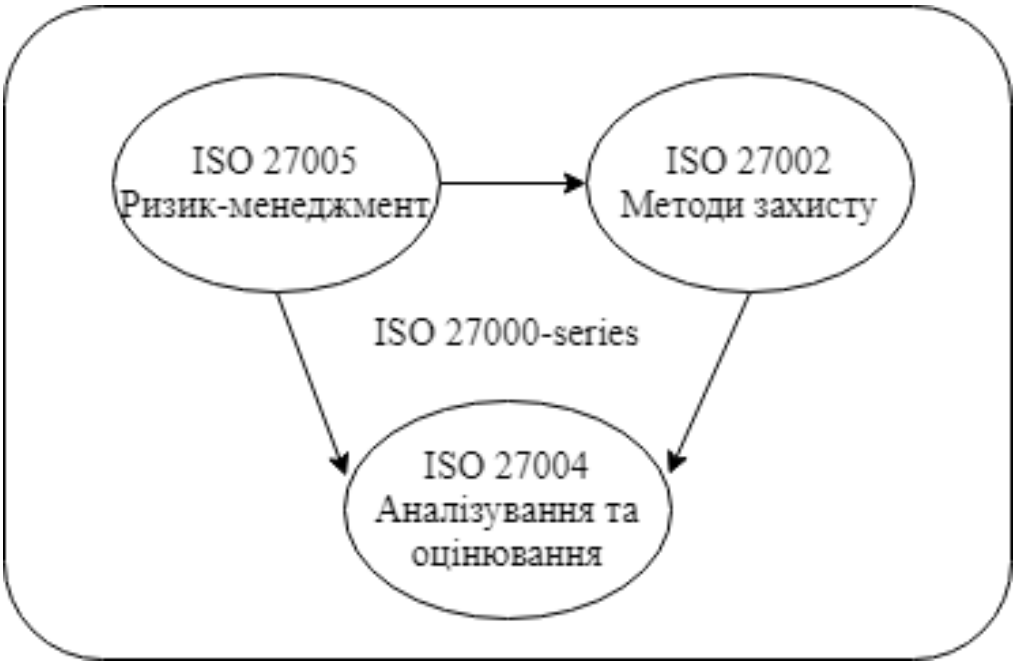

Рис. 1.6. Зв’язок стандартів серії ISO 27000

Процес ризик-менеджменту згідно зі стандартом складається з встановлення контексту, оцінки та обробки ризику, прийняття ризику, комунікацій ризику, а також моніторингу й переоцінки ризику інформаційної безпеки (рис.1.7) [9].

Можна побачити, що процедури оцінки і обробки ризику можуть виконуватись ітеративно. Такий підхід дозволить збільшити глибину і деталізацію при кожному наступному повторюванні процесу.

Першочергово встановлюється контекст, після чого ризик оцінюється. У випадку, коли в результаті в наявності є достатня кількість інформації для ефективного визначення дій, необхідних для зниження ризику до прийнятного рівня, можна переходити до наступного етапу – обробки ризиків. Якщо ж інформації недостатньо, проводиться необхідна кількість ітерацій оцінки ризику в умовах зміненого контексту (можуть бути змінені критерії оцінки, критерії прийняття і критерії впливу ризиків), після чого проводиться обробка ризиків.

Проте вона може не одразу забезпечити прийнятний рівень залишкового ризику. В такому випадку знов проводиться ітерація зі зміною параметрів контексту, і наступні за ним етапи.

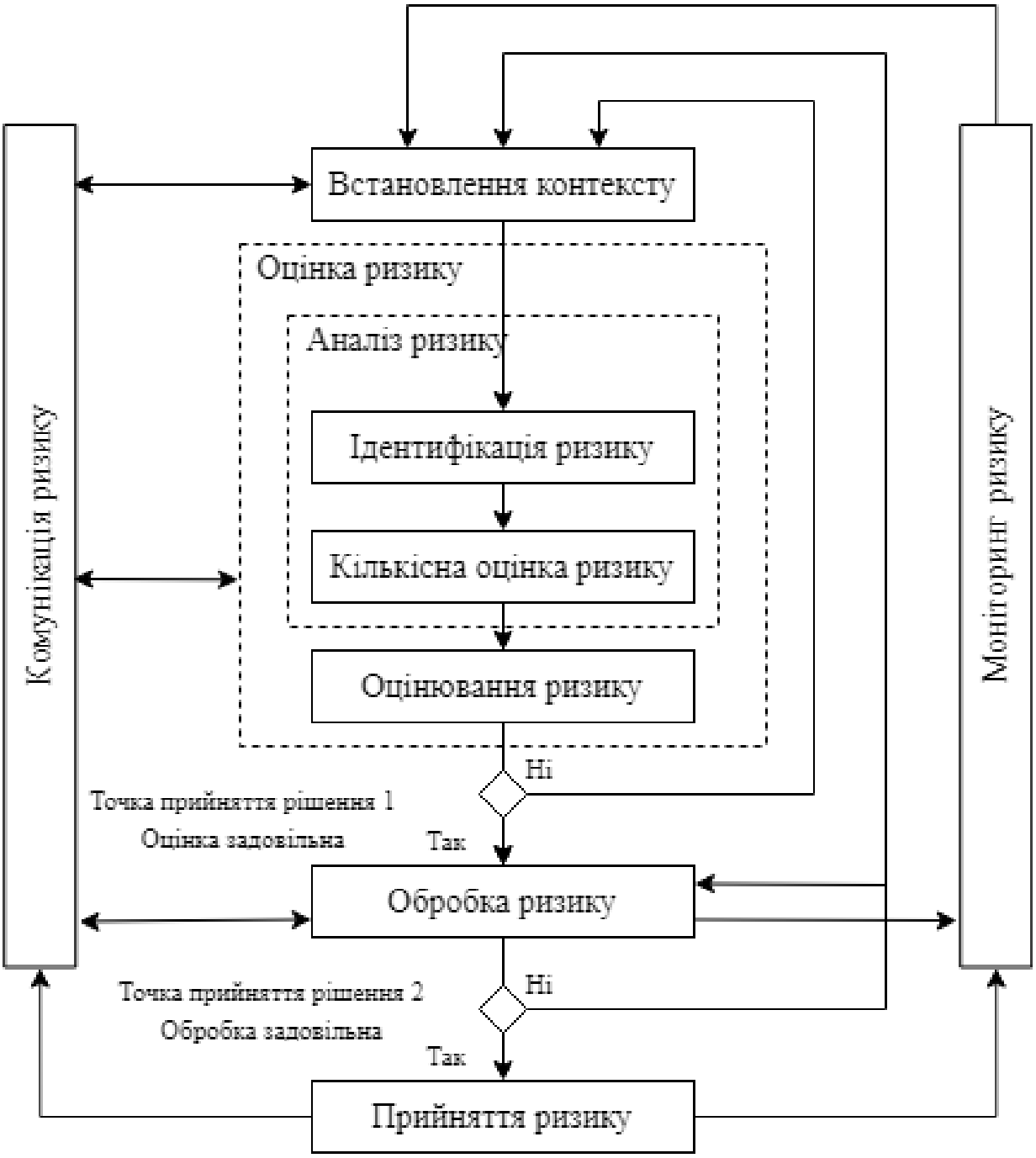

Рис. 1.7. Схема менеджменту ризиків інформаційної безпеки згідно з ISO 27005

В Україні актуальні стандарти з ризик менеджменту є ідентичними до стандартів міжнародної організації зі стандартизації [10]:

- ДСТУ ISO 31000:2018 “Менеджмент ризиків. Принципи та настанови” (ISO 31000:2018, IDT);
- ДСТУ ISO/IEC 27005:2019 “Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки” (ISO/IEC 27005:2018, IDT);

- ДСТУ IEC/ISO 31010:2013 “Керування ризиком. Методи загального оцінювання ризику” (IEC/ISO 31010:2009, IDT);
- ДСТУ ISO/TR 31004:2018 “Менеджмент ризиків. Настанови з впровадження ISO 31000” (ISO/TR 31004:2013, IDT):
- ДСТУ ISO Guide 73:2013 “Управління ризиком. Словник термінів” (ISO Guide 73:2009, IDT)

1.2 Методологія управління інформаційними ризиками

Для розгляду методології управління ризиками інформаційної безпеки необхідно в першу чергу визначитися з деякими термінами [11]:

- Ризик – це результат невизначеності при досягненні цілей.
- Рівень ризику – це його величина, яка може бути розрахована як добуток ймовірності виникнення певної події та розміру наслідків цієї події.
- Залишковий ризик – це ризик, який залишився після обробки.

Процес управління ризиками інформаційної безпеки описано у стандарті ISO/IEC 27005. Варто відзначити, що даний процес є циклічним і пов’язаний із системою управління інформаційною безпекою, описаною моделлю PDCA в стандарті ISO/IEC 27001. Взаємозв’язок між процесом СУІБ і процесом менеджменту ризику ІБ показано в табл. 1.2.

Таблиця 1.2

Взаємозв’язок СУІБ та процесу УРІБ

Процес СУІБ	Процес менеджменту ризику ІБ
Планування	Встановлення контексту Оцінка ризику Планування обробки ризику Прийняття ризику
Дія	Реалізація плану обробки ризику
Перевірка	Проведення постійного моніторингу та переоцінки ризиків
Вплив	Підтримка та вдосконалення процесу менеджменту ризиків ІБ

Першим етапом процесу ризик-менеджменту є етап встановлення контексту. Для його проведення в першу чергу необхідно зібрати всі дані про організацію, які стосуються ризик-менеджменту. Після цього необхідно визначити основні критерії, необхідні для менеджменту ризиків інформаційної безпеки. До таких критеріїв належать критерії оцінки ризиків, критерії впливу та критерії прийняття ризику.

Критерії оцінки ризику повинні враховувати вартість інформаційних активів, вимоги до забезпечення їх доступності, конфіденційності та цілісності, вимоги законодавства та договірних зобов’язань, роль інформаційних бізнес-процесів, очікування та реакцію причетних сторін, а також ймовірні негативні наслідки для нематеріальних активів та репутації організації.

Критерії впливу повинні враховувати величину збитків або витрат на відновлення внаслідок реалізації негативних подій, порушення інформаційної безпеки такі, як втрата конфіденційності, цілісності та доступності, порушення оперативної діяльності, порушення планів та графіків, репутаційні збитки, порушення вимог законодавства та договірних зобов’язань.

Критерії прийняття ризику обираються, спираючись на політику організації, її цілі та інтереси причетних сторін. Вони повинні враховувати критерії бізнесу, особливості законодавчо-нормативного середовища, технології, фінанси, операції,

соціальні та гуманітарні фактори. Кожна організація самостійно обирає свої власні шкали для рівнів прийняття ризику.

Окрім цих трьох критеріїв також слід врахувати межі та сферу застосування процесу управління ризиками інформаційної безпеки. До уваги беруться бізнес-цілі та бізнес-процеси, політики організації, в тому числі і політика ІБ, структура, функції, інформаційні активи організації, законодавчі вимоги та очікування зацікавлених сторін.

Після встановлення основних критеріїв, меж та сфери діяльності, проводиться етап оцінки ризику. В ході проведення процесу оцінки організацією повинна бути знайдена вартість її інформаційних активів, повинні бути ідентифіковані актуальні загрози, вразливості та наявні засоби захисту, розрахована ефективність цих заходів і повинні бути визначені можливі наслідки у разі реалізації ризиків. Як результат будуть отримані якісна та/або кількісна оцінка ризиків та перелік оцінених ризиків відповідно до призначених пріоритетів згідно з критеріями оцінки ризику. Процес оцінки ризиків складається з ідентифікації ризиків, встановлення значень ризиків та їх порівняння.

Етап ідентифікації ризиків показує, які негативні події можуть виникнути, а також які умови чи фактори і за яких обставин можуть призвести до завдання організації збитків. Процес передбачає розгляд всіх ризиків, незалежно від того, знаходиться джерело ризику під контролем організації чи непідконтрольне їй. Дії, які необхідно провести на етапі ідентифікації, представлені на рис. 1.8.

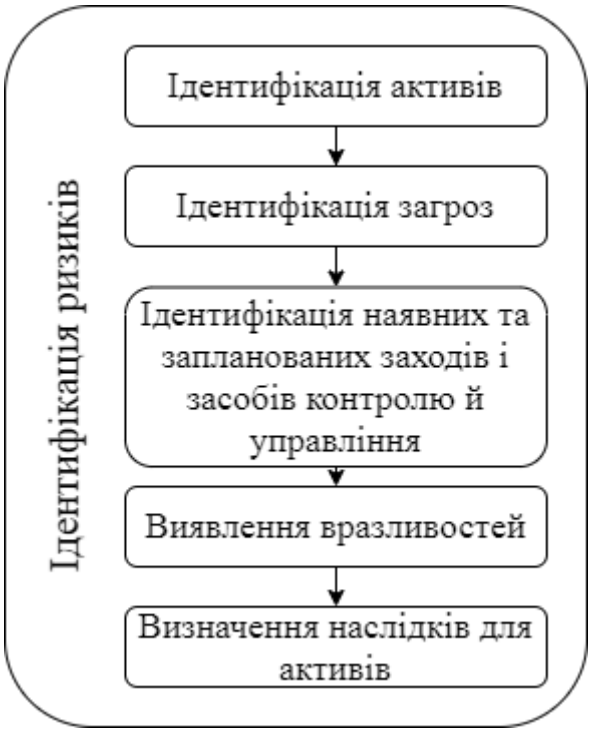

Рис. 1.8. Етапи ідентифікації ризиків

Першим кроком є ідентифікація активів. Вона повинна бути виконана достатньо деталізовано для того, щоб забезпечити необхідну кількість достовірної інформації для подальшої оцінки ризику. Також для кожного активу призначається володілець, який хоч і може фактично не володіти активом, але буде нести відповідальність за його отримання, розробку, підтримку, використання та безпеку. В результаті ідентифікації активів в наявності буде перелік пов’язаних з ризик-менеджментом активів і перелік бізнес-процесів, пов’язаних з цими активами.

Після цього ідентифікуються загрози: навмисні та випадкові, та відповідні їх джерела. Інформацію щодо ймовірності виникнення загроз можна отримати на основі минулого досвіду, з внутрішніх джерел організації, наприклад, від володільців активів, персоналу відділу кадрів, спеціалістів ІБ тощо, та з зовнішніх джерел – від страхових компаній чи зовнішніх консультантів. В результаті буде створено перелік загроз із визначенням їх виду та джерела.

Третім етапом є ідентифікація наявних та запланованих заходів і засобів контролю й управління. Вона необхідна для того, щоб уникнути зайвих витрат часу та ресурсів, які можуть виникнути, наприклад, у разі дублювання таких заходів і

засобів. Наявні заходи та засоби контролю й управління повинні бути переглянуті, оскільки їх неналежне функціонування може стати причиною вразливості. Для їх визначення можуть проводитися перевірки разом із відповідальними за ІБ співробітниками, переглядатися документи, що містять інформацію про засоби захисту, розглядатися результати внутрішніх аудитів та проводитися моніторинг периметру з метою огляду та перевірки фізичних засобів контролю на предмет правильного й ефективного функціонування. В результаті буде отримано перелік існуючих та запланованих заходів і засобів контролю та управління, їх місцезнаходження та стан використання.

Наступним кроком є виявлення вразливостей. Необхідно виявити вразливості, які можуть бути використані загрозами для спричинення збитку активам чи організації. Важливо враховувати не тільки вразливості в апаратному чи програмному забезпеченні, але і в бізнес-процесах, фізичній інфраструктурі, персоналі та стосунках із зовнішніми сторонами.

В результаті буде отримано: по-перше – перелік вразливостей, пов’язаних з активами, загрозами та заходами і засобами контролю й управління, по-друге – перелік вразливостей, не пов’язаних з ідентифікованими загрозами, і які в подальшому потребують моніторинг на предмет змін.

Останнім кроком є визначення наслідків для активів у зв’язку з порушенням конфіденційності, цілісності та доступності. Такими наслідками можуть бути зменшення ефективності, втрата бізнесу, репутаційні збитки тощо. Формуються сценарії інцидентів – опис загроз, що використовують одну чи більше вразливостей в інциденті ІБ.

Після ідентифікації ризику необхідно встановити його значення. У залежності від критичності активів, відомих вразливостей і минулих інцидентів обирається ступінь деталізації для аналізу ризику. Аналіз може бути кількісним, якісним чи комбінованим. Завдяки простоті якісного аналізу він використовується першим для визначення найбільш небезпечних та пріоритетних ризиків. Після цього вже до виявлених ризиків за необхідністю застосовується кількісний аналіз, який потребує більшу кількість часу, ресурсів і більшу кваліфікацію.

Для встановлення значення ризику необхідно проаналізувати дві величини: потенційні наслідки реалізації загрози ІБ і власне ймовірність реалізації цієї загрози. Під наслідками мається на увазі рівень негативного впливу на організацію внаслідок порушення властивостей інформаційних активів.

Спочатку проводиться аудит наявних активів з подальшою їх класифікацією за критичністю, а також оцінюється можливий негативний вплив на організацію внаслідок порушення властивостей цих активів. Цей вплив при кількісному аналізі доцільно записувати в грошових величинах. Також оцінюється вартість активів, яка може бути розрахована виходячи із вартості заміни чи відновлення активів та інформації, а також їх втрати чи компрометації.

Після визначення негативного впливу проводиться оцінка ймовірності реалізації загрози. Під час оцінки враховується рівень складності у використанні вразливості та частота реалізації загрози. Для цього можна скористатися статистичними даними щодо аналогічних загроз, інформацією про можливі джерела навмисних загроз, наявні в організації вразливості та заходи захисту. Активи можуть бути розділені по групах, базуючись на тому, що для кожної групи будуть застосовані різні сценарії атак. Такий розподіл дозволить більш точно провести оцінку активів.

В кінці етапу визначається рівень ризиків для всіх сценаріїв розглянутих атак, як добуток ймовірності реалізації загрози за кожним сценарієм і відповідним йому наслідкам.

Завершальним етапом при оцінці ризиків є оцінка небезпечності ризику. Для цього необхідно порівняти отримані значення ризиків із критеріями оцінки та критеріями прийняття ризиків, які були встановлені на першому етапі. При прийнятті рішення необхідно враховувати ймовірність виникнення негативних наслідків та їх величину, ступінь впевненості в коректності проведеної ідентифікації та аналізу ризиків, а також властивості активів, забезпечення захисту яких є найбільш актуальним для організації, і важливість бізнес-процесів.

Після етапу оцінки ризиків, якщо отримано достатньо інформації та немає необхідності переглядати контекст та повторно оцінювати ризики, проводиться

обробка ризику. В наявності вже повинен бути перелік ризиків з призначеними пріоритетами відповідно до критеріїв оцінки небезпечності ризиків. Мета даного етапу полягає у виборі заходів і засобів контролю й управління для зниження, збереження, запобігання чи перенесення ризиків, а також у виборі плану обробки ризиків. План діяльності з обробки ризику надано на рис. 1.9 [12].

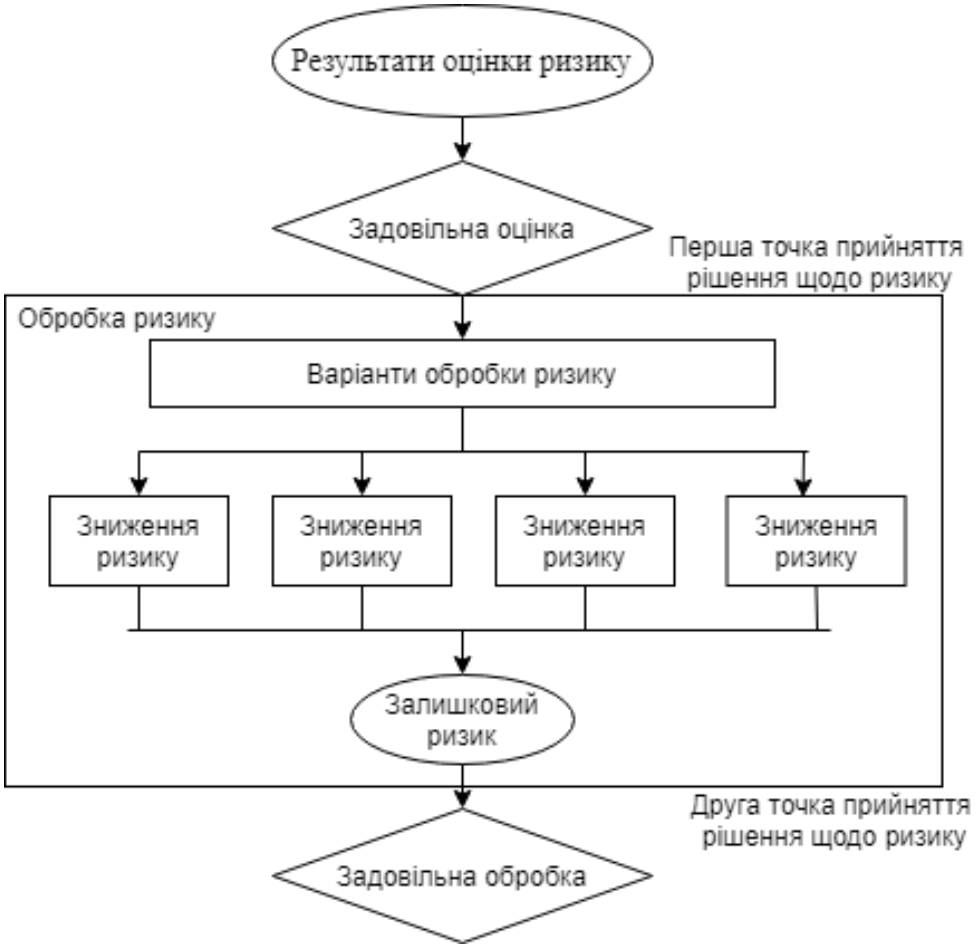

Рис. 1.9. Етапи обробки ризику

Обирати метод обробки слід спираючись на оцінку результат оцінки ризику, очікувану вартість впровадження заходів захисту і очікувані переваги кожного з методів. Необов’язково застосовувати лише один метод: їх можна комбінувати, наприклад, модифікувати наслідки чи ймовірність ризику та передати залишковий ризик. Кращим буде метод, легший в реалізації та не потребуючий значної кількості ресурсів, але при цьому ефект від зниження ризиків повинен бути значним, і більша кількість загроз повинна бути нейтралізована. Прийняття дорогих рішень потребує їх економічного обґрунтування.

Відповідальним особам, визначеним на етапі встановлення контексту, необхідно сформувати план обробки ризиків, в якому буде вказано пріоритет і час, протягом якого необхідно закінчити обробку кожного ризику. Також необхідно перевірити актуальність заходів захисту, якщо такі були впроваджені в організації раніше, і їх вартість. При цьому слід також враховувати взаємозв'язок між заходами захисту та загрозами, для протидії котрим вони були впроваджені.

Після створення плану з обробки ризиків оцінюються залишкові ризики. Це може вимагати проведення ще однієї оцінки ризиків або ж її оновлення з урахуванням очікуваного ефекту від використання запропонованих способів обробки ризику. Як результат буде отримано план обробки ризику та значення залишкового ризику, які будуть необхідні для прийняття рішення керівництвом організації.

Розглянемо більш детально стратегії з обробки ризику.

Модифікація (зниження) ризику змінює значення залишкового ризику до прийнятного рівня шляхом застосування додаткових чи зміни існуючих заходів захисту. При використанні цієї стратегії необхідно обирати доцільні та обґрунтовані заходи захисту, які будуть відповідати вимогам, визначеним на етапах оцінки та обробки ризику. Необхідно враховувати такі обмеження: спосіб обробки не повинен виходити за межі виділеного часу та бюджету, вартість витрат на обслуговування засобів захисту (впровадження, адміністрування, обслуговування персоналом) не повинно перевищувати вартість активу, що захищається.

В межах обраної стратегії можуть бути застосовані такі заходи захисту, як корекція, усунення або мінімізація негативного впливу, виявлення та попередження потенційних порушників, моніторинг і забезпечення обізнаності співробітників. В результаті повинен бути в наявності список можливих заходів захисту з зазначенням їх вартості, переваг і недоліків, а також пріоритету впровадження.

Збереження ризику застосовується тоді, коли рівень ризику відповідає критеріям прийняття ризику, тому немає необхідності реалізувати додаткові заходи захисту.

Запобігання ризику буквально означає, що керівництво організації вирішує не проводити певну діяльність або змінити її умови таким чином, щоб можна було уникнути ризику, пов’язаного з цією діяльністю.

Може бути прийнято рішення передати ризик тій організації, яка зможе максимально ефективно ним керувати. В такому разі слід врахувати, що сама передача ризику може бути ризиком: вона може створити нові ризики або модифікувати вже існуючі, і тому необхідно провести додаткову обробку ризиків.

Рішення щодо прийняття ризику робиться на основі оцінки залишкових ризиків та планів обробки ризиків, в яких повинно бути описано, яким чином будуть оброблені оцінені ризики для того, щоб досягти критеріїв прийняття ризиків. Отримані плани обробки аналізуються відповідальними особами та щодо них приймається рішення та визначають умови, за яких це рішення буде позитивним. У найпростішому випадку значення залишкового ризику порівнюється з визначеним на етапі встановлення контексту прийнятним рівнем ризику, проте слід враховувати, що в окремих випадках буде необхідно переглянути критерії прийняття ризиків у зв’язку з виникненням нових обставин і умов. В такому разі відповідальні особи можуть прийняти ризики, які не відповідають критеріям прийняття, вказавши про це в коментарі до рішення. Як результат буде отримано перелік прийнятих ризиків з обґрунтуванням ризиків, які не відповідають стандартним критеріям прийняття ризику в організації.

Після цього на етапі комунікації ризиків проводиться діяльність із впровадження розробленого плану обробки ризиків. Ця діяльність включає закупівлю та налаштування засобів захисту та іншого обладнання, укладаються договори з реагування на інциденти та страхування, ведеться юридична діяльність з контрагентами. В той же час до керівництва організації доводиться інформація щодо виявлених ризиків ІБ і заходах обробки, які для них застосовуються. Це робиться для досягнення загального розуміння діяльності, що проводиться. Також розроблюються плани комунікації ризиків ІБ для проведення скоординованої діяльності в звичайних та екстрених випадках.

Не можна забувати, що ризикам властиво змінюватися з часом. В організації можуть змінитися певні активи та їх цінність, ймовірність реалізації загрози та рівень наслідків, також можуть з’явитися нові загрози та вразливості. Тож, необхідно проводити постійний моніторинг на предмет змін. Рекомендується залучати зовнішніх спеціалістів в галузі аналізу актуальних загроз ІБ. Разом з ризиками ІБ необхідно регулярно перевіряти і використовувані способи їх обробки для визначення міри їх актуальності та ефективності в умовах потенційно зміненої ситуації. Процес моніторингу потребує найбільшої уваги в моменти, коли трапляються значні зміни в роботі організації та її бізнес-процесах.

Процес управління ризиками необхідно постійно підтримувати та вдосконалювати для забезпечення актуальності контексту, оцінки та плану обробки ризиків у наявних умовах. Всі зміни повинні бути узгоджені з зацікавленими сторонами, всі змінені критерії та оцінки повинні відповідати актуальним бізнес-процесам та цілям організації. За необхідністю можна змінювати або ж вдосконалювати наявний підхід, методологію та інструменти управління ризиками.

1.3 Процедури прийняття рішень по ризикам в умовах невизначеності

В загальному випадку невизначеність можна охарактеризувати як відсутність чи недостатність інформації про деякий процес, подію тощо. Вона передбачає наявність таких факторів, при яких не можна буде точно визначити результати певних дій, а також вплив цих факторів на результат. [13]

Невизначеність може бути викликана або протидією розумного суперника, або недостатньою обізнаністю про умови, в яких необхідно прийняти рішення. [14]

В умовах невизначеності кожне рішення може привести до настання одного з множини всіх результатів, проте невідомі ймовірності виникнення цих результатів.

В залежності від характеру невизначеності моделі прийняття рішень поділяють на ігрові та статистично невизначені. В ігрових моделях невизначеність обумовлюється свідомими діями супротивника. Для прийняття рішень в такому випадку використовується теорія ігор. [15]

Задача прийняття рішення в умовах невизначеності, обумовленою недостатньою обізнаністю про умови, може бути сформульована наступним чином: особі, що приймає рішення (далі – ОПР), необхідно обрати тільки один варіант рішення з n можливих: $x_1, x_2, \ldots, x_n$, і нехай існує m умов чи станів середовища, при котрих будуть реалізовані можливі варіанти: $y_1, y_2, \ldots, y_m$. ОПР володіє інформацією про оцінки кожного варіанту рішення при кожній умові (x_i,y_i). Ця інформація задана у вигляді матриці виграшів або програшів ОПР: $A=|a_{ij}|$.

Нехай ОПР невідома інформація щодо ймовірності виникнення кожної з умов y_j. В такому випадку доцільно буде скористатися критеріями оптимальності вибору рішень із теорії статистичних рішень.

Не існує єдиного правильного підходу до вибору критерію. Вибір робиться самостійно ОПР і залежить від його характеру, вподобань, досвіду, інтуїції тощо. Розглянемо далі деякі з таких критеріїв.

Критерій середнього виграшу. Цей критерії передбачає попереднє встановлення значень ймовірностей виникнення кожної з умов P_j. Вони можуть бути отримані з експертних оцінок або суб'єктивних тверджень. Виграш буде оцінюватись як математичне очікування оцінок виграшу за всіма станами середовища, тобто за всіма умовами. Якщо розраховується виграш, оптимальним рішенням буде максимальна оцінка, якщо розраховуються збитки – мінімальна.

Розглянемо приклад, коли необхідно прийняти рішення щодо вибору одного з трьох варіантів захисту комп'ютерної системи (x_1, x_2, x_3). Було проведено аналіз ризиків, який дозволив виявити узагальнені загрози ІБ (y_1, y_2, y_3, y_4) і оцінити втрати внаслідок їх реалізації. Експерти оцінили ймовірність реалізації кожної загрози і отримали такі результати: $P_1=0,15, P_2=0,2, P_3=0,3, P_4=0,35$. Необхідно занести дані в матрицю збитків. В рядках маємо 3 стратегії захисту, в стовпцях – 4 типи загроз,

на перетині – оцінка збитку у разі вибору певної стратегії та реалізації конкретної загрози [16].

$$\begin{Vmatrix} -800 & -1000 & -650 & -780 \\ -850 & -900 & -510 & -780 \\ -900 & -850 & -640 & -800 \end{Vmatrix}$$

Далі розрахуємо математичне очікування збитку для кожної стратегії за формулою знаходження математичного очікування для дискретних величин:

$$M_i = \sum_{j=1}^{m} P_j \cdot a_{ij} \tag{1.1}$$

Отримаємо такі середні значення:

$M_1 = (-800) \cdot 0{,}15 + (-1000) \cdot 0{,}2 + (-650) \cdot 0{,}3 + (-780) \cdot 0{,}35 = -788$

$M_2 = -733{,}5$

$M_3 = -777$

Оскільки необхідно отримати мінімальні збитки, тобто в нашому випадку максимальне значення, то за критерієм середнього виграшу ОПР доцільно буде обрати другу стратегію захисту комп’ютерної системи.

Окремий випадок критерію середнього виграшу – це критерії Лапласа [17]. Згідно з даним критерієм робиться припущення, що ймовірності настання кожної умови однакові, оскільки немає достатніх підстав припускати інше. В такому випадку формула набуває вигляду:

$$M_i = \frac{1}{j} \sum_{j=1}^{m} a_{ij} \tag{1.2}$$

Для значень з прикладу буде отримано такий результат:

$$M_1 = -\frac{1}{4}(800 + 1000 + 650 + 780) = -807{,}5$$

$$M_2 = -760$$

$$M_3 = - - 797{,}5$$

Як можна побачити, у випадку, якщо невідомі ймовірності, будуть отримані інші значення. Проте в даному випадку стратегія не змінюється: за критерієм Лапласа при впровадженні заходів захисту з другого варіанту отримаємо в результаті найменші значення збитків.

Критерій Вальда – це критерій крайнього песимізму. [18]. В якості оптимальної за даним критерієм обирається стратегія, яка при найгірших умовах гарантує найкращий результат.

Критерії Вальда може орієнтуватися як на мінімум серед максимальних значень витрат, так і на максимум серед мінімальних значень виграшу.

Алгоритм методу полягає в пошуку в кожному рядку єдиного найгіршого значення (мінімальний виграш чи максимальний збиток), а після цього серед знайдених значень обирається найкраще (максимальний виграш чи мінімальний збиток). Оптимальним буде рішення, в рядку якого було отримано оптимальне значення.

На нашому прикладі: оскільки в матриці маємо від'ємні збитки, спочатку з кожного рядку необхідно обрати мінімальне значення (максимальне, якщо збитки записувати як додатні значення) або ж максимальне абсолютне значення.

Отримаємо такі результати: $a_{12}=-1000$, $a_{22}=-900$, $a_{31}=-900$.

Після цього обираємо серед них максимальне значення. В даному випадку оптимальними будуть друга і третя стратегії. Це означає, що при їх виборі найгірший результат, який може бути отримано, буде збиток, рівний 900 у. о.

Критерій "максімаксу" – це повна протилежність критерію Вальда. [19]. Якщо за критерієм Вальда розглядалися найгірші умови з можливих, то за критерієм "максімаксу" розглядаються найоптимістичніші умови. Оптимальним стає вибір, який забезпечує максимальний виграш чи мінімальний програш.

Алгоритм даного методу полягає в знаходженні найкращого значення в кожному рядку і виборі серед отриманих значень найкращого.

В нашому випадку обираємо мінімальні абсолютні значення, отримаємо результати: a_{13}=-650, a_{23}=-510, a_{33}=-640. Оптимальним за критерієм “максімаксу” буде другий варіант, оскільки він забезпечує найменший збиток при найкращих умовах.

Критерій Гурвіца, також відомий як критерій песимізму-оптимізму, встановлює баланс між випадками крайнього оптимізму та крайнього песимізму шляхом зважування обох способів поведінки відповідними вагами α і (1-α). Коефіцієнт оптимізму α знаходиться в проміжку від 0 до 1 і обирається ОПР в залежності від його схильності до оптимізму чи песимізму. Чим більше ОПР схильна до оптимізму, тим більше α і відповідно тим менше (1-α). При відсутності схильності зазвичай обирається $\alpha=0,5$.

Критерій Гурвіца враховує найкраще і найгірше значення кожної альтернативи. Для знаходження величини критерію Гурвіца знаходиться сума добутку коефіцієнту оптимізму та найкращого значення й добутку коефіцієнту песимізму та найгіршого значення [20].

$$H_i(\alpha) = \alpha \cdot a_{i\_best} + (1-\alpha) \cdot a_{i\_worst} \tag{1.3}$$

Припустимо, що ОПР не схильний ні до оптимізму, ні до песимізму. В такому випадку отримаємо результати:

$$H_1(0,5) = 0,5 \cdot (-650) + 0,5 \cdot (-1000) = -825$$
$$H_2(0,5) = -705$$
$$H_3(0,5) = -770$$

Тож, за критерієм Гурвіца, друга стратегія зменшить збитки до мінімального значення. Основним недоліком такого методу є те, що він нечутливий до розподілу результатів між крайніми значеннями.

Критерій Севіджа [21] дещо відрізняється від раніше розглянутих критеріїв тим, що він для оцінки альтернатив використовує не початкову матрицю, а матрицю ризиків. Для цього для кожної альтернативи при конкретних заданих умовах розраховується різниця між найкращим значенням, яке можна отримати при заданих умовах, і наявним значенням Розглянемо використання даного критерію на нашому прикладі більш детально.

Спочатку для кожної загрози визначимо найкраще значення, тобто мінімальне значення збитку: $y_j = \max(a_{ij})$.

Буде отримано результати: a_{11}=-800, a_{32}=-850, a_{23}=-510, a_{14}=-780.

Після цього необхідно для кожної клітинки початкової матриці знайти різницю між знайденим найкращим значенням для кожної загрози і результатом, що розглядається в кожній клітині a_{ij}: $r_{ij} = y_j - a_{ij}$, а також побудувати матрицю ризиків за отриманими результатами.

$$\begin{vmatrix} 0 & 150 & 140 & 0 \\ 50 & 50 & 0 & 0 \\ 100 & 0 & 130 & 20 \end{vmatrix}$$

Знайдемо максимальне значення збитків за кожною стратегією: r_{12}=150, r_{21}=50, r_{33}=130. Оптимальною буде стратегія, яка виповідає рядку, який містить найменше значення, тобто за критерієм Севіджа більш доцільною буде друга стратегія.

Розглянуті критерії використовують у випадках, коли ОПР не володіє інформацією про ймовірності настання певних подій, умов, станів середовища. Якщо ж в наявності є інформація про розподіл ймовірностей, можна використовувати такі ймовірнісні характеристики ризику, як математичне очікування, дисперсія, середньоквадратичне відхилення і коефіцієнт варіації.

Розподіл ймовірностей – це закон, який описує область значень випадкової величини та відповідні ймовірності появи цих значень.

Математичне очікування показує середнє очікуване значення виграшу чи програшу. При нормальному розподілі ймовірностей відображає середнє значення випадкової величини.

Дисперсія показує середнє очікуване значення відхилень від математичного очікування, а середньоквадратичне відхилення – середній ступінь розкиду значень випадкової величини відносно її математичного очікування.

Зазвичай для прийняття рішення щодо вибору стратегії обробки ризику до уваги беруть математичне очікування, середньоквадратичне відхилення, і їх комбінацію – коефіцієнт варіації.

Для розрахунку математичного очікування можна скористатися формулою (1.1) у випадку задання функції розподілу для дискретних величин. Якщо величина є безперервною, використовується формула (1.4):

$$M[X] = \int_{-\infty}^{+\infty} x \cdot f(x)dx, \tag{1.4}$$

де *x* – аргумент функції розподілу, якою задана випадкова величина;

f(x) – функція щільності розподілу.

Дисперсія розраховується як різниця математичного очікування квадрату випадкової величини і квадрату математичного очікування випадкової величини:

$$D = M[X^2] - M^2[X] = \int_{-\infty}^{+\infty} x^2 \cdot f(x)dx - \left(\int_{-\infty}^{+\infty} x \cdot f(x)dx \right)^2 \tag{1.5}$$

Середньоквадратичне відхилення розраховується як квадратний корінь з дисперсії:

$$\sigma = \sqrt{D} \tag{1.6}$$

У випадку, якщо математичні очікування рівні, а середньоквадратичні відхилення різні, більш раціональним вважається рішення з меншим середньоквадратичним відхиленням, оскільки це означає менший розкид значень від очікуваного середнього і відповідно менший ризик. Однак така ситуація на практиці зустрічається рідко. Більш розповсюджений випадок, коли всі параметри різні. В такому випадку вводиться коефіцієнт варіації, який розраховується як частка середньоквадратичного відхилення і математичного очікування.

$$K = \frac{\sigma}{M} \tag{1.7}$$

Даний коефіцієнт фактично показує, який рівень ризику буде приходитися на одну одиницю прибутку або збитків. Чим більший коефіцієнт варіації, тим більша невизначеність і відповідно тим більший ризик при прийнятті рішення.

Тож, в процесі прийняття рішення в умовах невизначеності ключову роль відіграють особисті якості ОПР. Вибір критеріїв та методів, згідно з якими буде проводитися подальша робота з ризиками, залежить від його схильності до оптимізму чи песимізму, схильності до ризику тощо. Вибір підходу також може враховувати корисність того чи іншого рішення для бізнесу, на основі якого вирішується, доцільно буде ризикувати чи в цьому немає необхідності. Можна стверджувати, що прийняття рішення в умовах невизначеності – процес суб’єктивний, і не гарантує належної точності, однак за допомогою розглянутих критеріїв можна визначити критичні значення: максимальні та мінімальні збитки або прибутки, і вже порівнюючи їх, прийняти відповідне рішення.

Прийняте в умовах ризику рішення матиме більшу точність, оскільки будуть відомі дві характеристики, які, власне, і визначають ризик: це значення програшу або виграшу і значення ймовірності виникнення певної умови чи стану середовища. Для прийняття рішення на основі кількісних оцінок доцільно використовувати поняття теорії ймовірностей і статистики і вже після отримання результатів обрати найбільш оптимальний для організації.

Процес прийняття рішення в загальному вигляді представлено на рис. 1.10. [22]

Рис. 1.10. Схема алгоритму дій керівництва щодо прийняття рішення в умовах ризику та невизначеності

Висновки до першого розділу

Управління ризиками інформаційної безпеки є невід'ємним процесом забезпечення ІБ організації. Для вдалого функціонування цей процес повинен бути інтегрований у ключові процеси організації і застосований у процесі прийняття рішень.

Найбільш використовуваними стандартами в галузі ризик-менеджменту є міжнародні стандарти серії ISO 31000 та стандарт ISO 27005, який базується саме на ризиках інформаційної безпеки. Велика кількість національних стандартів була замінена на ISO 31000 і адаптована під наявні особливості країни, наприклад, таким чином було замінено австралійсько-новозеландський стандарт AS/NZS 4360:2004 у 2009 р. та адаптовано американську серію стандартів ANSI/ASSP Z690.

Процес управління ризиком в ISO 31000 та ISO 27005 схожий: спочатку повинен бути встановлений контекст, після чого ризики оцінюються, приймається рішення щодо їх обробки та можливості прийняття. Обидва стандарти наголошують, що процес ризик-менеджменту повинен бути ітеративним та на кожному етапі може проводитися моніторинг та комунікація ризиків.

Рішення щодо обробки ризику приймається ОПР, базуючись на визначеннях теорії ймовірностей та статистики. У випадку ситуації невизначеності, суб'єктивність прийнятого рішення полягає в індивідуальних якостях ОПР: його схильності до ризику, оптимізму чи песимізму. Від цих якостей залежить вибір конкретного методу оцінки, і в більшості випадків результати кожного методу будуть відрізнятися один від одного. Більш точне рішення може бути прийнято у випадку, якщо відомо розподіл ймовірностей, тому доцільно буде додатково залучати експертів для отримання хоча б приблизних кількісних значень ймовірностей, після чого можна буде порівняти результати і вже на основі цього прийняти більш обґрунтоване управлінське рішення.

Розділ 2 АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ І ЇХ ОЦІНКИ В ОРГАНІЗАЦІЇ

Для досягнення мети дослідження необхідно розглянути та класифікувати основні методи оцінки ризиків інформаційної безпеки, розглянути сучасні методології оцінки та аналізу ризиків. Базуючись на розглянутих методах буде наведено кількісні способи розрахунку значення ризиків.

2.1 Підходи до оцінки ризиків інформаційної безпеки

В стандарті ISO 31000:2018 надається таке визначення терміну: ризик – це вплив невизначеності на цілі. Причому в примітці додається, що вплив може бути як позитивним, так і негативним, і може сприяти реалізації можливостей і усуненню загроз, або ж створювати і призводити до них.

Якщо розглядати конкретно ризик інформаційної безпеки, то згідно з ISO 27005:2018, ризик інформаційної безпеки – це можливість того, що певна загроза зможе скористатися вразливістю активу чи групи активів, і тим самим завдасть збитків організації.

Тобто, якщо говорити про ризик інформаційної безпеки, він може мати лише негативний вплив. Для керування цим впливом створено процес управління ризиками інформаційної безпеки, одним з ключових етапів якого є оцінка ризику.

На етапі оцінки ризику (risk assessment) ризики повинні бути ідентифіковані, оцінені кількісно або якісно (risk evaluation) та розташовані за пріоритетами відповідно до критеріїв оцінки ризику та цілей організації, які були визначені на етапі встановлення контексту. Також порівнюється вартісна оцінка ризику з її максимально допустимим значенням, яке встановлює керівництво організації, а також з вартісною оцінкою інших ризиків.

Вартісна оцінка ризику визначається шляхом комбінування двох величин – ймовірності події та величини її наслідків. Зазвичай під подією мається на увазі реалізація загрози, що використовує вразливості активу для здійснення впливу на цей актив і порушення його безпеки, тобто таких властивостей, як конфіденційність, цілісність і доступність. Через порушення безпеки активу організація зазнає збитків. Цінність активу може бути визначена як величина цих збитків

Як було сказано раніше, в процесі оцінки ризику встановлюється цінність інформаційних активів організації, визначаються можливі загрози та вразливості стосовно цих активів, а також існуючі заходи і засоби контролю й управління та їх вплив на ідентифіковані ризики. Визначаються можливі наслідки та здійснюється пріоритизація та ранжування ризиків.

Враховуючи те, що процес управління ризиками є ітеративним, відповідно і оцінка ризику може і нерідко здійснюється за дві чи більше ітерацій. Спочатку зазвичай проводиться високорівнева оцінка, призначена для ідентифікації потенційно найбільш небезпечних, критичних ризиків. [9] На них базується подальша оцінка.

Під час наступних повторень процесу можна більш глибоко розглянути виявлені ризики. В тому випадку, якщо кількість здобутої інформації недостатня для адекватної оцінки ризику, слід провести більш детальний аналіз.

Відповідальним за вибір підходу до оцінки ризику є керівництво організації. Вибір ґрунтується на задачах і цілях оцінки ризику.

Високорівнева оцінка надає можливість визначити пріоритети та послідовність дій. Вона може розглядати організацію та її інформаційні системи в більш загальному вигляді, і в такому випадку буде вважатися, що технологічні аспекти не залежатимуть від проблем бізнесу. В такому випадку аналіз контексту буде фокусуватися на експлуатаційному та бізнес-середовищі, а не на технологічних компонентах. Високорівнева оцінка також може враховувати меншу кількість загроз та вразливостей, згрупованих у конкретних сферах. Ризики,

визначені у високорівневій оцінці ризику, часто мають більш загальний характер, ніж конкретно ідентифіковані ризики.

Внаслідок того, що при використанні високорівневої оцінки ризиків рідко розглядаються технічні деталі, вона буде краще застосована до забезпечення організаційних та нетехнічних засобів контролю, а також аспектів менеджменту технічних засобів контролю або ключових і загальних технічних засобів захисту, таких, як, наприклад, антивірусні програми та резервне копіювання.

До переваг високорівневої оцінки ризику можна віднести:

- простоту підходу;
- створення стратегічної картини програми забезпечення безпеки

організації, тобто високорівнева оцінка може бути використана для допомоги у плануванні;

- можливість раціонально і ефективно розподіляти ресурси та фінанси;
- можливість визначати системи, які в першу чергу потребують захисту.

Однак високорівнева оцінка ризиків має і недолік: внаслідок того, що початковий аналіз ризиків акцентує увагу на найбільш небезпечних ризиках, зменшується точність отриманих результатів, і це призводить до того, що деякі бізнес-процеси та системи, які дійсно потребують більш детальної оцінки ризиків, не будуть виявлені. Цього недоліку можна уникнути в разі наявності повної та достовірної інформації про всі аспекти організації, її інформації та системи.

Після того, як було проведено високорівневу оцінку ризиків, приймається рішення щодо необхідності проведення детальної оцінки для ідентифікації потенційних ризиків. Така оцінка необхідна у разі, якщо відсутність контрзаходів може призвести до значних несприятливих наслідків для організації, її бізнес-процесів і активів.

До дій, які входять до детальної оцінки ризиків ІБ, відносять: визначення цінності активів, оцінку загроз та оцінку вразливостей стосовно обраних активів. Отримані результати використовують для отримання значення ризиків і вибору стратегії обробки ризиків.

На відміну від високорівневої оцінки ризиків детальна оцінка потребую значної кількості часу та зусиль, а також компетентності з боку співробітників, які проводять оцінку, та керівництва організації.

З точки зору застосованого апарату всі підходи до оцінки інформаційних ризиків можна умовно розділити на кількісні, якісні та напівкількісні. [23]

Якісні підходи зазвичай базуються на описових (номінальних) або ранжируваних (порядкових) шкалах для наслідків та ймовірностей. Вони використовуються тоді, коли немає можливості отримати кількісні дані про об'єкт оцінки. В такому випадку об'єкту оцінки присвоюється показник, який зазвичай оцінюється за трибальною (низький, середній, високий), п'ятибальною чи десятибальною шкалою.

Для збору даних в якісному методі застосовуються опитування цільових груп, інтерв'ювання, анкетування тощо. В процесі аналізу ризиків необхідно залучати співробітників, які компетентні в тій галузі, в якій розглядаються ризики.

Етапи якісної оцінки ризику наведено на рис. 2.1 [24].

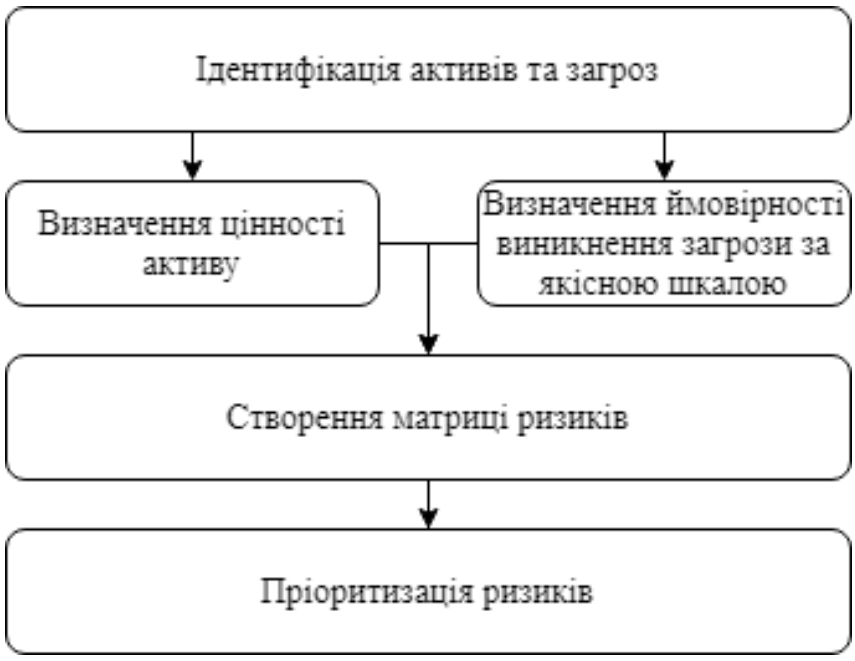

Рис. 2.1. Етапи якісної оцінки ризиків

Якісний аналіз ризику виконує 3 основні функції [25]:

- визначає пріоритети ризиків на основі впливу та ймовірності;

- визначає основні області, які схильні до ризику;
- покращує розуміння ризиків співробітниками організації.

В організації може бути наявна велика множина ризиків, але буде недоцільно реагувати на всі з них. До того ж, іноді заходи, спрямовані на зменшення впливу ризику, можуть коштувати більше, ніж сам ризик. Це пояснює першу функцію якісного аналізу: необхідно визначити пріоритети для розгляду найбільш значних ризиків. Визначення схильних до ризику областей досягається шляхом знаходження і категоризації ризиків за їх джерелом. Це може знадобитися для визначення пріоритетів активів та процесів організації і для графіку їх обробки.

У зв'язку зі своєю відносною простотою якісний аналіз зрозумілий для ризик-менеджерів організації. Як наслідок з цього, може покращитися ефективність обробки ризиків та визначення резервного бюджету на випадок виникнення інцидентів ІБ.

До переваг якісного підходу до оцінки і аналізу ризиків можна віднести, по-перше, його простоту використання. Це означає, що немає необхідності в спеціальному навчанні команди ризик-менеджерів, оскільки якісний метод не використовує складні інструменти аналізу та програмне забезпечення. Також метод потребує менше фінансових витрат і витрат часу. Оскільки метод класифікує ризики лише за ймовірністю та впливом, це дозволяє легко визначити, на які ризики слід звернути увагу, тобто легше здійснюється пріоритизація ризиків.

До основних недоліків якісного підходу можна віднести, по-перше, суб'єктивність, оскільки через те, що даний підхід не забезпечує якихось кількісних значень, він залежить від думки та досвіду того, хто його проводить. Для мінімізації суб'єктивності оцінки рекомендується залучати декількох людей до якісного аналізу ризиків, бажано з вдалим минулим досвідом проведення такого аналізу, оскільки команда без досвіду може не врахувати деякі дійсно важливі ризики чи дати їм неадекватну оцінку. Іншим недоліком є недостатність розмежування ризиків. Це означає, що якщо після пріоритизації ризики потрапляють до однієї категорії, наприклад, до категорії некритичних ризиків з високою ймовірністю та

малим впливом, складно далі оцінити і вирішити, який з цих ризиків необхідно оброблювати першим. Також якісний аналіз ризиків може оцінити окремо кожний ризик, але не надати оцінку ризику для організації в цілому. І останнє, не можна буде визначити, скільки фінансових ресурсів буде необхідно для обробки ризику та іншої діяльності з його управління.

В результаті якісний аналіз дає значення оцінки можливості прийняття результату ризикової події. Після цього за необхідності здійснюється кількісний аналіз для більш детального розгляду конкретних обраних ризиків.

Кількісні підходи використовуються для вимірювання наслідків та ймовірностей, виражених в числових шкалах, у вигляді діапазонів та розподілів, тобто коли їх можна представити у вигляді кількісних значень, виражених у відсотках, грошах, людських ресурсах, часі тощо. У випадку кількісної оцінки ризиків необхідно враховувати розмірність значень та визначити одиниці виміру для використання в оцінці.

При кількісному підході всім елементам оцінки присвоюються конкретні реальні кількісні значення. Об’єктом оцінки може бути цінність активу в грошовому виразі, ймовірність реалізації загрози, збиток від реалізації загрози, вартість захисних засобів.

При кількісному підході спочатку ідентифікуються загрози, активи, вразливості. Для цього можна використовувати асоціативні карти (mind maps), анкетування, інтерв’ювання, аналіз документації, SWOT-аналіз. Після цього проводиться аналіз наслідків та частоти виникнення, проводиться калькуляція і оцінка ризику. Етапи кількісної оцінки зображено на рис. 2.2. [26]

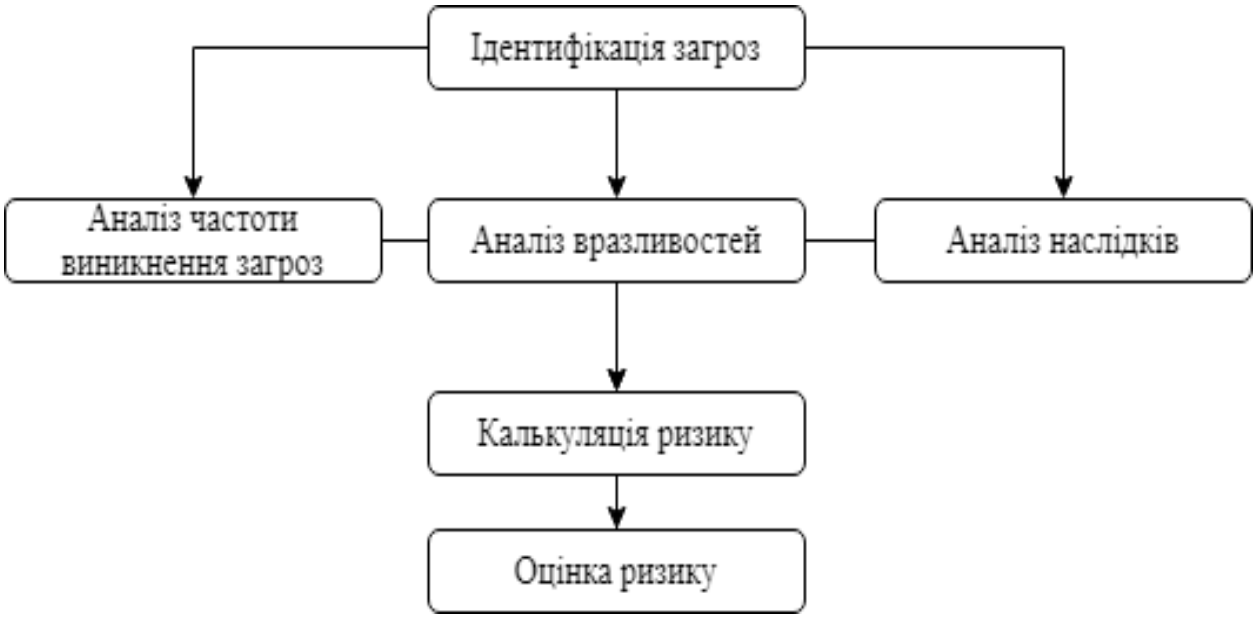

Рис. 2.2. Етапи кількісної оцінки ризиків

Першочергово доцільно буде провести легший у використанні і менш ресурсозатратний якісний аналіз ризиків, а вже після цього за необхідністю проводити кількісний аналіз. Можна побачити аналогію якісної та кількісної оцінки з високорівневою та детальною оцінкою, які були описані у стандарті ISO 27005.

2.2 Аналіз сучасних методик оцінки інформаційних ризиків

Метод CRAMM, повна назва – CCTA Risk Analysis and Management Method, був розроблений Центральним Комп'ютерним та Телекомунікаційним Агентством – британською урядовою організацією, у 1985 р.

Він був призначений для використання у великих організаціях, таких як державні органи та промисловість. [27]

Етапи методу CRAMM представлені на рис. 2.3.

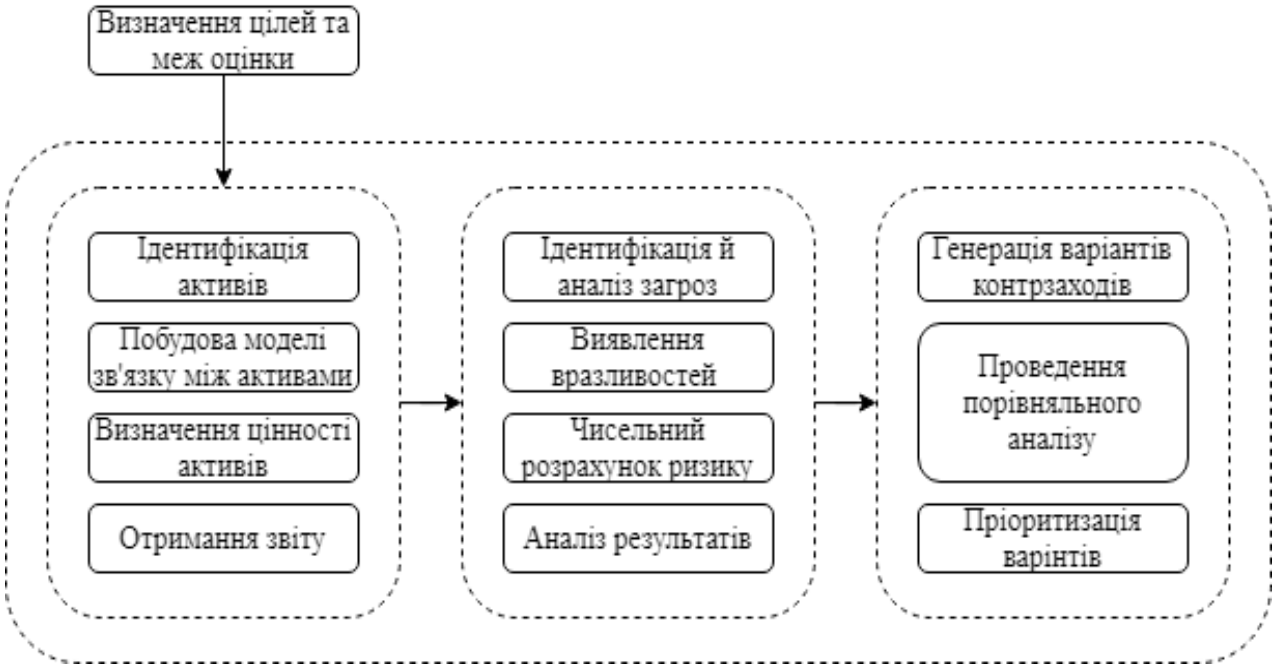

Рис. 2.3. Етапи методології CRAMM

Першим етапом є ідентифікація й оцінка активів. Після того, як було встановлено загальні цілі та межі оцінки, інформаційні, програмні та технічні активи повинні бути ідентифіковані та оцінені, зазвичай будується модель, що описує зв’язок між ними.

Цінність активів визначається, ґрунтуючись на значенні можливого збитку, який настане в разі порушення властивостей цих активів. Цінність технічних активів визначається як вартість, необхідна на їх відновлення у випадку їх знищення або пошкодження. Цінність інформаційних та програмних активів визначається у випадках, коли актив знищено (порушення цілісності) або він є недоступним протягом певного часу (порушення доступності), коли порушено конфіденційність внаслідок несанкціонованого доступу чи розголошення інформації, та коли виникають помилки, пов’язані з передачею інформації. Зазвичай для оцінки вартості активів використовується інтерв’ювання.

Результатом першого кроку буде визначення необхідності проведення повного аналізу безпеки організації.

Другим етапом є оцінка загроз і вразливостей. Він полягає у фактичній оцінці ризиків шляхом ідентифікації і аналізу потенційних загроз для системи, оцінки

вразливостей системи до виявлених загроз, і в результаті, з врахуванням знань про активи, загрози та вразливості ризик може бути розраховано. В якості вихідних даних будуть отримані ідентифіковані та оцінені ризики. На цьому кроці не передбачено застосування контрзаходів.

Третім етапом є вибір контрзаходів та створення рекомендації. На цьому етапі, використовуючи перелік вбудованих в CRAMM контрзаходів, визначаються доступні стратегії зменшення ризику і проводиться їх пріоритизація за вартістю та ефективністю впровадження. Після цього формується план обробки ризику, на основі якого буде модифікуватися інформаційна система.

До переваг даної методології можна віднести наступні фактори:

- складність оцінки може бути адаптована до вимог організації;
- процес оцінки автоматизовано в програмному забезпеченні;
- методика володіє великою базою знань для оцінки ризиків і вибору контрзаходів;
- методика може бути використана в якості засобу аудиту;
- методика буде особливо корисною великим корпоративним організаціям.

До недоліків методології CRAMM можна віднести те, що:

- використання методики потребує експертних знань та високої кваліфікації;
- повна оцінка безпеки може вимагати дуже велику кількість часу і бути надмірно складною;
- методика може бути використана лише з програмним інструментарієм.

Отже, CRAMM є універсальним методом, який дозволяє вирішувати задачі різного рівня складності. Методологія містить базу даних, яка налічує більше 3000 заходів захисту. CRAMM використовує якісний підхід, орієнтований на активи, які класифікуються за категоріями, кожна з яких має свій визначений перелік загроз та вразливостей. Після ідентифікації й оцінки активів, загроз та вразливостей інструмент CRAMM автоматично надає перелік можливих контрзаходів.

Інша методика, яка використовує якісний аналіз – це методика FRAP (Facilitated Risk Assessment Process). Методика виявляє та оцінює ризики ІБ для обраної області дослідження, якою може бути ІС організації, бізнес-процес, додаток тощо. Простота методу дозволить зрозуміти отримані результати якісного аналізу неспеціалістам. Якісний аналіз проводиться за допомогою експертної оцінки.

Процес оцінки ризику за методикою FRAP складається з 3 етапів [28]. На першому етапі, що більшою мірою є підготовчим, визначаються межі та цілі оцінки та узгоджується спосіб, згідно з котрим будуть визначатися пріоритети ризику. Також приймається рішення щодо активів, які слід врахувати при проведенні аналізу.

Другий етап являє собою власне оцінку ризиків, які ідентифікуються та визначається їх рівень, враховуючи частоту виникнення загрози. На цьому етапі можна використовувати статистику та мозковий штурм.

На третьому етапі формуються звіти, в котрих надано перелік ризиків, а також рекомендації, як ці ризики може бути зменшено.

Методика FRAP не надає технічних подробиць, як проводити оцінку, тому значна роль при застосуванні цього методу приділяється вибору ведучого, який буде керувати процесом оцінки, використовуючи наявні в нього знання та досвід, а також більш технічні методики.

Згідно з даною методикою, немає необхідності в точному кількісному розрахунку ризиків, оскільки вважається, що це економічно неефективно через складність і велику кількість часу, необхідного на проведення кількісного аналізу, тому оцінки ризиків визначаються та для них встановлюються пріоритети лише за якісною шкалою.

В якості прикладу для визначення пріоритетів ризику може бути використана матриця ризиків, параметри якої виражені за трибальною шкалою [29]: ймовірність виникнення загрози може бути низькою, середньою та високою, так саме як і вплив від реалізації загрози. Матриця ризиків задає правила, за допомогою яких визначається рівень ризику (рис. 2.4).

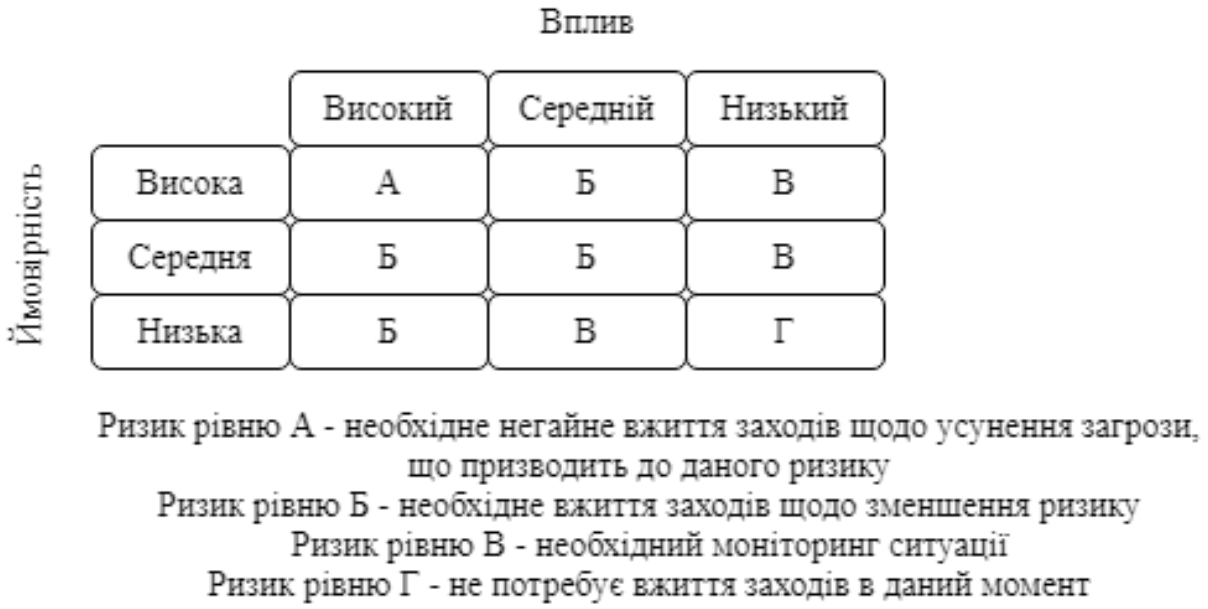

Рис. 2.4. Матриця ризиків

Для проведення аналізу ризиків методом FRAP необхідно 4 години часу та група від 7 до 15 чоловік, без необхідності залучення великої кількості зовнішніх консультантів: більша частина групи може складатися з співробітників і менеджменту організації, в якій проводиться аналіз ризиків. Використання методики передбачає дотримання припущення, що заходи захисту ще не впроваджені, і тому немає сенсу враховувати вразливості, викликані відсутністю цих заходів захисту.

До переваг методики можна віднести:

- простоту і швидкість виконання;
- відсутність необхідності залучення зовнішніх експертів, оскільки більша частина етапів процесу може бути виконана співробітниками організації, навіть якщо вони не є спеціалістами в галузі ІБ, як наслідок – мінімізація витрат на організацію процесу;
- бізнес-орієнтований підхід, що дає результати, актуальні для зацікавлених сторін.

Недоліки методу включають:

- високу залежність вдалого аналізу ризиків від ведучого, який повинен володіти достатньою інформацією про бізнес та ІБ, а також повинен вміти досконало вести переговори;
- відсутність регламентованого процесу УРІБ, відсутність допоміжних матеріалів, наприклад, каталогів загроз, вразливостей, наслідків реалізації загроз і контрзаходів;
- появу труднощів при економічному обґрунтуванні інвестиції на впровадження заходів захисту внаслідок неможливості проведення кількісної оцінки ризиків ІБ;
- найкраща ефективність методу буде досягнута не самостійно, а в поєднанні з іншою підходящою методикою.

Отже, даний метод застосовується для того, щоб якісно оцінити ризики ІБ організації. Метод FRAP буде більш доцільним для використання організаціям, які тільки здійснюють початкове впровадження процесів управління ризиками та ще не мають необхідності чи можливості розширювати їх до рівня всієї організації.

Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) була розроблена в університеті Карнегі-Меллон, для використання всередині організації. Вона може бути використана в організаціях, різних за розміром та сферою діяльності завдяки своїм модифікаціям – OCTAVE-S і OCTAVE-Allegro.

Методологія OCTAVE [30] у своїй початковій реалізації призначена для організацій з 300 чи більше співробітниками. Процес оцінки може здійснюватися власними силами організації, але є можливість залучати зовнішніх експертів для вирішення специфічних питань.

Даний метод складається з трьох етапів, які містять 8 процесів. На кожному з кроків може бути проведено один чи більше внутрішніх семінарів.

Перед проведенням першого етапу необхідно визначити першочергових та другорядних учасників процесу, визначити ролі та відповідальності, визначити

межі оцінки та бюджет, яке керівництво може виділити на оцінку та подальші дії стосовно ризиків.

Алгоритм оцінки ризиків згідно даної методології представлено на рис. 2.5.

Рис. 2.5. Етапи методу OCTAVE

На першому етапі, визначивши знання топ-менеджменту та співробітників організації стосовно важливих активів, загроз та вразливостей, вимог безпеки та наявних заходів захисту, створюються профілі загроз.

На другому етапі проводиться перевірка інформаційної інфраструктури організації з метою виявити технологічні вразливості, які можуть призвести до несанкціонованих дій стосовно критичних активів.

На третьому етапі розроблюються стратегії захисту та плани з метою знизити рівень ідентифікованих ризиків для критичних активів організації. Для цього проводиться аналіз ризиків шляхом визначення впливу загроз на критичні активи організації, створення критеріїв для оцінки цього впливу та власне оцінка впливу з використанням цих критеріїв. В результаті буде отримано профіль ризиків для кожного з критичних активів. Вже на основі отриманих даних розроблюються та

обираються стратегії захисту, які повинні бути схвалені топ-менеджментом організації.

До переваг методу можна віднести:

- його самостійність, оскільки оцінка може бути проведена відносно невеликою групою співробітників організації і не вимагає залучення зовнішніх експертів;
- його гнучкість та адаптованість: може використовуватися в різних за розміром і сферою діяльності організаціях завдяки наявності в методиці трьох методів – OCTAVE, OCTAVE-S і OCTAVE-Allegro;
- велику кількість супровідної документації.

Основним недоліком є складність оригінального методу з використанням великої кількості процесів.

Наступна методика оцінки і аналізу ризиків була розроблена компанією RiskWatch [31]. Наразі вона використовується в її програмних засобах. Для оцінки ризиків в даному методі використовується такі критерії, як очікувані річні втрати та оцінка повернення інвестицій (ALE – Annual Loss Expectancy та ROI – return on Investment відповідно). Згідно з методикою розраховується співвідношення значення наслідків реалізації загроз ІБ і ресурсів, необхідних на створення системи захисту. Процес аналізу ризиків представлено на рис. 2.6.

Рис. 2.6. Етапи методу RiskWatch

На першому етапі здійснюється підготовка до проведення аналізу: описується структура організації, склад досліджуваної системи, вимоги до інформаційної безпеки тощо. З переліку категорій активів, наявних в програмному забезпеченні RiskWatch, обираються ті, якими володіє організація та які потребують захисту. Перелік також можна доповнювати та модифікувати самостійно.

На другому етапі проводиться більш детальний розгляд системи, визначаються критичні активи, наслідки від реалізації загроз стосовно цих активів, вразливості тощо. Для цього в програмному забезпеченні пропонується відповісти на перелік питань стосовно категорій активів організації. Далі визначається цінність кожного активу, частота реалізації загроз та рівень вразливостей. Ґрунтуючись на отриманих даних, в результаті буде розраховано ефективність використання різноманітних елементів контролю ІБ.

На третьому етапі проводиться оцінювання ризику, тобто його кількісна оцінка. Для цього використовуються знання, отримані на попередніх етапах, і встановлюються зв’язки між активами, загрозами, вразливостями та втратами. Далі значення кожного ризику розраховується як математичне очікування збитків за рік за формулою (2.1).

$$M = P \cdot V, \tag{2.1}$$

де P – частота реалізації загрози протягом року;

V – вартість активу, стосовно якого реалізовано загрозу.

Одразу після цього моделюються сценарії, які передбачають розгляд аналогічних подій, але з впровадженням конкретних заходів захисту. Як результат, будуть отримані середні прогнозовані значення витрат з використанням заходів захисту та без них. Ці значення можна буде порівняти та зробити висновок щодо економічної доцільності впровадження тих чи інших заходів захисту.

На останньому етапі формується перелік звітів. До цього переліку входять короткі підсумки, детальні та поверхневі звіти про активи, звіт про їх вартість та

збитки внаслідок реалізації загроз, звіт про контрзаходи та результати аудиту безпеки.

Метод RiskWatch є одним із найбільш всебічних, але у той же час і одним з найдорожчих інструментів оцінки ризиків. Для отримання адекватних результатів внаслідок використання програмного засобу необхідне хоча б базове навчання користувачів і базові розуміння та практика в галузі ризик-менеджменту й інформаційних технологій.

Переваги даного методу включають:

- можливість проведення як якісної, так і кількісної оцінки ризиків;
- наявність великої бази даних, яка містить інформацію про категорії активів, загрози, вразливості та контрзаходи;
- можливість модифікувати та адаптувати базу даних під потреби своєї організації;
- можливість вибору та налаштування звітів;
- проведення поглибленого детального аналізу ризиків.

Наступний метод, CORAS, є інструментом для аналізу ризиків критично важливих систем. Його початкова мета була у створенні практичного фреймворку та комп’ютеризованої підтримки для точної, однозначної та ефективної оцінки ризиків критично важливих систем.

Згідно з методом оцінка ризиків виконується за 8 кроків, які представлені на рис. 2.7.

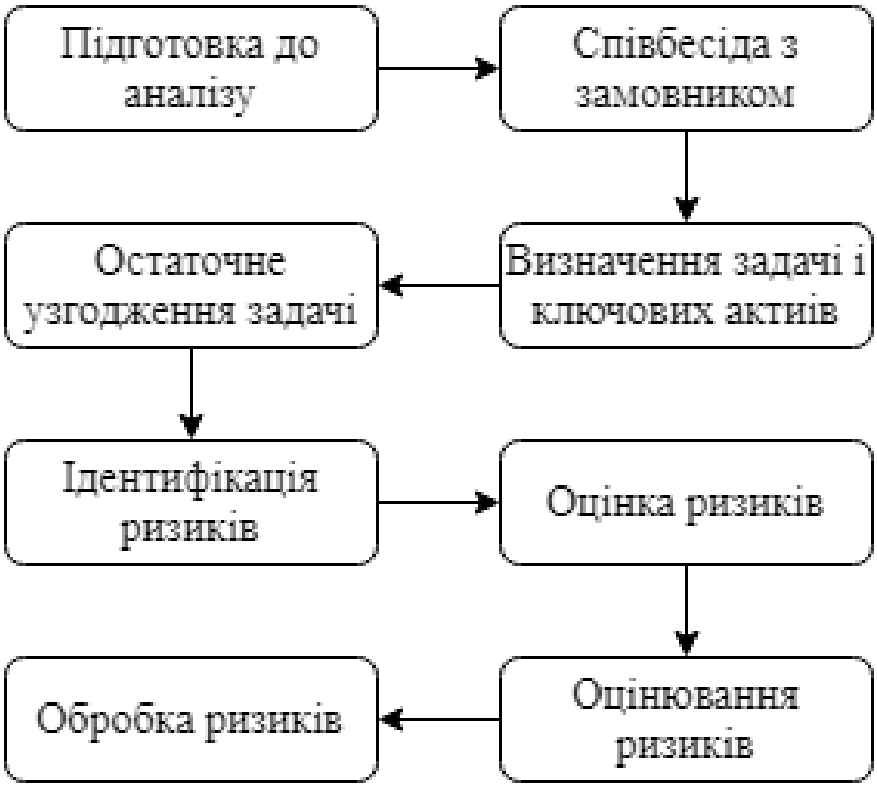

Рис. 2.7. Етапи методу CORAS

Перший крок, як і в більшості раніше розглянутих методів, є підготовчим. На цьому етапі визначаються цілі оцінки ризиків та необхідна глибина аналізу.

На другому етапі проводиться співбесіда з організацією-замовником. В процесі обговорення досягається взаєморозуміння сторін з приводу загальних цілей і планів, а також цілей, спрямованості і меж оцінки.

На третьому етапі, після проведення співбесіди і аналізу документації, аналітик описує задачу. Визначаються основні активи, що потребують захисту, проводиться високорівневий опис ключових загроз, сценаріїв інцидентів.

На четвертому етапі виконується перевірка коректності та повноти залученої до розгляду документації. Визначаються критерії оцінювання ризику для кожного з активів.

На п’ятому етапі вживаються заходи з ідентифікації ризиків, а саме ідентифікація загроз та інцидентів ІБ, сценаріїв загроз, вразливостей стосовно кожного активу.

На шостому етапі визначаються рівні ризику, які виникають при конкретному інциденті ІБ, які були розглянуті на минулому етапі.

На сьомому етапі здійснюється розподіл ризиків на допустимі та ті, які необхідно оцінити більш детально і можливо вжити стосовно них певні способи обробки ризиків.

Восьмий етап є завершальним і являє собою дії з ідентифікації та аналізу методів обробки. Критичні ризики повинні бути проаналізовані з метою визначення способів зменшення їх рівня, які обираються на основі вартості способу обробки.

До переваг методу можна віднести:

- безкоштовну підтримку інструменту;
- сприяння постійній комунікації та співробітництву з зацікавленими сторонами;
- детальне опрацювання, яке дозволяє використовувати метод для критично важливих з точку зору безпеки систем та великих організацій.

Недоліки методу включають:

- метод вимагає наявності певних експертних знань з різних галузей діяльності;
- оцінка ризиків даним методом може займати велику кількість часу;
- даний метод більше не оновлюється.

2.3 Методи чисельного розрахунку величини ризику

Найбільш поширеною на практиці є якісна оцінка ризиків, суть якої полягає у визначенні значень параметрів ризику за деякими, сформованим заздалегідь, якісним шкалами. Це може бути ймовірність реалізації загрози, ймовірність використання уразливості і величина збитку. Класичним прикладом шкали є трирівнева шкала оцінки параметрів ризику, який може набувати таких значень: «високий», «середній» і «низький».

Однак якісна оцінка не дозволяє аргументувати розмір інвестицій в інформаційну безпеку і сформувати раціональний комплекс заходів захисту. Одна з причин широкого застосування якісної оцінки ризику – труднощі в проведенні кількісної оцінки, обумовлені відсутністю конкретних вимог до складу початкових даних, правил оцінки та достатньої кількості статистичних даних.

Кількісна оцінка ризику R в найпростішому випадку розраховується за формулою (2.2).

$$R = p \cdot q, \tag{2.2}$$

де p – ймовірність ризикової події;

q – розмір збитку.

Зазвичай під ризиковою подією мається на увазі реалізація загрози. При кількісній оцінці ймовірність реалізації загрози може набувати значень в інтервалі від 0 до 1 та визначається за допомогою експертних, статистичних та інших методів. Прогнозування ймовірності ризикових подій з належною точністю є трудомістким завданням, тому отримати точну кількісну оцінку доволі важко. Однак об’єктивна кількісна оцінка ризиків дозволить покращити якість вибору заходів захисту для ІС організації.

При кількісній оцінці ризику величина збитку в результаті реалізації загрози набуває вартісних показників. Оскільки ймовірність – це безрозмірна величина, одиниці виміру ризику відповідають обраній одиниці виміру збитку.

Під час оцінки величини збитку від реалізації загрози необхідно враховувати наслідки, які можна розділити на матеріальні (фінансові) та нематеріальні (репутаційні, шкода навколишньому середовищу тощо). Для цього повинні бути задіяні профільні спеціалісти, такі як юристи, економісти, екологи, спеціалісти з ІБ тощо.

Якщо ймовірність ризиковою події розділити на дві складові – ймовірність реалізації загрози та ймовірність використання відповідної вразливості – то

формула (2.2) буде записана в більш деталізованому вигляді. В літературі, присвяченій питанням ІБ, можна зустріти таку формулу (2.3) [32,33].

$$R = p_t \cdot p_{\text{v}} \cdot q, \tag{2.3}$$

де p_t – ймовірність виникнення загрози;

p_v – ймовірність використання вразливості.

Формулу (2.3) можна ще точніше деталізувати шляхом додавання показників, що характеризують ефективність реалізованих заходів захисту (2.4) [34].

$$R = p_t \cdot (1 - E_v) \cdot p_v \cdot (1 - E_q) \cdot q, \tag{2.4}$$

де E_v – ефективність заходів захисту, що направлені на попередження вразливості;

E_q – ефективність заходів захисту, що направлені на мінімізацію наслідків.

Формули (2.2)-(2.4) застосовуються, якщо ризик визначається для однієї загрози чи вразливості. Припустимо, що модель загроз безпеки інформаційної системи підприємства складається з *K* елементів та має *X* загроз та *Y* вразливостей. Загроза може бути реалізована внаслідок використання однієї й тієї ж самої вразливості. Якщо припустити, що дані вразливості незалежні, то ймовірність порушення безпеки *k*-го елемента інформаційної системи в результаті реалізації *x*-ої загрози $p(k \mid x)$ можна розрахувати за формулою (2.5):

$$p(k \mid x) = p_t(x) \cdot \left(1 - \prod_{y=1}^{y} (1 - p_v(x \mid y))\right), \tag{2.5}$$

де $p_t(x)$ – ймовірність виникнення *x*-ої загрози;

$p_v(x \mid y)$ – ймовірність використання *y*-ої вразливості *x*-ою загрозою.

Якщо припустити, що загрози незалежні, то ризик безпеки *k*-го елементу інформаційної системи підприємства *R(k)* може бути розрахований за формулою (2.6):

$$R(k) = \sum_{x=1}^{x} p(k \mid x) \cdot q(k), \tag{2.6}$$

де *q(k)* – розмір збитку від порушення безпеки *k*-го елементу інформаційної системи підприємства.

Формула (2.6) має вагомий недолік – в ній багаторазово враховуються однакові наслідки, що настають при реалізації різноманітних загроз. Наприклад, пошкодження серверу може бути викликано пожежею, затопленням, фізичним впливом з боку людини, неправильною експлуатацією тощо. При цьому значення ризику, розрахованого за формулою (2.6), може бути більшим за реальний збиток від пошкодження серверу.

Якщо припустити, що реалізація загроз призводить до однакових наслідків, то ризик безпеки елементу інформаційної системи підприємства можна розрахувати за формулою (2.7):

$$R(k) = \left(1 - \prod_{x=1}^{x} (1 - p(k \mid x))\right) \cdot q(k), \tag{2.7}$$

Формула (2.7) нечасто застосовується, оскільки, як правило, різні загрози призводять до різних наслідків.

У випадку, якщо розмір збитку визначається окремо для порушення кожного з властивостей безпеки елементу інформаційної системи підприємства, ризик може бути розрахований за формулою (2.8) [35]:

$$R(k) = p(k_c) \cdot q(k_c) + p(k_i) \cdot \ q(k_i) + p(k_a) \cdot \ q(k_a), \tag{2.8}$$

де $p(k_c)$, $p(k_i)$, $p(k_a)$ – значення ймовірності порушення конфіденційності, цілісності та доступності k-го елементу інформаційної системи відповідно;

$q(k_c)$, $q(k_i)$, $q(k_a)$ – значення розміру збитку, що настає при порушенні конфіденційності, цілісності та доступності k-го елементу інформаційної системи відповідно.

Повний ризик R_{IS} визначається як сума ризиків безпеки елементів інформаційної системи до впровадження заходів захисту (2.9):

$$R_{IS} = \sum_{k=1}^{k} R(k), \tag{2.9}$$

В методиці оцінки ризиків компанії Microsoft [36] та методиці RiskWatch [31] замість показника ризику використовується показник *ALE (Annual Loss Expectancy)*, який розраховується за формулою (2.10):

$$ALE = AssetValue \cdot ExposureFactor \cdot Frequency, \tag{2.10}$$

де *Asset Value* – вартість елементу інформаційної системи;

Exposure Factor – коефіцієнт впливу, що характеризує, яка частина від вартості елементу інформаційної системи піддається ризику (у відсотках);

Frequency – частота реалізації загрози.

Показник *ALE* також можна розрахувати за формулою (2.11):

$$ALE = ARO \cdot SLE, \tag{2.11}$$

де *ARO (Annualized Rate of Occurrence)* – очікувана річна частота реалізації загрози;

SLE (Single Loss Expectancy) – очікуваний одиничний збиток, який визначається як різниця початкової вартості елементу інформаційної системи та його залишкової вартості після реалізації загрози.

Таким чином, розглянувши формули ризику (2.2)-(2.9) та наближеного до нього показника *ALE* (2.10) і (2.11), можна виділити дві основні складові ризику ІБ:

- ймовірність або частота виникнення ризикової події (реалізації загрози, порушення властивостей елементу інформаційної системи);
- розмір збитку внаслідок виникнення ризикової події.

Висновки до другого розділу

У другому розділі було проаналізовано якісні та кількісні підходи до оцінки ризиків ІБ, було проведено аналогію с високорівневою та детальною оцінкою ризиків. Було визначено, що в більшості випадків на практиці застосовується якісна оцінка ризиків завдяки простоті і швидкості у використанні та відсутності жорстких вимог до кваліфікації співробітників та бюджету організації. Вона дозволяє виявити необхідність у подальшій кількісній оцінці ризиків ІБ.

Також були розглянуті загальновизнані методики та інструменти аналізу та оцінки ризиків, такі як RiskWatch, CRAMM, OCTAVE, CORAS та FRAP. Було визначено, що найбільш точну оцінку можна отримати завдяки комбінуванню якісною та кількісної оцінки ризиків. Хоча більшість методик схожа за алгоритмом дій, які виконуються на кожному етапі, всі вони мають різний рівень складності аналізу, різні вимоги, і, відповідно, в результаті дають різну точність оцінки. Вибір конкретної методики залежить від розміру організації, її цілей, бюджету та кваліфікації співробітників та топ-менеджменту. Велика кількість технік оцінки ризиків, які використовуються в даних методиках, описана у додатках стандарту IEC 31010:2019.

Було розглянуто формули для знаходження кількісного значення величини ризику. Вони можуть бути застосовані, якщо в наявності є достатня кількість достовірної інформації про активи організації, їх цінність, частоту реалізації загроз протягом певного проміжку часу, прогнозовану ймовірність реалізації, дані про наявні технічні й організаційні вразливості та можливі наслідки їх використання. Цю інформацію можна отримати експертним та статистичним шляхом. Як можна побачити, чим точніша оцінка ризику необхідна, тим більше початкових даних потребує аналіз.

Розділ 3 ДОСЛІДЖЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ І МЕТОДИК ОЦІНКИ РИЗИКІВ В ОРГАНІЗАЦІЇ

3.1 Підготовка організації до проведення дослідження

В якості прикладу було розглянуто АТ “Альпарі Банк”. Було проведено якісну оцінку наявних ризиків та обрано стратегії їх обробки з рекомендаціями щодо зменшення їх величини. Також було надано рекомендації з вдосконалення процесу управління ризиками.

3.1.1 Характеристика організації

АТ “Альпарі Банк” – це універсальний банк, який пропонує свої послуги фізичним особам, приватним підприємництвам та корпоративному бізнесу. Розташований в м. Києві за адресою вул. Тарасівська, 19. Клієнтами банку є українські та іноземні юридичні та фізичні особи. Їх обслуговування здійснюється відповідно до чинного законодавства України. Базу клієнтів банку становлять представники сучасного високодохідного бізнесу разом з фізичними особами середнього і більшого достатку.

Банк переслідує такі цілі, як забезпечення стабільної клієнтської бази та зростаючої кількості операцій на ринку банківських послуг, розміщення банківських коштів в реальний сектор економіки та державні цінні папери, видача мікрокредитів фізичним особам, забезпечення збільшення капіталізації та інвестиційної привабливості банку, збільшення долі на банківському ринку та покращення якості кредитно-інвестиційного портфеля.

Банк планує в найближчі п’ять років стати повноцінним фінансовим супермаркетом, який пропонує клієнтам як власні сервіси, так і партнерські продукти, а також прагне забезпечити повнофункціональний дистанційний електронний офіс обслуговування клієнтів з використанням мобільних технологій та Інтернет-банкінгу.

Найвищим органом управління банку є Загальні збори акціонерного товариства. Постійно діючим колегіальним виконавчим органом управління, що здійснює поточну діяльність, є Правління банку, яке призначається рішенням Наглядової ради в кількості не менше трьох чоловік. Наглядова рада здійснює контроль над діяльністю Правління банку, захищає права вкладників, кредиторів та акціонерів банку. Члени Наглядової ради обираються Загальними зборами акціонерного товариства з числа акціонерів або їх представників і незалежних членів. Керівництвом банку є Голова Правління Мельник П. П. та Голова Наглядової ради Ющенко В. А.

3.1.2 Дослідження за допомогою SWOT-аналізу

SWOT-аналіз передбачає оцінку внутрішніх та зовнішніх факторів, які мають вплив на організацію. За допомогою цього методу можна буде визначити сильні та слабкі сторони, а також виявити потенційні загрози та можливості.

Сильні (S) та слабкі (W) сторони можна легко оцінити, оскільки вони належать до внутрішніх факторів, в яких організація повинна бути обізнана, якщо вона зацікавлена в успішності свого бізнесу. Зазвичай враховують такі області, як фізичні активи (споруди, приміщення, обладнання), фінансові активи (всі можливості отримання прибутку), людські активи (співробітники організації та цільова аудиторія), поточні процеси (всі процеси, які наявні в компанії, наприклад,

мотиваційні програми, програми навчання та підготовки фахівців, система ієрархії підрозділів тощо). Першочергово необхідно оцінити саме сильні та слабкі сторони, а вже потім переходити до загроз та можливостей, на які впливають в основному зовнішні фактори.

Для визначення сильних сторін необхідно виявити переваги банку над конкурентами, зрозуміти, що подобається клієнтам та знайти способи збільшення прибутку. Для визначення слабких сторін, відповідно, необхідно знайти недоліки у порівнянні з конкурентами, виявити процеси, які можна покращити, та ситуації, яких слід запобігати, а також можна отримати зворотній зв'язок від клієнтів щодо слабких сторін банку.

Після визначення внутрішніх факторів можна переходити до зовнішніх. Зовнішні фактори зазвичай непідконтрольні жодній організації. Їх можна класифікувати за такими категоріями, як стан ринку (створення нових технологій, продуктів тощо, зміна потреб цільової аудиторії), фінансування, демографічні дані, стосунки з партнерами та постачальниками, політична та екологічна ситуація в країні, економічні тенденції.

До загроз слід віднести перешкоди, які трапляються в процесі діяльності, вразливості, які можуть загрожувати бізнесу та інші проблеми. До можливостей зазвичай вносяться зміни в галузі діяльності чи політичні, економічні та інші зміни, які корисні для бізнесу.

Отже, почнемо з сильних сторін. До сильних сторін АТ "Альпарі Банк" можна віднести:

- високу ефективність роботи банку, стабільність роботи з моменту створення;
- персональний підхід до кожного клієнта та гнучкість послуг, що надаються;
- швидкість в ухваленні рішень, професійна команда топ-менеджерів, зацікавлена в розширенні бізнесу;
- високу якість послуг, що надаються, наявність міцних ділових зв'язків.

До слабких сторін можна віднести:

- високу плинність кадрів нижчої ланки, наприклад, операціоністів;
- недостатню розрекламованість банку у порівнянні з конкурентами;
- недостатню мотивацію співробітників нижчої та середньої ланки.

Загрози визначаються в залежності від наявних в банку активів та будуть детально розглянуті в наступних підрозділах. В якості прикладу можливості можна навести можливість виходу банку на нові ринки, що дозволить залучити нових клієнтів та отримувати більший прибуток.

3.1.3 Оцінка існуючих ризиків, аналіз можливих ризиків

При оцінці ризиків вони першочергово повинні бути ідентифіковані. Це означає, що повинні бути ідентифіковані активи банку, загрози, що на них впливають, вразливості, та оцінена величина наслідків для активів у разі реалізації загрози.

Розглянемо перелік активів банку, які підлягають захисту, відповідальних за них осіб та визначимо ступінь важливості цих активів за десятибальною шкалою (1 – неважливий, 10 – дуже важливий) для подальшої оцінки ризиків. Ступінь важливості визначатимемо ґрунтуючись на цілях та на загальних потенційних збитках, викликаних порушенням функціонування чи знищенням активів, яких може зазнати банк.

Активи можемо розділити на такі категорії: програмне та апаратне забезпечення, інформація, людські ресурси, інфраструктура та аутсорсингові послуги.

До програмного забезпечення можна віднести такі активи, як прикладне та системне ПЗ, ПЗ для програмування та драйвери. Прикладне ПЗ може включати в себе офісні програми, текстові редактори, електроні таблиці, менеджери для роботи

з базами даних, електронну пошту тощо. До системного ПЗ відносять встановлені операційні системи, веб-сайти тощо. В загальному випадку до програмного ПЗ можна віднести ПЗ, призначене для програмування, яке містить асемблери, компілятори, редактори зв’язків, проте воно не використовується в банку, тож їх враховувати в роботі не будемо. Приклади драйверів – це драйвер для миші, принтеру, мережі тощо. В табл. 3.1 визначено відповідальних осіб та важливість активів ПЗ для банку.

Таблиця 3.1

Активи програмного забезпечення

Назва активу	Відповідальний за актив	Оцінка
Прикладне ПЗ	Системний адміністратор	7
Системне ПЗ	Системний адміністратор	10
Драйвери	Системний адміністратор	5

До апаратного забезпечення входять такі активи, як комп’ютери та периферія, носії інформації (зовнішні жорсткі диски, резервні копії тощо), сервери, мережеве обладнання (маршрутизатори, бездротові точки доступу, файрволи, Bluetooth-пристрої тощо), персональні та корпоративні комунікаційні пристрої (мобільні телефони, системи корпоративної телефонії PBX), інше апаратне забезпечення (вимірювальні прибори, сигналізації, картки тощо). Відповідальних осіб та оцінку важливості активів апаратного забезпечення надано в табл. 3.2.

Таблиця 3.2

Активи апаратного забезпечення

Назва активу	Відповідальний за актив	Оцінка
Комп’ютери	Користувач	8
Комп’ютерна периферія	Керівник ІТ-підрозділу	4
Носії інформації	Користувач	7
Сервери	Керівних ІТ-підрозділу	9
Мережеве обладнання та ПЗ	Мережевий аналітик	9
Персональні комунікаційні пристрої	Користувач	4
Корпоративне комунікаційне обладнання	Мережевий аналітик	7
Інше апаратне забезпечення	Користувач	5

Далі розглянуто інформаційні активи, такі як бази даних, контракти з партнерами, постачальниками, клієнтами тощо, веб-сторінки та веб-сайти, кореспонденція з клієнтами, керівництва та стандарти, наприклад, для навчання персоналу чи використання обладнання, внутрішні документи з планування, звітності, прийняття рішень, а також кадрові документи. Дані щодо них наведено в табл. 3.3.

Таблиця 3.3

Інформаційні активи

Назва активу	Відповідальний за актив	Оцінка
Бази даних	Адміністратор баз даних	9
Контракти	Керівник юридичного відділу	7
Веб-сторінки та веб-сайти	Системний адміністратор	7
Кореспонденція	Менеджер по роботі з клієнтами	5
Керівництва і стандарти	Старший адміністратор	5
Внутрішні документи	Старший адміністратор	7
Кадрові документи	Голова відділу кадрів	7

Серед людських активів можна виокремити топ-менеджмент (членів правління, членів Наглядової ради, керівників організаційних підрозділів), менеджерів (керівників груп, проект-менеджерів тощо), експертів (системних адміністраторів, архітекторів безпеки тощо) та звичайних співробітників. Відповідальним за них є голова відділу кадрів.

Інфраструктура включає такі активи, як споруди, меблі, сейфи, електричне обладнання, кабелі, системи фізичного захисту (камери, замки, пожежна безпека), транспортні засоби, системи опалення, вентиляції та кондиціонування. Відповідальним за ці активи є співробітник з операційних питань (Operation Officer).

Аутсорсингові послуги включають електропостачання, канали зв'язку, послуги інтернет-провайдерів, обслуговування ІС, постачання обладнання тощо. Відповідальним за ці послуги є менеджер з контрактів.

Далі наведено стислий перелік наявних та потенційних загроз, деякі з яких слід врахувати в процесі оцінки ризиків ІБ. Їх можна розділити на фізичні загрози, загрози порушення конфіденційності, цілісності та доступності інформації, витоку та несанкціонованого доступу до інформації чи активів.

Фізичні загрози включають:

- здійснення фізичного НСД до приміщень, серверних кімнат, обладнання, комплексу засобів захисту, з метою отримання можливості обходу системи захисту, а також отримання доступу до носіїв інформації, паперової документації тощо;
- крадіжку, пошкодження чи знищення комп'ютерного обладнання, носіїв інформації або паперової документації співробітниками організації або зовнішніми зловмисниками;

Внаслідок певних дій співробітників або порушників ІБ може буди розголошена та розкрита конфіденційна інформація. Загрози витоку конфіденційної інформації включають:

- прослуховування зовнішніх каналів зв'язку зловмисниками;

- витік конфіденційної інформації з мережі по каналам зв’язку, таким, як електронна пошта, чати, миттєві повідомлення тощо;
- витік конфіденційної інформації через носії інформації, мобільні пристрої, ноутбуки тощо;
- порушення конфіденційності даних, що передаються лініями зв’язку, які проходять за межами контрольованої зони, яке здійснюється зовнішніми порушниками шляхом пасивного прослуховування каналів зв’язку;
- порушення конфіденційності даних, що передаються лініями зв’язку, які проходять в межах контрольованої зони, яке здійснюється внутрішніми порушниками шляхом пасивного прослуховування каналів зв’язку з використанням спеціалізованих програмних засобів;
- перехоплення інформації, що передається каналами зв’язку, з метою її подальшого використання для обходу засобів мережевої автентифікації;
- витік конфіденційної інформації внаслідок її ненавмисного розкриття співробітниками організації;
- статистичний аналіз мережевого трафіку з боку порушника на предмет пошуку конкретної інформації, частоту та напрямок її передачі, інформацій про типи даних, що передаються тощо;
- несанкціоноване розкриття інформації, що містить дані про місцезнаходження критичних для організації або конфіденційних засобів обробки інформації;
- розкриття конфіденційної інформації підрядниками чи партнерами організації.

Для організації важливим є забезпечення безперервності бізнесу та забезпечення доступності послуг користувачам. Загрози порушення доступності сервісів та знищення інформаційних активів включають:

- атаки на систему типу “відмова в обслуговуванні”;
- недоступність ІТ-сервісів і інформації внаслідок фізичного чи логічного збою комп’ютерного чи периферійного обладнання;

- збої в мережевому обладнанні чи його пошкодження внутрішніми порушниками, пошкодження носіїв інформації;
- фізичне пошкодження ліній зв’язку внутрішніми та зовнішніми порушниками;
- знищення даних внаслідок системного збою, помилки або використання непротестованого ПЗ;
- впровадження несанкціонованого та непротестованого коду, випадкова модифікація ПЗ, збої в системах захисту;
- випадкове чи навмисне знищення критично важливої для організації інформації з боку співробітників організації та зовнішніх зловмисників;
- навмисне пошкодження ПЗ та резервних копій з боку співробітників організації;

Загрози порушення цілісності даних та їх несанкціонованої модифікації включають:

- помилки та випадкові дії користувачів, внаслідок яких була порушена цілісність даних;
- помилки технічного персоналу, внаслідок яких була порушена цілісність або була модифікована конфігурація системи;
- навмисне пошкодження цілісності та несанкціонована модифікація конфігурації системи та даних з боку співробітників організації;
- фальсифікацію записів та шахрайство, несанкціоновану модифікацію журналів аудиту;
- навмисну несанкціоновану модифікацію даних з боку зовнішніх порушників.

Загрози здійснення НСД включають:

- крадіжку ідентифікаторів користувачів з метою їх подальшого використання;
- розкриття паролів та іншою інформації, необхідної для автентифікації;
- НСД до журналів та засобів аудиту;

- підробка адрес у заголовках мережевих пакетів чи інформації канального рівня, внаслідок чого зовнішній зловмисник може бути прийнятий за легального користувача системи;
- можливість НСД з боку порушника внаслідок збоїв у роботі засобів захисту;
- НСД до веб-сайту організації, бездротової мережи, резервних копій даних;
- виявлення порушниками, як зовнішніми, так і внутрішніми, вразливих місць в ІС організації з подальшим їх використанням для здійснення НСД;
- впровадження несанкціонованого, неперевіреного та шкідливого програмного коду, логічні бомби.

Юридичні загрози включають:

- нелегальне використання ПЗ, його нелегальний імпорт або експорт;
- несанкціоноване використання матеріалів, які є інтелектуальною власністю, невідповідність вимогам законодавчою та нормативної бази;
- невиконання контрактних зобов'язань.

Для подальшої оцінки ризику необхідно виявити вразливості та розглянути їх зв'язки з загрозами, які можуть використовувати ці вразливості. Розглянемо 3 групи найбільш критичних вразливостей.

Перша група вразливостей, пов'язана з безпекою кадрових ресурсів, надана в табл. 3.4.

Таблиця 3.4

Зв'язок між вразливостями та загрозами в галузі безпеки кадрових ресурсів

Вразливість	Загроза, яка використовує вразливість
Недостатня обізнаність користувачів та їх навчання з питань ІБ	Помилки користувачів, технічного персоналу
Після звільнення співробітника в нього залишаються права доступу	НСД, розголошення конфіденційної інформації
Відсутність механізмів моніторингу	Несанкціоноване використання ПЗ

Продовження табл. 3.4

Зв'язок між вразливостями та загрозами в галузі безпеки кадрових ресурсів

Вразливість	Загроза, яка використовує вразливість
Незадоволений та немотивований персонал	Крадіжка або фізичне пошкодження обладнання та інших активів, розголошення конфіденційної інформації
Відсутність політик щодо коректного використання засобів телекомунікацій та передачі повідомлень	Несанкціоноване використання мережевого обладнання

Цей перелік можна продовжувати, оскільки персонал залишається вагомим фактором виникнення ризиків ІБ. Підбору співробітників, їх навчанню та контролю слід приділяти найбільшу увагу, адже у більшості випадків внутрішній порушник ІБ своїми діями може завдати значно більшої шкоди організації, ніж зовнішній зловмисник.

Далі розглянемо вразливості, які також певною мірою перекликаються з кваліфікацією працюючих спеціалістів в організації. В табл. 3.5 представлені вразливості, пов’язані з контролем доступу, та їх зв’язок з загрозами.

Таблиця 3.5

Зв’язок між вразливостями та загрозами в галузі контролю доступу

Вразливість	Загроза, яка використовує вразливість
Відсутність політики чистих столів та екранів	Пошкодження, втрата чи розголошення інформації
Неправильне розмежування доступу в мережі	Несанкціоноване підключення до мереж
Відсутність механізмів ідентифікації та автентифікації, неналежне управління паролями	Використання ПЗ неавторизованими користувачами, НСД, привласнення чужого ідентифікатору користувача
Відсутня чи некоректна політика контролю доступу	НСД до інформації, системам чи програмному забезпеченню
Відсутність контролю й аналізу прав доступу користувачів	Можливість НСД з боку співробітників, яких було звільнено

Далі, в табл. 3.6 надано перелік вразливостей, пов’язаних з управлінням комунікаціями та операціями.

Таблиця 3.6

Зв’язок між вразливостями та загрозами в галузі управління комунікаціями та операціями

Вразливість	Загроза, яка використовує вразливість
Неадекватне управління мережею	Перенавантаження трафіку
Відсутність процедур резервного копіювання	Втрата інформації
Складний користувальницький інтерфейс	Ненавмисні помилки користувачів
Повторне використання, крадіжка, передача засобів зберігання інформації без належної очистки	НСД до інформації, розголошення конфіденційної інформації
Незахищені з’єднання с мережами загального користування	Використання ПЗ неавторизованими користувачами

Далі сформуємо перелік основних вагомих загроз та вразливостей, що впливають на найбільш важливі для організації активи.

Системне програмне забезпечення.

1. Загроза здійснення порушником деструктивного впливу на систему шляхом експлуатації вразливостей ПЗ. Вразливістю, що впливає на ймовірність реалізації загрози, може бути слабкість механізмів аналізу ПЗ на наявність вразливостей. Загроза ймовірніше за все бути реалізована в разі відсутності перевірки на наявність вразливостей в ПЗ перед його використанням, а також у разі використання ПЗ, підтримка якого була припинена виробником.

2. Загроза завантаження нештатної операційної системи, яка полягає в підміні порушником завантажуваної ОС шляхом несанкціонованої зміни в BIOS/UEFI шляху доступу до завантажувача ОС. Вразливістю, що впливає на ймовірність реалізації загрози, може бути слабкість технологій розмежування доступу до управління BIOS/UEFI. Загроза ймовірніше за все бути реалізована в разі доступності порушнику такого параметру налаштування BIOS/UEFI, як вказання джерела завантаження ОС.

3. Загроза отримання порушником привілеїв у системі без проходження процедури автентифікації. Це може бути реалізовано внаслідок виконання дій, які порушують умови коректної роботи засобів автентифікації, наприклад, введення даних, формат яких не підтримується. Причиною загрози є наявність помилок у заданих значеннях параметрів налаштування механізмів автентифікації.

4. Загроза приведення системи до стану “відмова в обслуговуванні” полягає в можливості відмови в доступі до системи легальним користувачам внаслідок значного збільшення кількості мережевих з’єднань з системою чи при використанні недоліків реалізації мережевих протоколів. Джерелом загрози може бути як внутрішній, так і зовнішній порушник.

Сервери

1. Загроза компрометації серверів внаслідок недостатньої компетентності або неуважності адміністраторів. Причинами можуть бути несвоєчасно оновлення адміністраторами серверів та робочих станцій, нехтування журналом подій ядра системи та мережевим графіком, використання стандартних паролів.

2. Загроза знищення чи крадіжки важливої інформації з серверу внаслідок встановлення на них додатків, в яких наявні шкідливі програми.

3. Загроза “спаму” веб-серверу полягає в можливості неправомірного здійснення порушником масової розсилки різних видів повідомлень на веб-сервер без запиту з боку останнього. Вразливість, що впливає на можливість реалізації загрози, – вразливості механізмів фільтрації повідомлень, що надходять з мережі Інтернет.

Прикладне програмне забезпечення

1. Загроза підміни ПЗ полягає в можливості впровадження порушником в систему шкідливого ПЗ внаслідок того, що користувачем було завантажено та встановлено шкідливе ПЗ, замасковане під легітимне вільно розповсюджуване ПЗ. Вразливістю в даному випадку є наявність прав у співробітників організації встановлювати ПЗ, завантажене з мережі Інтернет. Причинами інциденту можуть бути некомпетентність, неуважність співробітників, а також злий намір з метою помсти чи отримання вигоди.

2. Загроза опосередкованого управління групою програм через спільно використовувані дані полягає в можливості зміни порушником алгоритму роботи групи програм, які одночасно використовують спільні дані, такі як глобальні змінні, файли конфігурації тощо), шляхом перехоплення управління над одною з них. Вразливістю є слабкість в механізмі контролю введених змін в спільні дані для кожної з програм. Загроза скоріш за все буде реалізована внаслідок вдалого перехоплення управління порушником над одною з програм в групі, програми якої використовують спільні дані.

3. Загроза некоректної реалізації політики ліцензування в хмарі передбачає можливість відмови користувачам хмарних сервісів у віддаленому доступі до ПЗ, яке вони орендують, при цьому винним є постачальних послуг.

Бази даних

1. Загроза експлуатації вразливих та неадекватно конфігурованих БД. Несвоєчасне оновлення БД та збереження початкових налаштувань може стати вразливістю для здійснення атаки проти організації. Оновлення БД часто ігнорується та відкладається внаслідок необхідності вимикати ІС, що є критично важливою для організації, на час завантаження оновлення. Як результат, оновлення може затягнутися на декілька місяців, протягом яких БД залишається вразливою.

2. Загроза крадіжки носіїв інформації, які містять резервні копії БД. Вони зазвичай не захищені належним чином, що збільшує можливість реалізації загрози. Також впливає ігнорування проведення аудиту та моніторингу дій адміністраторів з низькорівневим доступом до конфіденційної інформації.

3. Загроза отримання зловмисником необмеженого доступу до БД шляхом проведення SQL- та NoSQL-ін’єкцій. Убезпечитися від цього можна, не змішуючи формати даних.

4. Загроза розголошення конфіденційної інформації внаслідок зловживання привілеями. Наприклад, у разі, якщо співробітника звільнюють не за власним бажанням, він із міркувань помсти або отримання вигоди може вкрасти конфіденційні дані або іншим способом нанести збитків організації. Надмірні привілеї надаються користувачам випадково та залишаються після їх звільнення

внаслідок неправильно створених та використовуваних механізмів розмежування прав доступу.

Мережеве обладнання та ПЗ

1. Загроза передачі даних по прихованим каналам. Порушник може неправомірно вивести інформацію, що захищається, із системи, а також передавати керуючі команди шляхом їх прихованого розміщення у відкритих даних, що легітимно передаються мережею, маскування їх під службові протоколи або приховування їх в потоці інших даних. Спричинити інцидент може недостатність заходів захисту, спрямованих на захист від витоку інформації, а також недостатність контролю даних. Одною з причин може бути невідповідальність співробітників організації та їх недостатня обізнаність в питаннях ІБ.

2. Загроза НСД до мережевого обладнання полягає в можливості зміни шкідливими програмами алгоритму роботи ПЗ мережевого обладнання та параметрів його налаштування з використанням вразливостей в ПЗ мережевого обладнання.

3. Загроза підміни бездротового клієнту чи точки доступу полягає в можливості отримання порушником автентифікаційних та інших захищуваних даних, які передаються в ході автоматичного підключення точок бездротового доступу або клієнтського ПЗ до довірених суб’єктів мережевої взаємодії, які були підмінені порушником. Вразливість, що використовується загрозою, – слабкість механізмів автентифікації суб’єктів мережевої взаємодії при бездротовому доступі. Загроза може бути реалізована за умови, якщо порушник розмістить точку бездротового доступу з певними параметрами роботи, такими як MAC-адреса, назва, використовуваний стандарт передачі даних тощо, в зоні доступності для пристроїв бездротового доступу організації.

Комп’ютери

1. Загроза впровадження шкідливого коду внаслідок відвідування заражених сайтів у мережі Інтернет. Порушник може виявити сайти, які найчастіше відвідує користувач, зламує їх та впроваджує свій шкідливий код. Вразливості, що впливають на дану загрозу, – слабкість заходів антивірусного захисту та

відсутність правил міжмережевого екранування. Загроза може бути реалізована, якщо у співробітників організації є права на необмежений доступ до мережі Інтернет, а також якщо порушник знає найбільш відвідувані співробітниками сайти.

2. Загроза порушення роботи комп’ютеру та помилкового блокування доступу до його даних внаслідок некоректної роботи встановлених на ньому засобів захисту. Загроза може бути реалізована в тому випадку, якщо встановлені засоби захисту передбачають блокування файлів.

3. Загроза отримання привілеїв порушником в системі і отримання доступу до конфіденційної корпоративної інформації внаслідок цільової атаки на робочу станцію співробітника організації з метою визначення вразливостей, наявних в використовуваному ПЗ.

4. Загроза пошкодження, знищення чи крадіжки комп’ютерного обладнання співробітниками організації внаслідок невмотивованості, помсти чи власної вигоди, чи зовнішніми порушниками внаслідок слабкості фізичних механізмів захисту.

Далі в табл. 3.7 наведено оцінені за десятибальною шкалою експертним методом збитки для кожного з активів внаслідок реалізації кожної загрози.

Таблиця 3.7

Оцінка збитків для активів внаслідок реалізації загроз

Загрози	Збитки для активу
Системне ПЗ	
Загроза експлуатації вразливостей ПЗ	8
Загроза завантаження нештатної ОС	7
Загроза отримання поршником привілеїв у системі	9
Загроза приведення системи до стану “відмова в обслуговуванні”	7
Сервери	
Загроза деструктивних дій внаслідок некомпетентності	9
Загроза знищення чи крадіжки інформації	9
Загроза “спаму веб-серверу”	2
Прикладне ПЗ	
Загроза впровадження шкідливого ПЗ	8
Загроза перехоплення управління над програмами	7
Загроза втрати доступу до хмарних сервісів	5
Бази даних	
Загроза експлуатації вразливих місць БД	8
Загроза крадіжки носіїв інформації	7
Загроза отримання доступу до БД	8
Загроза зловживання привілеями	6
Мережеве обладнання та ПЗ	
Загроза передачі даних по прихованим каналам	6
Загроза НСД до мережевого обладнання	7
Загроза підміни точки доступу	5
Комп’ютери	
Загроза впровадження шкідливого коду	7
Загроза блокування доступу до даних	3
Загроза отримання привілеїв порушником	5
Загроза пошкодження комп’ютерного обладнання	2

Ймовірності реалізації кожної з зазначених загроз були визначені і оцінені теж за десятибальною шкалою на основі схильності організації до вразливостей та частоті реалізації подібних загроз за минулі періоди. Розподіл ймовірностей для

кожної з загроз надано в табл. 3.8. Для зручності розглянуті загрози ІБ були пронумеровані від З-1 до З-21, в такому порядку, в якому вони перелічені у табл. 3.7.

Таблиця 3.8

Розподіл ймовірностей наявних в організації загроз ІБ

З-1	З-2	З-3	З-4	З-5	З-6	З-7
3	3	4	6	5	3	8
З-8	З-9	З-10	З-11	З-12	З-13	З-14
6	5	2	4	6	4	7
З-15	З-16	З-17	З-18	З-19	З-20	З-21
4	3	3	5	2	6	7

Ґрунтуючись на даних про ймовірності реалізації загроз та оцінці наслідків для активів, можна оцінити величину ризику як добуток цих двох величин для подальшого визначення найбільш критичних і розробки плану реагування на них. Інформація занесена у табл. 3.9.

Таблиця 3.9

Оцінка величини ризиків ІБ

№	Опис ризику	R
1	Ризик того, що організація зазнає збитків внаслідок деструктивного впливу на систему у зв’язку з експлуатацією вразливостей ПЗ	24
2	Ризик, що буде підмінена порушником і завантажена нештатна ОС	21
3	Ризик отримання порушником привілеїв у системі внаслідок помилок в налаштування механізмів автентифікації	36
4	Ризик неможливості нормального функціонування внаслідок приведення системи до стану “відмова в обслуговуванні”	42
5	Ризик того, що сервери будуть скомпрометовані внаслідок недостатньої компетентності та неуважності відповідальних співробітників	45
6	Ризик того, що інформація на сервері піддасться негативному впливу внаслідок встановлення додатків, в яких наявні шкідливі програми.	27
7	Ризик того, що відносно веб-серверу буде здійснюватися “спам”	16
8	Ризик того, що використовуване співробітниками організації приладне ПЗ буде підмінено на шкідливе внаслідок завантаження безкоштовного ПЗ з мережі Інтернет.	48

Продовження табл. 3.9

Оцінка величини ризиків ІБ

№	Опис ризику	R
9	Ризик того, що порушник перехопить управління над групою програм, які використовують спільні дані	35
10	Ризик того, що організація втратить доступ до хмарних сервісів внаслідок некоректної реалізації політики в хмарі	10
11	Ризик того, що через несвоєчасне оновлення та неправильне налаштування БД порушник зможе отримати доступ до них	32
12	Ризик, що будуть вкрадені носії інформації з резервними копіями БД	42
13	Ризик того, що порушник отримає доступ до БД, використовуючи SQL- та NoSQL-ін’єкції	32
14	Ризик того, що внаслідок неправильного розмежування прав доступу звільнені та немотивовані співробітники можуть зловживати привілеями для нанесення збитку організації.	42
15	Ризик передачі інформації по прихованим каналам	24
16	Ризик, що ПЗ для мережевого обладнання буде змінено внаслідок НСД	21
17	Ризик отримання порушником захищуваних даних у випадку підміни ним точки доступу	15
18	Ризик того, що комп’ютер буде заражений шкідливим кодом внаслідок відвідування співробітниками заражених сайтів	35
19	Ризик того, що дані на комп’ютері будуть заблоковані внаслідок неправильної роботи встановлених на ньому заходів захисту	6
20	Ризик того, що робоча станція співробітника піддасться цільовій атаці, внаслідок чого порушник зможе отримати такі ж привілеї, як і власник робочої станції	30
21	Ризик того, що невмотивовані співробітники пошкодять чи вкрадуть комп’ютерне обладнання	14

Далі за допомогою матриці ризиків, зображеній в табл. 3.10, можна визначити пріоритетність ризиків. Отримаємо, що ризики, величина яких більша або дорівнює 36, потрапляють до зони критичних ризиків. Ризики, величина яких не більша 16, є допустимими. Інші ризики потрапляють до “жовтої зони”.

Таблиця 3.10

Матриця ризиків (за впливом та ймовірністю)

10										
9										
8										
7										
6										
5										
4										
3										
2										
1										
	1	2	3	4	5	6	7	8	9	10

3.1.4 Розробка плану реагування на ризики

Ризики, які потрапили до червоної зони – це критичні ризики, які повинні обов’язково бути оброблені, ризики з зеленої зони підлягають моніторингу, проте обов’язкових дій щодо їх обробки не передбачається. Ризики з жовтої зони повинні бути оброблені у випадку наявності часу та бюджету, виділеного на обробку ризиків.

В результаті було отримано, що до ризики розподілені наступним чином (номер ризику відповідає їх порядку в табл. 3.9):

- критичні ризики – Р-3, Р-4, Р-5, Р-8, Р-12, Р-14;
- некритичні ризики – Р-1, Р-2, Р-6, Р-9, Р-11, Р-13, Р-15, Р-16, Р-18, Р-20;
- допустимі ризики – Р-7, Р-10, Р-17, Р-21.

Першочергово розглядаються критичні ризики. Якщо розставити їх за пріоритетами, то в першу чергу загрозу представляють ризики, пов’язані більшою мірою з людським фактором: некомпетентністю, неуважністю, халатністю та навмисним нанесенням шкоди. Також проблемою є налаштування механізмів автентифікації та розмежування доступу. Основний акцент робиться на забезпеченні доступності сервісів та конфіденційності інформації.

Ухилитися від критичних ризиків зазвичай не є можливим без втрат для організації. Ухилення від ризику в більшості випадків може досягатися лише за умови припинення діяльності, яка призводить до виникнення ризику, що економічно недоцільно.

Витрати на передачу ризиків зазвичай не оправдовують себе через їх велику суму. Прийняти критичний ризик з подальшим компенсуванням його наслідків теж не є правильним рішенням, оскільки враховуючи його частоту реалізації та наслідки, це буде коштувати організації великої кількості фінансових та інших ресурсів.

Оптимальним рішенням буде зменшити ступінь ризику – ймовірність його виникнення та наслідки. Для цього необхідно чи впровадити додаткові заходи захисту, чи змінити щось в організаційній роботі.

В першу чергу слід дотримуватись певних правил щодо управління співробітниками організації. При прийомі на роботу нових співробітників, діяльність яких буде пов’язана з забезпеченням ІБ, обов’язково на етапі співбесіди необхідно впевнитися, що вони мають достатній рівень компетентності для посади, яку вони планують обійняти, а також в тому, що вони можуть заслуговувати на довіру на цій посаді, особливо в тих випадках, коли вона критично впливає на

діяльність всієї організації. У випадку, якщо робоча діяльність передбачає надання доступу до засобів обробки конфіденційної інформації, щодо співробітника повинна проводитися більш детальна перевірка.

Слід зазначити, що співробітники-користувачі залишаються основною мішенню зловмисників, оскільки ймовірність успіху вища при використанні зловмисником соціальної інженерії, фішингу, ніж технічної атаки. До того ж, це не потребує значної кількості фінансових та інших ресурсів, і для компрометації системи зазвичай вистачає одного розкритого облікового запису. Також самі співробітники можуть бути джерелом загрози та самостійно нанести шкоди організації. Причиною цього може бути зміна в особистому житті співробітника, що може зробити його вразливим до застосування психологічного впливу або примусу, в результаті якого він може знищувати або передавати конфіденційну інформацію конкурентам чи іншим зацікавленим у нанесенні шкоди організації сторонам. Також якщо співробітник невмотивований або ображений на керівництво чи на організацію, він так само може вкрасти, продати чи знищити інформацію, а також нанести шкоди фізичному обладнанню.

Для зменшення ступеня ризиків, пов’язаних з обізнаністю співробітників, необхідно створити політику безпеки організації, в якій буде описано допустимі дії користувачів. В процесі призначення на посаду нові співробітники повинні бути ознайомлені з персональною відповідальністю за дотримання правил, описаних у політиці безпеки організації.

Обов’язковим є регулярне проведення перепідготовки співробітників з питання інформаційних ризиків, які стосуються організації та співробітників, під час їх роботи та під час дозвілля. Співробітників, які займаються питанням інформаційної безпеки, слід мотивувати на їх розвиток. Можна створити механізми для перевірки ефективності навчання з питань інформаційної безпеки, яке слід проводити для всього персоналу. Цей механізм працюватиме, базуючись на зворотному зв’язку.

Іншим важливим аспектом, який також напряму стосується співробітників організації, є політика контролю доступу. Вона повинна бути актуальною та

вдосконалюватися. Найбільш поширеними і вдалими принципами контролю доступу на основі ролей є принципи “знає той, хто повинен знати”, коли співробітникам надається доступ тільки до тієї інформації, яка їм необхідна для виконання своїх службових обов’язків, та принцип “доступ за необхідності”, коли співробітникам надається доступ тільки до тих засобів обробки інформації, які необхідні їм для виконання службових обов’язків.

Також слід зазначити, що користувачі можуть отримувати доступ тільки до тих мереж та мережевих служб, до яких в них є доступ, оскільки несанкціоноване або незахищене підключення до мережевих служб може спричинити негативний вплив для всієї організації. Особливо важливо контролювати цей процес для мережевих з’єднань критично важливих для бізнесу додатків, а також для користувачів, які знаходяться в місцях з високим рівнем ризику.

Для надання користувачам прав доступу вони повинні бути зареєстровані за допомогою певного ідентифікатору. Завдяки цьому ідентифікатору можуть відстежуватися дії користувача та у випадку спричинення ним неправомірних дій стосовно організації він понесе відповідальність. Також обов’язково необхідно забезпечити негайне блокування або видалення ідентифікаторів користувачів, які вибули чи були звільнені з організації з метою попередження отримання ними доступу до ІС організації в майбутньому. Також слід виявляти та видаляти неактуальні ідентифікатори та в жодному разі не призначати їх іншим користувачам. Права доступу повинні періодично переглядатися та оновлюватися через певні проміжки часу, а також у разі підвищення співробітника чи при його переході на нову посаду всередині організації, звільненні, а також переході на нижчу посаду. Всі права доступу повинні призначатися лише після авторизації користувачів.

Щодо привілейованих прав доступу, то вони обов’язково повинні бути призначені по мінімуму, але щоб їх було достатньо для виконання функціональних задач. Повинен проводитися постійний моніторинг процесу призначення привілейованих прав доступу для переконання в тому, що привілеї відповідають службовим обов’язкам співробітників, які ними володіють. Привілейовані права

доступу повинні переглядатися частіше від звичайних для того, щоб переконатися в тому, що користувачі не отримали привілеї несанкціонованим чином. Також повинні бути визначені вимогу до тривалості дії цих прав доступу.

Одною з проблем порушення ІБ, яка виникає також внаслідок дій користувачів, є недостатня складність використовуваних паролів. Для зменшення ймовірності загроз, пов’язаних з подібними вразливостями, повинна бути застосована система керування паролями. Вона передбачає обов’язкове виконання користувачами певних правил, першим з яких є зміна паролів на складний одразу після отримання та в подальшому їх регулярна зміна чи зміна за необхідністю. Кожен користувач зобов’язаний використовувати свої ідентифікаційні дані та пароль для забезпечення відстеження. Забороняється зберігати та відправляти дані у незахищеному вигляді, зберігати файли з паролями разом із даними прикладної системи та відображати паролі, що вводяться на екрані, для забезпечення їх секретності.

Для забезпечення збереженості носіїв інформації, на яких можуть міститися резервні копії БД або інша конфіденційна інформація, недостатньо бути впевненим у співробітниках організації. Адже якщо в організації немає належно захищеного фізичного периметру, джерелом загрози може стати зовнішній порушник. Для запобігання цього рекомендується розміщувати критично важливі активи таким чином, щоб виключати можливість відкритого доступу. Також приміщення, споруди та офіси повинні давати мінімум інформації про своє призначення, щоб не дозволити порушнику ІБ зробити висновок щодо наявності в них діяльності з обробки інформації. Засоби зберігання та обробки інформації, а також об’єкти, які потребують спеціальних заходів захисту, повинні охоронятися для того, щоб зменшити загальний рівень необхідного захисту.

Іншим критичним ризиком є приведення системи до стану “відмова в обслуговуванні”. Убезпечити системи від DoS/DDoS-атак можливо, виконуючі деякі інструкції. По-перше, необхідно прослідкувати, щоб всі сервери, що мають прямий доступ до зовнішньою мережі, могли бути легко та швидко віддалено перезавантаженні. Також необхідно слідкувати, щоб використовуване ПЗ

залишалось в актуальному стані і своєчасно оновлювалось, що дозволить зменшити кількість DoS/DDoS-атак, які використовують помилки в сервісах. Мережеві сервіси, призначені для адміністративного використання, повинні бути приховані брандмауером від всіх, хто не повинен мати до них доступ. На маршрутизаторах слід встановити систему аналізу трафіку, що дозволить своєчасно дізнатися про початок атаки та вжити заходів щодо її попередження або мінімізації наслідків.

Отже, знизити ймовірність реалізації зазначених вище загроз можна шляхом посилення контролю над співробітниками організації, починаючи від прийому на роботу і закінчуючи звільненням, з врахуванням їх знань та навичок, характеру, історії тощо, систематичним переглядом та оновленням політики контролю доступу, а також вдосконаленням механізмів автентифікації.

Стосовно деяких некритичних ризиків з жовтої зони може бути застосована стратегія передачі ризику, проте оскільки велика частина з них пов’язана з людським фактором, після обробки критичних ризиків величина некритичних ризиків, пов’язаних з вразливістю людського фактору, також стане меншою. В даному випадку також недоцільно використовувати стратегію ухилення від ризику, оскільки в такому разі організація втратить більше через невиконання певної діяльності, ніж від наслідків реалізації загроз.

Для зменшення некритичних ризиків слід використовувати ліцензійне та оновлене ПЗ, своєчасно оновлювати БД для попередження несанкціонованого доступу, мотивувати співробітників організації, можливо, шляхом покращення умов праці, ініціювати роботу з їх навчання та підготовки для того, щоб вони були усвідомлені про актуальні загрози та вразливості ІБ.

Допустимі ризики, внаслідок малої ймовірності їх реалізації та незначного впливу, організація може прийняти. Прийняття ризику означає, що вони повинні бути переглянуті під час наступної оцінки, оскільки за цей час величина ймовірності або збитків може змінитися.

3.2 Рекомендації щодо вдосконалення процесів управління і методик оцінки ризиків у сфері захисту інформації в організації

Першочергово необхідно правильно визначити цілі і задачі оцінки ризиків, оскільки їх відсутність чи некоректне формулювання зменшить користь від процесу управління ризиками до мінімуму. Топ-менеджмент організації повинен бути обізнаний щодо переваг та можливостей існуючих систем управління ризиками, оскільки без цього не буде належного усвідомлення результатів, отриманих після проведення оцінки, тобто не буде зрозуміло, які дії слід вчиняти стосовно ризиків.

Для адекватного планування процесу управління ризиками керівництво організації повинно бути в змозі самостійно сформулювати, які саме результати вони бажають отримати. В такому разі вже можна буде конкретно визначити етапи процесу, виділити необхідну кількість ресурсів та спрямуватися на досягнення певного результату.

Основним недоліком при управлінні ризиками в досліджуваній організації є власне відсутність служби ризик-менеджменту і відсутність процедур оцінки ризиків. Служба ризик-менеджменту характеризується тим, що вона є інформаційно-аналітичним центром. Співробітники служби ризик-менеджменту повинні аналізувати зміни, які виникли всередині організації, а також надавати топ-менеджменту інформацію, яка може бути в подальшому застосована при стратегічному плануванні.

До функцій і задач потенційної служби ризик-менеджменту слід включити:

- планування та прогнозування:
    - дослідження ризикового середовища, в якому проводиться діяльність організації;
    - дослідження потенційного впливу ризикового середовища на ефективність діяльності організації;

- визначення цілей діяльності, засобів та ефективних методів, що дозволять досягти цих цілей;

- організація:
  - створення умов для досягнення цілей організації з використанням раніше визначених засобів та методів;
  - формування структури ризик-менеджменту;
  - формування структури апарату управління;
  - визначення взаємозв'язків між підрозділами організації;
  - розробка нормативів, методик тощо;
- регулювання:
  - вплив на об'єкт управління, який забезпечує стійкість цього об'єкту у випадку непередбачуваної зміни його характеристик;
- мотивація:
  - визначення реальних потреб співробітників, наприклад, шляхом опитувань;
  - матеріальне і моральне стимулювання;
  - мотивація, спрямована на зацікавленість співробітників у належних результатах своєї діяльності;
- контроль:
  - проміжний контроль етапів робіт з управління ризиками;
  - порівняння отриманих результатів роботи з планованими;
  - внесення змін в план робіт з управління ризиками.

В умовах обмеженого фінансування рекомендується створювати службу ризик-менеджменту поступово, починаючи з одного співробітника, який буде досконально володіти навичками спілкування та підприємницьким мисленням, а також буде компетентним в галузі управління ризиками. Кращим варіантом буде, якщо цей співробітник вже велику кількість часу працює в цій організації чи хоча б в тій же галузі діяльності, оскільки він повинен знати специфіку галузі та організації для вдалого управління ризиками. Спочатку призначений на посаду

ризик-менеджера співробітник буде виконувати за можливості всі перелічені вище функції і задачі служби ризик-менеджменту.

За умови, якщо ризик-менеджер не зможе виконувати свої задачі в зазначені терміни внаслідок збільшення потоку інформації, яку йому необхідно буде обробити, виникне необхідність розширювати організаційну структуру служби ризик-менеджменту. Вона може бути розширена за рахунок залучення вузькогалузевих спеціалістів в загальній галузі управління ризиками.

За умови, що ризик-менеджер, якого було призначено на цю посаду першим, володіє достатнім рівнем компетентності та набув належного практичного досвіду, його рекомендуються призначити на посаду головного ризик-менеджеру, якому будуть підпорядковуватися спеціалісти служби ризик-менеджменту, які будуть формувати певні відділи всередині служби. Схематично організаційну структуру зображено на рис. 3.1.

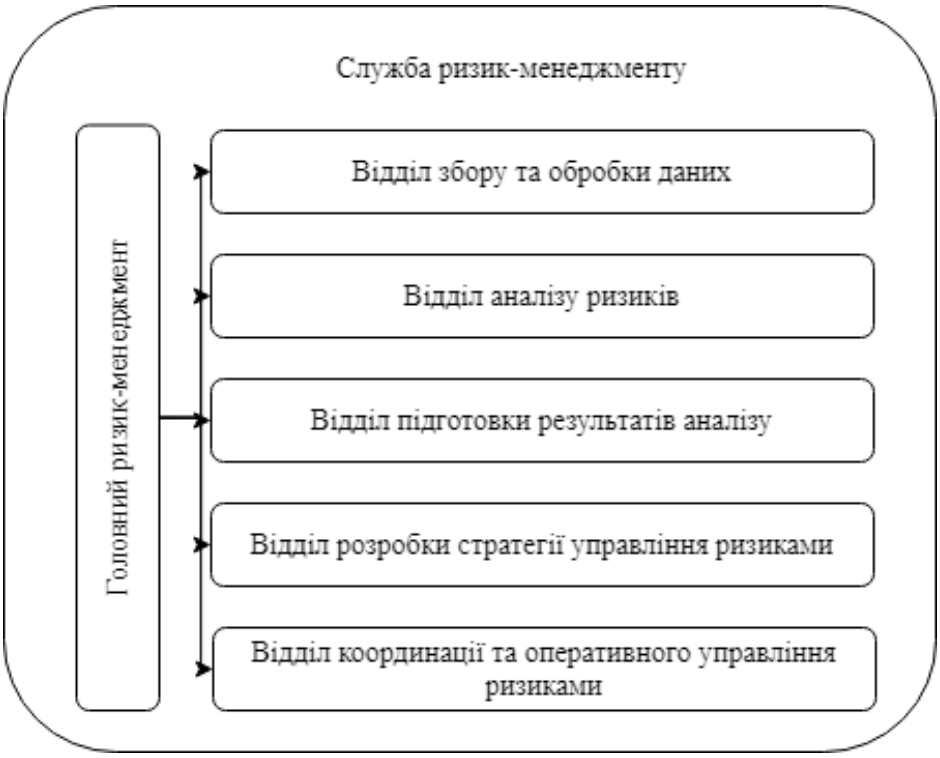

Рис. 3.1. Рекомендована організаційна структура служби ризик-менеджменту

Відділ збору і обробки інформації буде виконувати функцію регулярного збору та сортування інформації щодо наявних та потенційних ризиків та класифікації факторів ризику.

Відділ аналізу ризиків буде визначати можливі значення ризикових факторів, аналізувати отримані результати, надавати дані для подальшої розробки превентивних заходів з управління ризиками, а також тестувати розроблені заходи.

Відділ підготовки результатів аналізу буде займатися підготовкою інформації безпосередньо для розробки стратегії обробки ризиків, а також надавати інформацію керівництву щодо наявних рівнях ризику в організації.

Відділ розробки стратегії управління ризиками буде займатися розробкою стратегії обробки ризиків, інструкцій та методів зменшення ступеня ризику, коригувати стратегію обробки ризиків, базуючись на результатах тестування стратегії і змінах значень характеристик ризиків.

Відділ координації та оперативного управління ризиками буде здійснювати контроль за всіма етапами процесу управління, а також впроваджувати превентивні заходи, розроблені на минулих етапах.

Лінійність пропонованої організаційної структури дозволить чітко визначити відповідальності, оскільки кожний відділ буде виконувати свої конкретні задачі, покращити координацію дій, спростити процес управління завдяки існуванню лише одного каналу зв’язку, а також більш оперативно приймати рішення.

Висновки до третього розділу

Таким чином, було розглянуто найбільш критичні інформаційні ризики АТ “Альпарі Банк”. Було визначено, що більшу частку їх становлять ризики, пов’язані з людським фактором. Причиною цього може бути неправильна мотивація співробітників, наявність великої кількості конкурентів, які можуть впливати на співробітників, призначення на критичні посади, які потребують глибоких знань в галузі ІБ, некомпетентних співробітників та їх власні якості.

В ході дослідження було визначено, що найбільш критичними є ризики, пов’язані з розголошенням чи іншим видом розкриття конфіденційної інформації і порушенням доступності послуг і інформації.

Було виявлено основні недоліки управління ризиками, такі, як відсутність служби ризик-менеджменту, відсутність процедур оцінки ризиків та ігнорування інформаційних ризиків та загроз.

Було запропоновано способи мінімізації критичних ризиків, виконання яких не потребує значної трати ресурсів, проте які можуть забезпечити належний рівень ІБ.

Також було рекомендовано впровадити службу ризик-менеджменту поступово, в умовах обмеженого фінансування.

Було висунуто вимоги до кваліфікації та якостей співробітників, яких слід залучити до роботи даної служби. Було розкрито основні функції і задачі, яка має виконувати потенційна служба ризик-менеджменту, її організаційна структура та задачі кожного з відділів.

ВИСНОВКИ

1. Процес ризик-менеджменту є невід’ємним процесом забезпечення ІБ організації. Доцільно впроваджувати цей процес не як самостійну відокремлену від інших процесів частину, а інтегрувати його в ключові процеси організації та застосовувати при прийнятті управлінських рішень. Процес управління ризиками в загальному випадку найбільш вдало описується в стандарті ISO 31000. Щодо процесу управління ризиками ІБ, детальний алгоритм дій надано в стандарті ISO 27005.

2. Було визначено, що для прийняття рішень щодо вибору стратегії обробки ризиків доцільно скористатися елементами теорії ймовірностей та статистики, такими як середнє очікуване значення, середньоквадратичне відхилення, коефіцієнт варіації, критерії Севіджа, Гурвіца тощо. Вибір стратегії певною мірою залежить від ОПР, особливо ця залежність зростає у випадках, коли рішення приймається в умовах недостатності достовірної інформації.

3. Було розглянуто підходи до оцінки інформаційних ризиків, їх відмінності, переваги та недоліки. Було визначено, що на практиці в більшості випадків застосовується якісна оцінка ризиків завдяки свої простоті та відсутності жорстких вимог до кваліфікації співробітників та виділеного фінансування на оцінку ризиків. Також було розглянуто деякі методики та інструменти оцінки і аналізу інформаційних ризиків, було визначено сферу їх застосування та визначено, в яких типах організацій доцільніше буде використовувати ту чи іншу методику.

4. Було розглянуто перелік формул для визначення кількісного значення ризику, які можуть бути застосовані, якщо в наявності є достатня для оцінки кількість достовірної інформації про об’єкт оцінки. Ця інформація зазвичай включає інформацію про активи, які необхідно захищати, наявні в організації, їх цінність, частоту або ймовірність реалізації загроз, кількість та значущість наявних

вразливостей, ймовірність їх експлуатації тощо. Для отримання більш точної оцінки знадобиться більша кількість початкових даних.

5. Серед переліку наявних та потенційних загроз, наявних в організації, було визначено найбільш критичні, які можуть здійснити вплив на важливі активи, які захищаються. Була проведена якісна оцінка ризику на основі даних про цінність активів і частоту інцидентів (реалізації загроз), і далі за допомогою матриці ризиків було визначено пріоритети ризиків ІБ за категоріями: критичні, некритичні та допустимі. Щодо допустимих ризиків рекомендовано задіяти стратегію прийняття та періодично проводити їх моніторинг. Було розроблено рекомендації, як зменшити ступінь критичних ризиків та вдосконалити процес ризик-менеджменту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов А. В. Международные стандарты управления рисками: не Базелем единым. *Рынок ценных бумаг.* 2015. № 5. С. 23-33. URL: http://partad.ru/UploadFiles/GetUploadedPdfFile?uploadFileId=113.
2. Данько Н., Теличко К. Огляд міжнародних стандартів з управління ризиками. *Охорона праці і пожежна безпека.* 2018. № 8. URL: https://oppb.com.ua/news/oglyad-mizhnarodnyh-standartiv-z-upravlinnya-ryzykamy.
3. Перевод стандарта ISO 31000:2018. Risk management. Guidelines. URL: https://risk-academy.ru/download/iso31000/.
4. ISO/TR 31004:2013. Risk management. Guidance for the implementation of ISO 31000. URL: https://www.iso.org/standard/56610.html.
5. IEC 31010:2019. Risk management. Risk assessment techniques. URL: https://www.iso.org/ru/standard/72140.html.
6. ISO Guide 73:2009. Risk management. Vocabulary. URL: https://www.iso.org/ru/standard/44651.html.
7. «Делойт». Управление рисками. Правила игры меняются. URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/rules-of-game-changing.pdf.
8. Федерация европейских ассоциаций риск менеджеров. Стандарты управления рисками. URL: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf.
9. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. URL: https://www.iso.org/ru/standard/75281.html.
10. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ISO/IEC 27005:2018 IDT). [Чинний від 01.11.2019]. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797.

11. Управление рисками информационной безопасности. Часть 7. Стандарт ISO/IEC 27005:2018 (продолжение). Стандарт IEC 31010:2019. URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-7-standart-iso-iec-27005-2018-prodolzhenie-sta/?sphrase_id=1659.
12. Агурьянов И. Обработка рисков информационной безопасности. URL: https://www.securitylab.ru/blog/personal/aguryanov/30003.php.
13. Неопределенность и ситуация риска. URL: http://www.risk24.ru/neopred.htm.
14. Беспалова О. В. Отличительные особенности понятий «неопределенность» и «риск». *Пожарная безопасность: проблемы и перспективы.* 2016. URL: https://cyberleninka.ru/article/n/otlichitelnye-osobennosti-ponyatiy-neopredelennost-risk/viewer.
15. Критерий среднего выигрыша. *Студопедия.* 2015. URL: https://studopedia.su/18_5233_kriteriy-srednego-viigrisha.html.
16. Выбор оптимальной стратегии защиты компании. URL: http://www.lghost.ru/lib/security/kurs2/theme04_chapter03.htm.
17. Богоявленский С. Б. Принятие решений в условиях неопределенности. Критерий Лапласа. 2014. URL: http://risking.ru/materials/risktheory/part2_9.html.
18. Богоявленский С. Б. Принятие решений в условиях неопределенности. Критерий Вальда. 2014. URL: http://risking.ru/materials/risktheory/part2_7.html.
19. Принятие решений в условиях полной неопределенности. *Моделирование рисковых ситуаций в экономике и бизнесе.* URL: http://www.bibliotekar.ru/riskovye-situacii-2/10.htm.
20. Богоявленский С. Б. Принятие решений в условиях неопределенности. Критерий Гурвица. 2014. URL: http://risking.ru/materials/risktheory/part2_11.html.
21. Критерий Сэвиджа. URL: https://math.semestr.ru/games/savage.php.
22. Принятие решений в условиях риска и неопределенности. URL: https://studall.org/all-75786.html.

23. ГОСТ Р 58771-2019. Менеджмент риска. Технологии оценки риска. [Действует с 01.03.2020]. URL: http://docs.cntd.ru/document/1200170253.
24. Шиляев С. Методика оценки рисков информационной безопасности. *Контур.* 2015. URL: https://kontur.ru/articles/1691.
25. Safran. An introduction to qualitative risk analysis. URL: https://www.safran.com/content/introduction-qualitative-risk-analysis.
26. Engineering Safety Consultants. Quantitative risk assessment – QRA. URL: https://esc.uk.net/quantitative-risk-assessment/.
27. URL: https://intuit.ru/studies/courses/531/387/lecture/8996?page=1.
28. Thomas R. Petlier, CISSP. Effective Risk Analysis. 2000. URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/304slide.pdf.
29. Аналіз методики FRAP. 2015. URL: https://studopedia.su/20_7596_analiz-metodiki-FRAP.html.
30. Software Engineering Institute. Introducing OCTAVE Allegro: Improving the information security risk assessment process. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419.
31. Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний. URL: http://citforum.ru/products/dsec/cramm/cramm1.shtml.
32. Астахов А.М. Искусство управления информационными рисками. Москва: ДМК Пресс, 2010. 312 с.
33. Ларина И.Е. Экономика защиты информации: учеб. пособие. Москва: МГИУ, 2007. 92 с.
34. Р Газпром 4.2-3-003-2015. Система обеспечения информационной безопасности ОАО «Газпром». Методика оценки рисков. Москва: ОАО «Газпром», 2015. 178 с.
35. Мур М. Управление информационными рисками. *Финансовый директор.* 2003. № 9. С. 64-68.

36. Microsoft Solutions for Security and Compliance. The Security Risk Management Guide. San Francisco: Microsoft Corporation, 2006. 129 p.