МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вікторія КОТЕЦЬКА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувачка вищої освіти гр. УБД-42

Вікторія КОТЕЦЬКА
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЯКИМЕНКО
К.в.н., доц. Ім’я, ПРІЗВИЩЕ

Рецензент: ГАЛІНА ГАЙДУР
Д.т.н., проф. Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Котецька Вікторія Ігорівна
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аналіз процесів управління ризиками інформаційної безпеки організації”,
керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н., доц.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від 27.02.24 № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *міжнародні стандарти, наукова та технічна література, методики управління ризиками, загрози та вразливості порушень інформаційної безпеки*

4. Перелік питань, які мають бути розроблені:
4.1.Визначити роль і значення інформаційної безпеки в процесах управління ризиками.
4.2.Проаналізувати методичні підходи щодо аналізу процесів управління ризиками інформаційної безпеки організації
4.3.Дослідити вплив процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки організації (для обраного прикладу), та розробити рекомендації

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Визначити роль і значення інформаційної безпеки в процесах управління ризиками	08.04.2024	
4.	Розглянути методичні підходи щодо аналізу процесів управління ризиками інформаційної безпеки організації	22.04.2024	
5.	Дослідити вплив процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки організації (для обраного прикладу)	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

здобувачка вищої освіти _____ Вікторія КОТЕЦЬКА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувачка Котецька В.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Аналіз процесів управління ризиками інформаційної безпеки організації"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка КОТЕЦЬКА Вікторія у кваліфікаційній роботі проаналізувала процеси управління ризиками інформаційної безпеки організації; використала методи аналізу, порівняння, класифікаціЇ, а також системний підхід до аналізу управління ризиками; дослідила вплив процесів управління ризиками на ефективність системи управління інформаційної безпеки в організації; розробила практичні рекомендації за темою дослідження.

КОТЕЦЬКА Вікторія показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки КОТЕЦЬКОЇ Вікторії на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. здобувачка Котецька В.І. допускається до захисту роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти КОТЕЦЬКОЇ Вікторії

на тему “Аналіз процесів управління ризиками інформаційної безпеки організації”

Актуальність.

Сучасні інформаційні системи вразливі від цілого ряду загроз, які спрямовані на інформацію і зниження в цілому рівня інформаційної безпеки будь-якої організації. Метою процесу управління ризиками інформаційної безпеки є виявлення, контроль та мінімізація невизначеності негативного впливу таких різних чинників дій.

Дослідженню процесів обробки, реагування, аналізу, розслідування ризиків інформаційної безпеки та використанню методик їх оцінки приділяється все більше уваги, тому тема роботи, пов’язана з аналізом процесів управління ризиками інформаційної безпеки організації, є актуальною.

Позитивні сторони.

1. У роботі досліджено інформаційна безпека у процесах управління ризиками, проаналізовані методичні підходи та досліджено вплив процесів управління ризиками на ефективність системи управління ризиками в організації.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Авторка опрацювала значну джерельну базу: близько 50 публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо покращення управління ризиками інформаційної безпеки організації і показано на прикладі обраної компанії.

Недоліки.

Доцільно було б збільшити розмір шрифту тексту в елементах рисунків – для кращого сприймання.

Однак, це зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок:

Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувачка КОТЕЦЬКА Вікторія заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: професор кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор_____ Галина ГАЙДУР
(*підпис*) (*Ім’я, ПРІЗВИЩЕ*)

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу процесів управління ризиками інформаційної безпеки організації. Робота складається зі вступу, трьох розділів що містять 20 рисунків, висновків і списку використаних джерел із 51 найменувань. Загальний обсяг роботи становить 92 аркушів, з яких 6 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз процесів управління ризиками інформаційної безпеки організації.

Об'єктом дослідження є процеси управління ризиками інформаційної безпеки в організаціях.

Предмет дослідження є сучасні методи управління ризиками інформаційної безпеки організації.

Методи дослідження. Для вирішення поставленого наукового завдання у роботі використано методи аналізу, порівняння, класифікація, а також системний підхід до аналізу управління ризиками інформаційної безпеки організації.

Як результат у роботі досліджена інформаційна безпека у процесах управління ризиками, проаналізовані методичні підходи та досліджено вплив процесів управління ризиками на ефективність системи управління ризиками в організації.

Галузь застосування. Розроблені рекомендації можуть бути використані при вдосконаленні процесів управління ризиками інформаційної безпеки організації.

Ключові слова: УПРАВЛІННЯ РИЗИКАМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ ТА ВРАЗЛИВОСТІ, ОРГАНІЗАЦІЙНІ І ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ, ОЦІНКА РИЗИКІВ.

ABSTRACT

The qualification work is devoted to the analysis of the organization's information security risk management processes. The work consists of an introduction, three sections containing 20 drawings, conclusions and a list of used sources from 51 denominations The total amount of work is 92 sheets from which 6 sheets contain a list of conventional abbreviations and a list of used sources.

The purpose of the study is an analysis of the organization's information security risk management processes.

The object the study there are information security risk management processes in organizations.

The subject of the study there are modern methods of managing information security risks of the organization.

Research methods. To solve the scientific task, the work uses methods of analysis, comparison, classification, as well as a systematic approach to the analysis of information security risk management of the organization.

As a result, information security in risk management processes was investigated, methodical approaches were analyzed, and the influence of risk management processes on the effectiveness of the risk management system in the organization was investigated.

Field of application. The developed recommendations can be used to improve the organization's information security risk management processes.

Keywords: RISK MANAGEMENT, INFORMATION SECURITY, THREATS AND VULNERABILITIES, ORGANIZATIONAL AND TECHNICAL MEASURES OF PROTECTION, RISK ASSESSMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

Якщо в КР певний термін, скорочення чи позначення повторюється менше трьох разів, його у перелік не включають, а його розшифрування наводять у тексті при першому згадуванні. Перелік друкується двома колонками, в яких ліворуч за абеткою наводять позначення чи терміни, праворуч - їх детальне розшифрування (тлумачення).

ІБ	Інформаційна безпека
СУІБ	Систем управління інформаційною безпекою
NIST	Національний інститут стандартів і технологій
CRAMM	Метод аналізу та управління ризиками ССТА
OCTAVE	Метод оцінки активів, загроз, вразливостей і заходів з контролю доступу
COBIT	Керування корпоративними інформаційними технологіями та відповідність
FRAP	Рамки аналізу ризиків для проектів
FMEA	Аналіз можливих несправностей та їх ефектів
FAIR	Факторний аналіз інформаційних ризиків
USAID	Агентство США з міжнародного розвитку

ВСТУП

Актуальність теми. Інформаційні технології відіграють важливу роль у функціонуванні будь-якої організації, тому управління ризиками інформаційної безпеки стає критично важливим завданням. Зростання обсягів даних та підвищення складності кіберзагроз ставлять нові виклики перед організаціями у захисті конфіденційної інформації.

Без належного аналізу та управління ризиками інформаційної безпеки, організації ризикують зіткнутися з серйозними наслідками, такими як витік даних, фінансові втрати та шкода репутації. Актуальність теми аналізу процесів управління ризиками інформаційної безпеки є незаперечною, оскільки ефективне управління цими ризиками не лише забезпечує захист важливих даних, але й сприяє стабільному функціонуванню бізнесу, зменшенню можливих збитків та підвищенню довіри з боку клієнтів і партнерів.

Метою роботи є аналіз процесів управління ризиками інформаційної безпеки організації.

Об’єктом дослідження є процеси управління ризиками інформаційної безпеки в організаціях.

Предмет дослідження є сучасні методи управління ризиками інформаційної безпеки організації.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Визначити роль і значення інформаційної безпеки в процесах управління ризиками.
2. Проаналізувати методичні підходи щодо аналізу процесів управління ризиками інформаційної безпеки організації.
3. Провести дослідження впливу процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки організації на прикладі конкретного випадку.

Методи дослідження. Для вирішення поставленого наукового завдання у роботі використано методи аналізу, порівняння, класифікація, а також системний підхід до аналізу управління ризиками інформаційної безпеки

організації.

Як результат у роботі досліджена інформаційна безпека у процесах управління ризиками, проаналізовані методичні підходи та досліджено вплив процесів управління ризиками на ефективність системи управління ризиками в організації.

Практичне значення одержаних результатів. Цей аналіз дозволить ідентифікувати основні проблеми та потенційні загрози, які стикаються з управлінням ризиками інформаційної безпеки в організації. Враховуючи ці результати, можна розробити та впровадити ефективні стратегії та заходи для запобігання/мінімізації ризиків, пов'язаних з інформаційною безпекою. Це сприятиме підвищенню рівня захищеності інформації, зменшенню можливих втрат та забезпечить стабільність функціонування організації в умовах зростаючих кіберзагроз.

Апробація результатів за темою “Вплив ризиків на ефективність інформаційної безпеки в організаціях, підходи до аналізу” було доведено на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 РОЛЬ І ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСАХ УПРАВЛІННЯ РИЗИКАМИ

В цьому розділі розглядається роль інформаційної безпеки у керуванні ризиками, зокрема, її важливість для забезпечення стійкості та захисту даних. Після цього досліджуються вимоги нормативних документів, що регулюють управління ризиками у цій області, а також проводиться аналіз попереднього досвіду щодо виявлення загроз і вразливостей.

1.1 Визначення інформаційної безпеки та її роль в управлінні ризиками

Інформаційна безпека є важливою для будь-якої організації. Основне завдання в цій сфері полягає на забезпеченні захищеності даних від несанкціонованого доступу, збереження конфіденційності, доступності та цілісності інформації. Серйозною проблемою є витік даних, який може порушити довіру клієнтів, втрату ресурсів та пошкодження репутації організації. До того ж інформаційна безпека включає в себе не лише захист від зловмисних атак, але і управління ризиками.

Управління ризиками інформаційної безпеки - це важливий процес, який охоплює виявлення, контроль та оцінку ризиків, що пов'язані з інформаційними системами. Це включає ідентифікацію потенційних загроз для безпеки, а також оцінку ймовірності та можливих наслідків кожної з них. Забезпечуючи безпеку вживаються заходи контролю, спрямовані на зниження виявлених ризиків до прийнятного рівня. Це дозволяє організаціям:

- Запобігати кіберінцидентам та витокам даних, знижуючи фінансові втрати від простоїв, порушень та штрафів.
- Відповідати нормативним вимогам та галузевим стандартам, зміцнюючи довіру клієнтів, партнерів та інвесторів.

- Приймати обґрунтовані рішення щодо інвестицій в кібербезпеку, оптимізуючи ресурси та максимізуючи захист.

Завдяки кращому розумінню ризиків, організації можуть вдосконалювати процеси, підвищувати стійкість та збільшувати конкурентну перевагу [1].

Для великих організацій, де обов'язки розподілені між різними командами, управління ризиками ІБ забезпечує централізований огляд ризиків, що дозволяє ефективно координувати заходи з кібербезпеки. Формалізоване управління ризиками також дає змогу обґрунтовувати інвестиції в додаткові засоби контролю та системи безпеки. Наприклад, якщо організація планує впровадити вдосконалену систему виявлення вторгнень, вона може використовувати управління ризиками для обґрунтування витрат, демонструючи ризики, які будуть пом'якшені. Такий підхід допомагає визначити найефективнішу конфігурацію системи та контролювати її ефективність з часом [2].

Щоб забезпечити ефективний захист, організації повинні розуміти вразливості своєї інформаційної системи та ризики, пов'язані з її використанням. Управління ризиками інформаційної безпеки допомагає виявити ці вразливості та розробити стратегії захисту, які відповідають потребам конкретної організації. Це може включати в себе не лише технологічні заходи, такі як шифрування та брандмауери, але й політики та процедури, спрямовані на попередження витоку даних.

Процес управління ризиками ІБ спрямований на виявлення, контроль та мінімізацію невизначеності, що пов'язана з впливом можливих загроз на інформаційні активи. Цей процес є важливим для забезпечення безперервності функціонування критичних інформаційних систем. Процес управління ризиками ІБ можна обумовити чотирма основними етапами:

1. Етап аналіз ризику здійснює ідентифікацію та оцінка загроз, які можуть скомпрометувати інформаційну безпеку важливих інформаційних активів. Цей аналіз дозволяє виявити потенційні слабкі місця в системах та визначити профілактичні заходи для зниження ймовірності виникнення загроз.

2. Етап оцінки ризику включає визначення рівня ризику, що обчислюється як функція важливості активів, ймовірності виникнення загрози, наявності вразливостей та потенційного збитку, який може бути завданий у разі реалізації загрози. Це дозволяє пріоритезувати ризики та визначити, які з них потребують негайного втручання.

3. Етап зниження ризику впроваджує конкретні контролі та заходи для запобігання визначеним ризикам. Це можуть бути технічні, організаційні та адміністративні заходи. Також передбачаються засоби відновлення, які дозволять забезпечити безперервне функціонування системи захисту інформації у випадку реалізації ризиків. Цей етап також включає розробку планів дій на випадок інцидентів, що допомагає мінімізувати негативні наслідки.

4. Етап оцінки вразливостей та контролю передбачає аналіз основних властивостей критичних систем та виявлення тих, які можуть бути використані для реалізації загроз. Це дозволяє внести зміни та покращити заходи безпеки для забезпечення їхньої дієвості.

На рис. 1.1 можна побачити цикл процесу управління ризиками ІБ, який забезпечує безперервність функціонування інформаційних систем. Цей рисунок показує взаємозв’язок між етапами аналізу ризику, оцінки ризику, зниження ризику та оцінки вразливостей і контролю, демонструючи їхню циклічність та безперервність у процесі управління ризиками ІБ [3].

Рис. 1.1 – Цикл процесу управління ризиками

Управління ризиками інформаційної безпеки є важливою складовою для будь-якої організації, оскільки воно дозволяє виявити та вирішити потенційні вразливості, що можуть призвести до серйозних інцидентів безпеки, таких як витік конфіденційної інформації або кібератаки. Також воно захищає їх від загроз, не лише зберігаючи цифрові активи, а й забезпечуючи відповідність законодавству, сприяючи довірі між зацікавленими сторонами та допомагаючи у прийнятті рішень. Цей процес в ІБ зокрема допомагає визначити, які загрози та вразливості є найбільш критичними та потребують термінової уваги. Організації, які діють у сферах з жорстким регулюванням, часто повинні використовувати і підтримувати програми управління ризиками інформаційної безпеки. Наприклад, є вимоги щодо конфіденційності даних клієнтів або корпоративної інформації. Вони зобов'язують організації проводити регулярні аналізи ризиків ІБ з метою відповідності стандартам та уникнення штрафних санкцій. Зокрема великі організації мають складну структуру з розподіленими обов'язками, що ускладнює координацію та управління ризиками кібербезпеки. Управління ризиками інформаційної безпеки надає централізоване уявлення про ризики, дозволяючи ефективно координувати заходи забезпечення безпеки. Крім того, формалізоване управління ризиками дозволяє аргументувати

витрати на додаткові заходи безпеки та системи. Наприклад, якщо організація розглядає можливість впровадження системи виявлення вторгнень, вона може використати систему управління ризиками для обґрунтування витрат, показуючи ризики, які будуть зменшені. Також організації, де велика частка працівників працює віддалено, можуть бути надзвичайно вразливими до витоків даних. Це може передбачити, що віддалена робота може підвищити ризик недостатньої захищеності до інформаційної безпеки. Недостатня захищеність може посилити загрозу витоку даних внаслідок неавторизованого доступу до мережі або недбалого використання пристроїв. З цієї причини, організаціям, які мають віддалених працівників, надзвичайно важливо вживати заходи для забезпечення безпеки даних, такі як використання захищених з'єднань, шифрування даних та вдосконалення політик безпеки. Такі заходи допоможуть зменшити ризик витоку даних та зберегти конфіденційність, цілісність та доступність інформаційних активів.

Основна мета управління ризиками ІБ передбачає забезпечення безпеки, конфіденційності та цілісність інформації. Для досягнення цієї мети визначаються всі можливі загрози, включаючи зловмисні дії, технічні недоліки, людські помилки, природні катастрофи та інші фактори, які можуть загрожувати інформаційній безпеці [4].

Одним із важливих елементів управління ризиками інформаційної безпеки є регулярні аудити та оновлення політик безпеки.

Політика інформаційної безпеки включає всі аспекти забезпечення безпеки даних в організації. Це передбачає плани та процедури для проведення навчання користувачів, управління проектами, операційну діяльність, управління ризиками та оцінку політики. Навчання користувачів направлене на зменшення кількості інцидентів безпеки, пов'язаних з низьким рівнем знань співробітників. Операційна діяльність включає щоденне обслуговування поточних систем безпеки. Управління проектами стосується створення та впровадження нових систем безпеки, а управління ризиками являє собою процес виявлення вразливостей і прийняття заходів для контролю цих

слабкостей. Поступово, через появу нових загроз, політику інформаційної безпеки необхідно постійно адаптувати. Це являє собою включення планів надзвичайних ситуацій для реагування на інциденти, відновлення після аварій та плани забезпечення неперервності бізнесу. Надзвичайні ситуації можуть включати кібератаки, природні катастрофи, внутрішні порушення безпеки тощо. Для ефективної реакції на такі ситуації важливо визначати ролі та відповідальності персоналу, розробляти механізми швидкого відновлення даних та систем та встановити процедури забезпечення неперервності бізнесу для мінімізації втрат і перерв у роботі. Загалом ефективне управління ризиками інформаційної безпеки передбачає постійний моніторинг та аналіз існуючих загроз і заходів безпеки. Це дозволяє організації вчасно виявляти нові загрози, адаптувати свої стратегії та змінювати заходи контролю відповідно до змін у середовищі безпеки.

Додатково важливо постійно моніторити зміни в загрозах та впроваджувати нові технології та стратегії для перешкоджання потенційним інцидентам безпеки [5].

Ризики для інформаційних активів включають в себе можливість втрати конфіденційності, цілісності та доступності даних. Це може відбутися через несанкціоновану зміну, розголошення, знищення інформації та несанкціоноване використання інформаційних систем, як наприклад, відправлення спаму з незаконно присвоєного облікового запису.

В цілому головну мету в системі інформаційної безпеки організації відіграє забезпечення її стійкого функціонування та захист від загроз, запобігання розголошенню, втраті, спотворенню та знищенню службової інформації, а також підтримка нормальної виробничої діяльності. Для досягнення цих цілей загалом необхідно:

1. Відібрати інформацію з найважливіших потоків та віднести її до категорії обмеженого доступу (комерційної таємниці).

2. Прогнозувати та своєчасно виявляти загрози інформаційним ресурсам, аналізувати причини та умови, що можуть призвести до збитків і порушень у функціонуванні підприємства.

3. Створити умови для мінімізації ймовірності реалізації загроз та запобігання різним видам збитків.

4. Запроваджувати механізми оперативного реагування на загрози та ефективно контролювати доступ до ресурсів за допомогою правових, організаційних і технічних заходів.

5. Максимально відшкодовувати та локалізувати збитки, зменшувати негативний вплив порушень інформаційної та економічної безпеки на стратегічні цілі.

Щоб створити збалансовану модель інформаційної безпеки проводиться аналіз ризиків у сфері безпеки інформаційних потоків та визначити оптимальний рівень ризику для організації. Модель повинна забезпечувати досягнення цього рівня ризику.

Модель системи управління інформаційною безпекою, відповідно до міжнародного стандарту ISO/IEC 15408, ілюструє вплив зовнішніх та внутрішніх факторів на безпеку та схоронність ресурсів в організації, що представлені на рис. 1.2. У цій моделі зовнішні та внутрішні фактори позначені прямокутниками. Напрямки управлінського та природного впливу зображені відповідно пунктирними та суцільними стрілками.

Серед об'єктивних факторів, що відображаються у цій моделі:

- Загрози інформаційній безпеці визначаються ймовірністю їх виникнення та реалізації.
- Вразливості системи інформаційної безпеки впливають на ймовірність використання загроз.
- Втрати відображають реальний збиток внаслідок реалізації загрози для інформаційної безпеки.
- Ризики показують можливість завдання шкоди організації внаслідок реалізації загрози інформаційній безпеці [6].

Рис. 1.2 – Схема системи управління інформаційною безпекою у вигляді моделі процесів ІБ

Будова оптимальної моделі ІБ організації передбачає декілька важливих принципів. Спочатку проводиться аналіз ризиків у сфері інформаційної безпеки, під час якого виявляються потенційні загрози. Надалі визначається оптимальний рівень ризику для підприємства, що базується на певних критеріях та урахуванні його специфіки та розробляються та впроваджуються контрзаходи, спрямовані на зниження ризику до заданого рівня. Ця методика надає можливість детально розглянути вимоги до забезпечення інформаційної безпеки в організації. Також для досягнення цієї мети необхідно виконати:

- Визначення рівня доступу до інформації на різних рівнях.
- Прогнозування та вчасне виявлення можливих загрози для інформаційних ресурсів.
- Створення умов, що мінімізують ризики для інформаційних ресурсів.
- Розроблення механізму швидкого реагування на загрози та забезпечити оперативне втручання.

- Забезпечення максимального відшкодування збитків від незаконних дій фізичних та юридичних осіб.
- Обирання найефективніших заходів безпеки.
- Оцінювання ефективності заходів та порівняння різних варіанти.

Загалом можна визначити, що управління ризиками в галузі інформаційної безпеки відіграє важливу роль в забезпеченні надійного кіберзахисту. Його ефективність визначається можливістю дотримуватися правил, встановлених у сфері безпеки. Крім того, воно сприяє налагодженню сильного корпоративного управління, що в свою чергу допомагає приймати оптимальні рішення щодо розподілу ресурсів, спрямованих на безпеку.

Ефективний план управління ризиками надає можливість підвищити стійкість до кібератак і забезпечити безперервність бізнес-процесів. Він включає в себе заходи, спрямовані на захист IT-інфраструктури, клієнтів та співробітників від потенційних загроз [7].

Незважаючи на те, що управління ризиками інформаційної безпеки часто знаходиться поза увагою і може бути складним у впровадженні в організації, його значення важливо наголосити. Відповідна стратегія допомагає організаціям захистити себе від зростаючої загрози кібератак і зберегти свою діяльність в безпечному середовищі.

1.2 Вимоги нормативних документів, спрямованих на управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки вимагає комплексного підходу, що ґрунтується на вивченні, розробці та впровадженні спеціалізованих нормативних документів. Ці документи встановлюють стандарти, правила та процедури, необхідні для ефективного управління ризиками та забезпечення інформаційної безпеки в організації.

З погляду ведення бізнесу, інформаційна безпека стала не просто технічною проблемою, а стратегічним питанням, яке впливає на всі аспекти

діяльності організації: від фінансової стійкості до репутації та клієнтських відносин. Напади хакерів, витоки даних, віруси та інші кіберзагрози можуть негативно позначитися на функціонуванні організації, призводячи до фінансових втрат, порушення законодавства, втрати довіри споживачів та іншим проблемам.

Загалом нормативні документи стають головним інструментом, який визначає рамки та вимоги для забезпечення ефективного управління ризиками інформаційної безпеки. Політика інформаційної безпеки є одним з таких документів. Цей документ встановлює загальні принципи, цілі та стратегії, які організація приймає для захисту своєї інформації. Вона виступає фундаментом для будь-яких стратегій та практик управління ризиками, оскільки визначає основні принципи та підходи, а також встановлює вимоги до захисту від різних видів загроз, як внутрішніх, так і зовнішніх.

Політика інформаційної безпеки мусить бути детально розроблена, щоб враховувати всі можливі аспекти діяльності організації та ризики, пов'язані з інформацією. Вона встановлює відповідальності за захист інформації, які включають ідентифікацію осіб, відповідальних за кожний аспект безпеки, від керівників до звичайних співробітників. Політика безпеки також визначає чіткі правила доступу до інформації. Це означає встановлення процедур контролю доступу до систем та даних, встановлення правил щодо ролей та обов'язків користувачів, а також використання механізмів автентифікації та авторизації. Крім того, політика інформаційної визначає процедури обробки та зберігання даних. Це передбачає те що документ повинен встановлювати правила щодо обробки чутливої інформації, використання шифрування та інші технічні заходи для захисту даних під час їх транспортування та зберігання [8].

Також серед нормативних документів важливе місце займають стандарти інформаційної безпеки. Ці стандарти визначають конкретні технічні та організаційні вимоги до захисту інформації. Стандарти вимагають впровадження ризик-орієнтованого підходу до бізнес-процесів. Організації повинні аналізувати та оцінювати ризики, пов'язані з інформаційною безпекою,

і вживати заходів для їх зменшення. Використовуючи стандарт, організації можуть розробляти і реалізовувати ефективні стратегії управління ризиками інформаційної безпеки, що відповідають їхнім конкретним потребам.

ISO/IEC 27001:2022 є одним із найбільш впливових стандартів у сфері систем управління інформаційною безпекою (СУІБ). Цей стандарт встановлює основні вимоги до СУІБ та є універсальним посібником для організацій будь-якого розміру та галузі. Дотримання ISO 27001 свідчить про те, що організація впровадила надійну систему управління ризиками, пов'язаними з безпекою даних, відповідно до найкращих практик і принципів, закріплених у цьому міжнародному стандарті. Управління ризиками, на якому ґрунтується СУІБ згідно з ISO/IEC 27001:2022, рис. 1.3 передбачає виявлення, оцінку та управління ризиками інформаційної безпеки. Цей процес дозволяє організаціям ідентифікувати потенційні загрози та розробляти стратегії для їх зменшення, що важливо для забезпечення безпеки та захисту інформації.

Рис. 1.3 – ISO/IEC 27001:2022

Основними перевагами впровадження ISO/IEC 27001:2022 є:

1. Підвищення рівня інформаційної безпеки, являє собою систематичний підхід до управління ризиками дозволяє виявляти та усувати потенційні загрози, зменшуючи кількість та тяжкість інцидентів.

2. Збільшення довіри клієнтів та партнерів, передбачає сертифікацію ISO/IEC 27001 свідчить про серйозне ставлення організації до інформаційної безпеки, що збільшує довіру та покращує репутацію.

3. Підвищення ефективності бізнесу, обумовлює ефективну систему управління інформаційною безпекою допомагає уникнути простоїв та порушень, збільшуючи загальну ефективність бізнесу.

4. Відповідність нормативним вимогам, надає відповідність міжнародним нормативним вимогам щодо інформаційної безпеки, що допомагає уникнути штрафів та інших санкцій.

Стандарт ISO 27001 також має відношення до інших систем управління, таких як ISO 9001 та ISO 14001. Відповідно до цих систем, документація та процедури, необхідні для виконання ISO 27001, можуть бути частково використані вже існуючими системами управління якістю. Загалом цей стандарт базується на найкращих світових практиках в області управління інформаційною безпекою. Він вимагає від організацій розробляти, впроваджувати, функціонувати, моніторити, аналізувати та поліпшувати систему управління інформаційною безпекою. Цей стандарт є основою для розробки таких документів, як ISO 27002, ISO 27004 та ISO 27005, які доповнюють та деталізують його вимоги [9].

Засоби контролю ISO/IEC 27002 представляють собою набір заходів з інформаційної безпеки, кібербезпеки та захисту конфіденційності, а також рекомендації щодо їх впровадження, що ґрунтуються на загальноприйнятих галузевих стандартах. ISO/IEC 27002 містить вказівки щодо засобів контролю, які можна впровадити в організації. Це документ, призначений допомогти організаціям розробити свої власні стратегії забезпечення безпеки інформації відповідно до їх потреб і особливостей. Отже, перед впровадженням будь-яких заходів безпеки організації повинні проаналізувати свої конкретні потреби та ризики. Стандарт ISO/IEC 27002:2022 визначає декілька основних дій до інформаційної безпеки, які допомагають визначити засоби контролю безпеки, їх можна побачити на рис. 1.4.

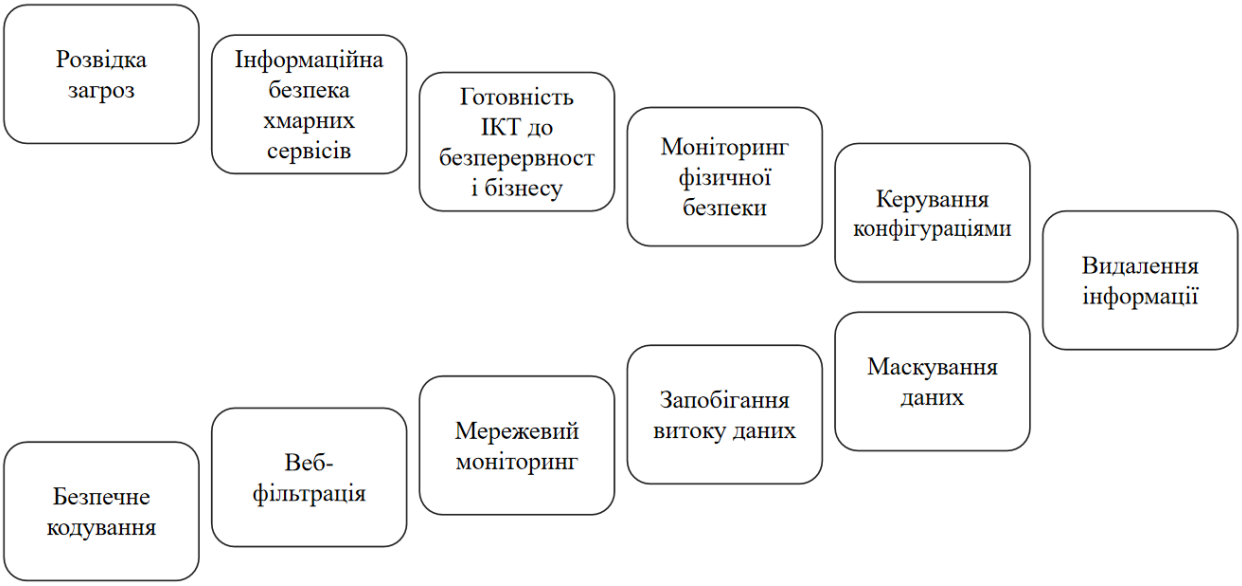

Рис. 1.4 – Список елементів керування відповідно до ISO/IEC 27002

Беручи за основу цей рисунок, можна побачити основний список елементів керування ISO/IEC 27002:2022, який складається з 11 елементів.

1. Розвідка загроз - це процес збору, аналізу і контекстуалізації даних про можливі ризики. Це допомагає компаніям отримати повну картину потенційних загроз і краще підготуватися до можливих атак.

2. Інформаційна безпека хмарних сервісів стає все важливішою з поширенням їх використання. Для зменшення ризиків пропонується правильний підхід, що передбачає створення процесів для використання, управління та виходу з хмарних сервісів. Така стратегія допомагає забезпечити захист даних і ефективно керувати безпекою під час користування цими сервісами.

3. Готовність інфомаційно-комунікаційних технологій до безперервності бізнесу - ключовий аспект забезпечення стійкості організація у випадку збоїв чи непередбачених подій. Він визначає процеси реагування, відновлення та аналізує ключові показники. Це допомагає забезпечити, те що організації мають достатню готовність до інфомаційно-комунікаційних технологій для підтримки безперервної роботи у складних ситуаціях.

4. Моніторинг фізичної безпеки є важливим для захисту критично важливих даних. Це включає розгортання систем відеоспостереження, датчиків руху та замків з захистом від несанкціонованого доступу, щоб запобігти неповідомленому проникненню в обмежені зони.

5. Керування конфігураціями важливо для забезпечення безпеки організації. Воно дозволяє налаштувати обладнання, програмне забезпечення та мережу з відповідними політиками захисту. Це включає встановлення правил мережевої безпеки, таких як списки блокувань і переадресація портів, а також забезпечує відповідність з вимогами стандартів безпеки.

6. Видалення інформації відіграє ключову роль у зниженні ризику даних, сприяючи зменшенню можливих порушень безпеки та відповідності законодавству. Він забезпечує відповідність з правовими нормами стосовно стратегій стирання даних, використовуючи сучасні методи збереження даних організації.

7. Маскування даних є ефективним заходом для захисту ідентифікаційної інформації в системах організації. Цей метод включає контроль доступу та шифрування конфіденційних даних, щоб ускладнити їх доступність. Маскування даних виходить за рамки звичайних заходів контролю доступу і може вимагатися для дотримання законодавства або нормативних вимог.

8. Запобігання витоку даних є дуже важливим для захисту організацій від вразливостей. Впровадження контролю є превентивним і детективним заходом, який допомагає активно виявляти, запобігати та реагувати на витоки даних з будь-яких джерел, як внутрішніх, так і зовнішніх.

9. Мережевий моніторинг є важливим для IT-підтримки та інформаційної безпеки, забезпечуючи головну частину стратегії захисту. Контроль дозволяє виявляти і реагувати на незвичайні дії, швидко вирішувати інциденти, підвищувати продуктивність систем і захищати цінні активи від кібератак.

10. Веб-фільтрація - важливий інструмент контролю, який допомагає організаціям захищати свої інформаційні системи від шкідливих веб-сайтів і

забезпечувати безпеку мережі. Цей процес також сприяє ефективному використанню ресурсів та зменшенню відволікання персоналу.

11. Безпечне кодування є важливим для захисту інформаційних систем від складних кіберзагроз. Впровадження контролю гарантує, що програми та мережі розробляються з урахуванням безпеки на кожному етапі, запобігаючи потенційним ризикам ще до їх виникнення. Це допомагає уникнути вразливостей, які можуть бути використані зловмисниками для атаки, таких як слабка генерація ключів чи недостатня перевірка введення даних [10].

Стандарт ISO/IEC 27005:2022 є важливим документом у галузі управління ризиками інформаційної безпеки. Він надає детальні вказівки та методологію для ефективної оцінки та управління ризиками в інформаційних системах. Цей стандарт визначає процеси та підходи до ідентифікації, аналізу та оцінки ризиків, а також надає рекомендації з впровадження заходів для зменшення ризиків. Його впровадження допомагає організаціям ефективно захищати їхню інформацію та забезпечувати стійкість їхніх інформаційних систем перед сучасними загрозами. Кожен з цих етапів має велике значення для забезпечення безпеки інформації та захисту корпоративних ресурсів. Даний стандарт зосереджений на процесі управління ризиками інформаційної безпеки та циклах управління ризиками, надаючи зрозуміле керівництво, крок за кроком приводячи через процес і використовуючи наведений рисунок процесу, який можна побачити на рис. 1.5.

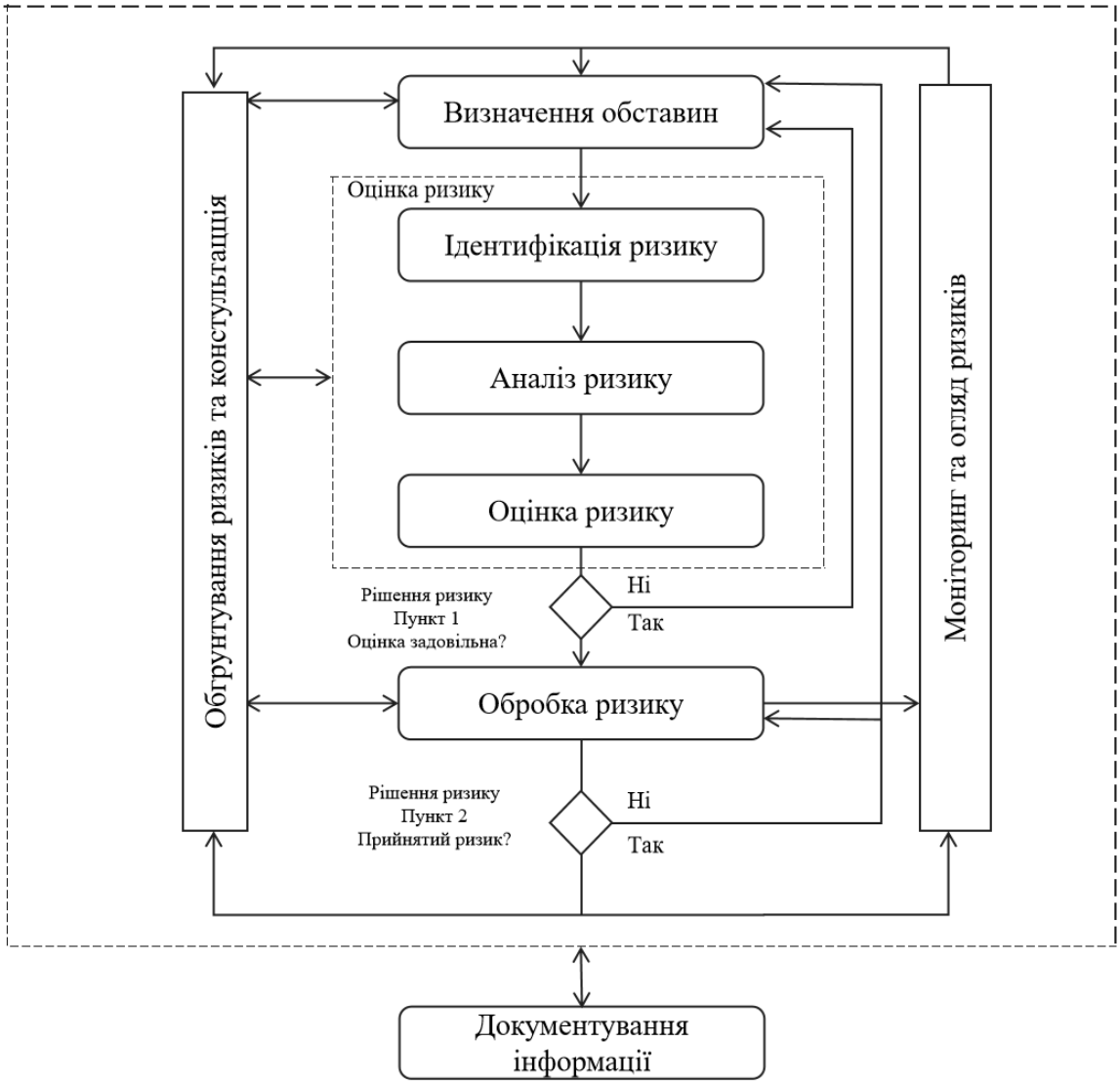

Рис. 1.5 – Схема алгоритму дій з управління ризиками ІБ відповідно до ISO/IEC 27005

Цей рисунок сприяє уникненню плутанини і розрізненню різних аспектів управління ризиками. Також важливо відзначити, що стандарт включає дві точки прийняття рішень щодо ризиків, що робить його унікальним у порівнянні з іншими стандартами ISO у сфері управління ризиками [11].

Однією з важливих вимог ISO/IEC 27005:2022 є здійснення оцінки ризиків, яка включає ідентифікацію потенційних загроз для безпеки інформації, визначення вразливостей системи та оцінку можливих наслідків. Цей процес допомагає визначити ймовірність виникнення певних загроз і їхній вплив на організацію. Крім того, стандарт рекомендує проводити процеси оброблення

ризиків, які включають у себе розроблення стратегій з управління ризиками, прийняття рішень про прийняття чи зменшення ризиків, а також моніторинг і перегляд ризиків у часі. Також встановлюються методи визначення прийнятного рівня ризику, що допомагає організаціям визначити, коли заходи з управління ризиками є необхідними. Інтеграція з іншими стандартами, такими як ISO/IEC 27001:2022, дозволяє організаціям впроваджувати цілісну систему управління ризиками та інформаційною безпекою згідно з міжнародними стандартами. Таким чином, ISO/IEC 27005:2022 надає комплексний підхід до управління ризиками інформаційної безпеки, що допомагає організаціям ефективно захищати свою інформацію та даних від потенційних загроз [12].

Загалом нормативні документи, що регулюють управління ризиками інформаційної безпеки, допомагають керівництву організації управляти ризиками ефективно та системно. Вони надають не лише вказівки для впровадження безпекових заходів, а й конкретні рекомендації для реагування на різноманітні загрози інформаційної безпеки. Докладний аналіз інформаційних ризиків, їх оцінка та управління є ключовими етапами, які допомагають підтримувати стабільність та надійність інформаційних систем. Ці нормативні документи також надають рекомендації щодо того, як організація може адаптувати свої заходи безпеки до конкретного контексту і потреб. Вони враховують специфіку діяльності різних секторів, що дозволяє розробити індивідуалізовані стратегії забезпечення безпеки. Такий підхід дозволяє організаціям ефективно захищати свою інформацію, мінімізуючи можливі ризики та вплив інцидентів на діяльність. На відміну від загальних рекомендацій, нормативні документи конкретизують процеси управління ризиками, надаючи конкретні інструкції для дій. Вони визначають ролі та відповідальність осіб у процесі управління ризиками та рекомендують етапи, які потрібно пройти для забезпечення ефективного контролю за безпекою. Такий підхід сприяє реалізації систематичних заходів безпеки, що є важливим для дотримання вимог стандартів та забезпечення безпеки інформації на всіх рівнях організації.

1.3 Аналіз досвіду у виявленні загроз, вразливостей та можливих наслідків порушень інформаційної безпеки

Важливою ціллю інформаційної безпеки є захист даних, які збирає та обробляє організація. Коли дані залишаються незахищеними, будь-хто може мати до них доступ. Це може призвести до серйозних наслідків для бізнесу, включаючи витік чутливої інформації та завдання шкоди. Системи інформаційної безпеки спрямовані на забезпечення захисту цих даних відповідно до вимог бізнесу та законодавства, застосовуючи відповідні заходи для забезпечення конфіденційності, комерційних таємниць та запобігання крадіжці інформації [13].

Загалом, технології, що використовуються у фінансовому секторі, призводять до зростання обсягів даних та змінюють способи їх зберігання й обробки. Це створює нові можливості для кіберзлочинців, які можуть використовувати різноманітні методи атак для зламування систем і отримання незаконного доступу до конфіденційної інформації. В умовах обмежених фінансових ресурсів організаціям необхідно ретельно вирішувати, як найефективніше розподілити свої ресурси для зниження ризиків і захисту від можливих загроз безпеки. Основна мета цього процесу полягає у визначенні того, як організації вирішують питання розподілу своїх ресурсів у сфері безпеки. Якісний аналіз ризику включає визначення джерел та причин ризику, а також етапів і робіт, на яких виникає ризик, тобто виявлення потенційних зон ризику. Він також передбачає ідентифікацію всіх можливих ризиків, визначення практичної користі та можливих негативних наслідків, які можуть виникнути під час реалізації рішення, що містить ризик [14].

Крім того велика кількість фінансових транзакцій та чутливих даних у цьому секторі роблять його особливо привабливим для кіберзлочинців. Також у сфері електронної комерції існують великі ризики, пов'язані з обробкою платіжних даних, особистої інформації клієнтів та інших конфіденційних даних.

Це створює потенційно вразливі точки в інформаційних системах, які можуть бути використані для несанкціонованого доступу та злому.

Ризик інформаційної безпеки складається з декількох важливих елементів, це:

- Суб'єкт загрози - це людина або система, яка може використовувати вразливість.
- Вразливість - це слабке місце в системі, яке може бути використане зловмисником.
- Результати - це наслідки використання вразливості.
- Вплив - це наслідки небажаних результатів [15].

Проаналізувавши досвід минулих порушень безпеки у цих секторах, можна виявити базові загрози та вразливості, такі як атаки з використанням шкідливих програм, фішинг, DDoS-атаки, витоки даних через недоліки в захисті, які зображені в таблиці 1.1. Розуміння цих загроз, їхніх можливих наслідків та заходів пом’якшення дозволяє розробляти та впроваджувати ефективні стратегії захисту, які включають у себе технічні, організаційні та правові заходи.

Таблиця 1.1

Загрози та вразливості спрямовані на ІБ

Тип кіберзагроз	Опис	Можливі наслідки	Заходи пом'якшення
Шкідливе програмне забезпечення	Програми, призначенідля завдавання шкоди комп'ютерам або крадіжки інформації.	Втрата даних, фінансові втрати, шкода репутації, порушення роботи комп'ютера	Використовувати антивірусне та антішпігунське програмне забезпечення. Регулярно оновлювати програмне забезпечення. Не завантажувати файли з ненадійних джерел. Не відкривати підозрілі вкладення в електронних листах. Не переходити за посиланнями в них.

Продовження таблиці 1.1

Тип кіберзагроз	Опис	Можливі наслідки	Заходи пом'якшення
Фішинг	Шахрайські електронні листи, веб-сайти, текстові повідомлення, які намагаються обманом змусити людей розкрити особисту інформацію або виконати дії, які можуть завдати шкоди.	Розголошення конфіденційної інформації, фінансові втрати, зараження комп'ютера шкідливим програмним забезпеченням	Не відкривати підозрілі електронні листи, веб-сайти або текстові повідомлення. Не переходити за посиланнями в них. Не вводити особисту інформацію на незнайомих веб-сайтах. Використовувати антивірусне програмне забезпечення.
DDoS-атаки	Затоплення веб-сайту або сервера трафіком, щоб зробити його недоступним для законних користувачів.	Фінансові втрати, втрата репутації, простої	Використовувати служби захисту від DDoS-атак. Налаштувати брандмауер. Регулярно оновлювати програмне забезпечення. Співпрацювати з провайдером хостингу.
Витоки даних через недоліки в захисті	Несанкціонований доступ до конфіденційної інформації через вразливості в системах безпеки.	Втрата даних, фінансові втрати, шкода репутації, штрафи	Проводити регулярні тести на проникнення. Виправляти вразливості в системах безпеки. Шифрувати дані. Контролювати доступ до даних. Навчати персонал кібербезпеці.

Аналізуючи ці загрози, можна виявити спільні вразливості, такі як недостатній рівень свідомості персоналу щодо безпеки, використання слабких паролів або недостатня використання двофакторної аутентифікації.

Аналіз допомагає виявляти потенційні наслідки порушень безпеки, такі як фінансові втрати, пошкодження репутації організації,втрата довіри клієнтів, розголошення конфіденційної інформації, зараження обладнання шкідливими вірусами. Втрати можуть бути дуже значними, особливо коли йдеться про інформацію про клієнтів або фінансові дані. Наприклад, втрата клієнтської інформації може призвести до великих втрат відшкодувань, а також до втрати довіри та репутації, що може серйозно вплинути на довгострокову прибутковість організації. За допомогою попереднього аналізу можна розробляти стратегії превентивних заходів та готовності до відновлення після інцидентів. Це означає, що організації повинні мати плани відновлення даних та процесів після інцидентів безпеки, що допоможе мінімізувати час простою та втрати. Зменшення потенційних втрат та ризиків є важливим для забезпечення стійкості фінансового підприємства в умовах постійно зростаючих загроз інформаційної безпеки.

Застосування передових методів захисту даних, таких як моніторинг та виявлення відхилень, а також регулярне навчання персоналу з питань безпеки є дуже важливими компонентами ефективної стратегії інформаційної безпеки. Лише поєднання технологічних і організаційних заходів може забезпечити надійний захист в умовах постійно зростаючих загроз ІБ.

Для наглядного прикладу, можна використати стандарт ISO/IEC 27032:2012, який вносить значне розширення в загальну модель ризику, обумовлюючи ймовірність, як важливу позицію для загроз та вразливостей. Це надає можливість проводити аналіз стану інформаційної безпеки в екстрених ситуаціях: навіть у випадках, коли загрози не є значними, якщо вразливості відсутні, ймовірність реалізації ризику стає нульовою. Даний аспект являє собою розуміння та аналізі стану інформаційної безпеки, оскільки він враховує не лише наявність потенційних загроз, але й можливість їх реалізації через наявність вразливостей.

Аналізуючи стандарт ISO/IEC 27032:2012, можна підкреслити що він допомагає компаніям не лише ідентифікувати загрози, але й оцінювати рівень

вразливостей, що є необхідним для правильного аналізу інформаційної безпеки. Цей підхід дозволяє краще розуміти потенційні ризики та приймати ефективні рішення з покращення безпеки. Інформаційна безпека є більш ніж технічним захисту, вона також є стратегічним підходом до управління ризиками та забезпечення стійкості бізнесу в умовах непередбачуваних загроз. Це вимагає систематичного аналізу загроз, виявлення вразливостей та розробки відповідних заходів для їх запобігання. Тільки таким чином організації можуть гарантувати безпеку своїх даних та забезпечити успішну [16].

Також важливим аспектом для стратегії забезпечення інформаційної безпеки є виконання розвідування загроз. Її метою є не лише виявлення існуючих загроз, але й передбачення та протидія новим та невідомим атакам. Розвідка загроз охоплює комплексний процес збору, аналізу та обміну інформацією про суб'єкти загроз, їх тактики, методи та процедури, вразливості та індикатори компрометації. Завдяки розвідці загроз, організації можуть своєчасно виявляти потенційні небезпеки та приймати превентивні заходи для мінімізації ризиків. Рішення, побудовані на розвідці, забезпечують можливість активно реагувати на загрози, визначати пріоритети безпеки та посилювати загальний стан безпеки.

Аналіз ризиків ІБ являю собою стратегією управління ризиками, спрямованою на зменшення можливих наслідків порушень безпеки, які загрожують інформаційним активам. Ці порушення можуть мати різні форми, включаючи внутрішні та/або зовнішні загрози [17].

Розглядаючи більш детально, та оглядаючи зовнішні загрози можна виявити що вони становлять серйозну небезпеку для безпеки організацій. Це передбачає атаки, які виконуються ззовні мережі організації, з метою отримання несанкціонованого доступу до її ресурсів та інформації. Відповідно до мотивації та цілей зловмисників, зовнішні атаки можуть призвести до серйозних наслідків для бізнесу. Такі атаки часто орієнтовані на крадіжку важливої інформації, такої як фінансові дані, за допомогою вірусів чи

шкідливих програм. Також важливим є те, що такі атаки часто виконуються досвідченими хакерами, що становить серйозне загрозу для безпеки організацій.

Зовнішні атаки можуть призвести до різних наслідків, включаючи втрату конфіденційної інформації, фінансові втрати або порушення репутації організації. Ці наслідки можуть бути особливо серйозними через складність виявлення та обмеження контролю над зовнішніми атаками. Аналізуючи попередній досвід для захисту від зовнішніх загроз організаціям рекомендується використовувати широкий спектр заходів, таких як програмне забезпечення для виявлення вторгнень, шифрування даних та постійний моніторинг мережі. Також важливо надавати тренування на практиці для персоналу, що б вони розпізнавали фішингові атак та інші види соціальної інженерії, щоб забезпечити комплексний захист від зовнішніх загроз.

В той же час внутрішні загрози можуть виникнути коли особи, близькі до організації, навмисно або ненавмисно зловживають доступом до її мережі, щоб негативно вплинути на критично важливі системи або дані. Наприклад, можливе ненавмисне розсилання даних клієнтів зовнішнім сторонам, натискаючи на фішингові посилання в електронних листах або розповсюдження своїх облікових даних. Крім того, підрядники, ділові партнери та сторонні постачальники також можуть становити внутрішні загрози. Деякі інсайдери можуть намагатися обійти заходи безпеки через зручність або необдумані спроби бути більш продуктивними. У свою чергу, зловмисні інсайдери можуть навмисно порушувати протоколи кібербезпеки, щоб викрасти або знищити дані, або завдати іншої шкоди бізнесу. Також втрата даних та їх витік є ще однією серйозною внутрішньою загрозою. Більшість порушень безпеки виникають через людські помилки, такі як випадкове видалення або втрата носіїв інформації. Також через слабкі заходи кібербезпеки та небезпечні практики можуть призвести до кібератак чи навіть фізичного доступу до обладнання. Прикладом цього є відкриті сервери або комп'ютери, які можуть стати об'єктом крадіжки чи зміни налаштувань системи. Також, працівники, які неналежно переглядають шкідливі веб-сайти або завантажують вірусні файли,

можуть спричинити інциденти кібербезпеки без усвідомлення наслідків своїх дій [18].

Для захисту від внутрішніх загроз загалом встановлюють строгі політики безпеки та регулярно навчають персонал щодо правил безпеки та практик уникнення ризиків, також важливо проводити регулярні аудитувати та моніторити доступ до систем і даних, щоб вчасно виявляти та запобігати можливим загрозам.

Щоб запобігти внутрішнім загрозам, організації часто вжити заходи такі як:

- Обмеження доступу співробітників до конкретних ресурсів, необхідних для виконання своєї роботи.
- Навчання нових співробітників і підрядників обізнаності про безпеку, перед тим, як дозволии їм доступ до мережі.
- Налаштування підрядникам тимчасові облікові записи, термін дії яких закінчується в певні дати.
- Запровадження двофакторної автентифікації.
- Встановлення програмненого забезпечення для моніторингу співробітників, щоб зменшити ризик витоку даних і крадіжки інтелектуальної власності, виявляючи недбайливих, незадоволених або зловмисних інсайдерів.

Загалом запобігання внутрішнім загрозам - це постійний процес, який вимагає уваги та вдосконалення з часом [19].

Порівнюючи внутрішні та зовнішні загрози для організацій, очевидно, що обидва типи атак можуть призвести до серйозних наслідків. Хоча внутрішні атаки можуть здатися менш страшними через можливість контролювати внутрішні процеси, але вони все одно становлять значний ризик. Строгі правила безпеки можуть запобігти більшості внутрішніх загроз. Проте зовнішні атаки, зокрема на безпеку даних, так само небезпечні. Більшість таких атак спрямовані на порушення та використання інформації організації. Тому

важливо звертати увагу на будь-які підозрілі дії та вжити відповідні заходи безпеки, щоб захистити мережеві периметри від зовнішніх загроз.

Усі організації, потребують захисту від кібератак та загроз. Надійний захист інформації не лише забезпечує впевненість у тому, що дані організації та клієнтів захищені, але й зменшує вразливість до експлуатації ворожими силами та допомагає розвивати бізнес.

Додатково організації повинні регулярно збирати та оцінювати інформацію щодо вразливостей, що можуть вплинути на інформаційні системи та мережі. Оперативне вживання заходів щодо виправлення чи мінімізації цих вразливостей є вкрай важливим для запобігання злочинної діяльності.

Зазвичай обумовлюються декілька причин, що роз'яснюють важливість управління вразливістю. Це те що стрімке зростання кіберзлочинності ставить підвищений тиск на організації, змушуючи їх приділяти більше уваги інформаційній безпеці, а також ефективне усунення вразливостей допомагає попередити можливість втрати даних, порушення безпеки, що можуть серйозно пошкодити репутацію та фінансовий стан організації.

Управління вразливістю повинно являти собою частину загальної стратегії управління інформаційними ризиками. Це означає, що організації повинні розробляти та впроваджувати систематичний підхід до ідентифікації, оцінки, моніторингу та управління вразливостями у всіх аспектах своєї діяльності. Впровадження такого підходу дозволяє організаціям підвищити рівень захисту інформаційних систем та зменшити ризики кіберзагроз. Але якщо буде приділена недостатня увага до управління вразливістю, кіберзлочинці можуть використовувати вразливості, щоб отримати доступ та здійснити несанкціоновані дії у системах організації. Вразливість - це певний недолік інформаційної системи, який може бути використаний кіберзлочинцями для різноманітних цілей, таких як запуск кодів, отримання доступу до системної пам'яті, встановлення шкідливого програмного забезпечення, крадіжка даних, повне знищення або зміна корпоративних даних компанії. Аналізуючи попередній досвід, якщо в системі існують вразливості в програмному

забезпеченні, кіберзлочинець може скористатися цим, щоб виконати атаку віддаленого виконання коду або виконати атаку через впровадження шкідливого програмного забезпечення. Такі атаки можуть призвести до отримання несанкціонованого доступу до системи або навіть до повного контролю над нею. До того ж, використання вразливостей може призвести до втрати конфіденційності, цілісності та доступності даних. До прикладу, зловмисник, який отримав доступ до системи через вразливість, може вкрасти конфіденційні дані клієнтів або спотворити корпоративну інформацію.

Для цього виявлення вразливостей можуть використовуватися спеціальні програмні засоби, такі як сканери, які сканують інформаційні системи, веб-додатки та мобільні пристрої на предмет наявності відомих вразливостей. Цей допомагає ідентифікувати потенційні ділянки, які можуть бути використані кіберзлочинцями. Після виявлення вразливостей проводиться їх оцінка, включаючи визначення рівня загрози та потенційних наслідків атаки. На основі цієї оцінки встановлюються пріоритети у виправленні вразливостей. Після визначення пріоритетів здійснюється виправлення вразливостей. Це може включати усунення недоліків у програмному забезпеченні, оновлення конфігурацій, а також впровадження додаткових заходів захисту. Нарешті, проводиться складання звітів про вразливості, що містять інформацію про виявлені проблеми, їх оцінку та виправлені дії. Ці дії допомагають організаціям відстежувати та контролювати стан інформаційної безпеки.

Процес управління вразливістю є циклічним, оскільки з часом виникають нові вразливості. Тому цей процес вимагає постійної уваги та підтримки, але він дозволяє організаціям ефективно управляти ризиками і підвищувати рівень безпеки.

Загалом використовується декілька способів щоб контролювати вразливості:

- Усунення вразливості, якщо це можливо.
- Якщо усунення вразливості неможливе, можна зменшити ймовірність її використання або зменшити наслідки її експлуатації.

- Прийняти ризик і не реагувати.

Але один із найважливіших випадків є вразливість нульового дня, коли організація не може захистити себе від конкретних наслідків цієї невідомої вразливості. В таких випадках розробка стратегій для зменшення ймовірності та впливу може бути надзвичайно складною.

Отже, підсумовуючи попередній досвід, управління вразливістю відіграє важливу роль у забезпеченні безпеки інформаційних систем. Цей процес охоплює кілька ключових етапів, що включають виявлення, оцінку, розстановку пріоритетів, виправлення та складання звітів про вразливості [20].

За допомогою аналізу попередніх дослідів, організації не лише реагують на поточні загрози, але й попереджають подібні атаки в майбутньому. Також команди для забезпечення безпеки можуть виявляти патерни та тенденції, що допомагають у вдосконаленні своїх заходів захисту. Вони можуть визначати найбільш ймовірні сценарії ризику та розробляти відповідні стратегії для їхнього запобігання або зменшення. Також дуже важливим є мінімізація наслідків, як можуть виникнути після порушень в інформаційної безпеки, яке може нанести велику шкоду для організації. Перш за все, порушення може призвести до втрати конфіденційної інформації. Тому важливо мати належні заходи захисту та механізми виявлення та реагування на подібні загрози та вразливості для запобігання таким наслідкам.

Таким чином, систематичний аналіз досвіду у виявленні загроз, вразливостей та можливих наслідків порушень інформаційної безпеки є ключовим елементом ефективного управління інформаційною безпекою в фінансовому секторі та електронній комерції.

Висновок до розділу 1

У розділі було детально розглянуто чотири ключові етапи управління ризиками в галузі інформаційної безпеки: аналіз, оцінка, зниження ризику та оцінка вразливостей. Основна мета системи інформаційної безпеки полягає в

забезпеченні стабільності функціонування та захисті від різноманітних загроз, таких як витік, втрата, спотворення та знищення даних. Особлива увага приділяється вимогам нормативних документів, які визначають основи ефективного управління ризиками інформаційної безпеки, створюючи правовий та організаційний фундамент для ідентифікації, оцінки та мінімізації потенційних ризиків. Аналіз попереднього досвіду виявлення загроз та вразливостей підкреслив значимість систематичного підходу до оцінки ризиків у розробці ефективних стратегій захисту інформації. Цей процес сприяє передбаченню майбутніх загроз, ідентифікації ризиків та розробці стратегій їх уникнення, а також зменшенню можливих наслідків порушень безпеки.

Розділ 2 МЕТОДИЧНІ ПІДХОДИ ЩОДО АНАЛІЗУ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

У цьому розділі проводиться аналіз методів управління ризиками інформаційної безпеки організації та їх ефективності. Розглядається структура системи управління ризиками, можливості використання засобів захисту та вплив цих процесів на загальну ефективність.

2.1 Аналіз методики управління ризиками інформаційної безпеки організації

Для ефективного управління ризиками інформаційної безпеки використовуються різноманітні методики та підходи.

Одна з найпопулярніших та широко використовуваних методик управління ризиками - методика оцінки ризиків National Institute of Standards and Technology (NIST). Вона визначена у спеціальному керівництві NIST 800-30. Ця методика передбачає попередню оцінку двох ключових параметрів: потенційного збитку та ймовірності реалізації загрози.

Реалізація стандарту NIST 800-30 включає підготовку та проведення оцінок ризиків, аналіз і представлення результатів отриманої інформації, а також постійне супроводження процесу оцінки, щоб забезпечити актуальність і відповідність ризиків організації, зображені на рис. 2.1. [21].

Рис. 2.1 – Етапи впровадження NIST 800-30

Переваги методу NIST 800-30 полягають у його відносній простоті проведення заходів з оцінки ризиків та можливості адаптації до вимог конкретної організації, враховуючи її тип та розмір. Цей метод детально описує всі можливі ризики для інформаційних активів, а також передбачає використання різних способів обробки ризиків, таких як зниження, прийняття, перенесення та уникнення. Крім того, існує спеціальне програмне забезпечення, яке допомагає обробляти результати оцінки ризиків, використовуючи принципи методики.

Незважаючи на переваги, метод NIST 800-30 має деякі обмеження для застосування. По-перше, процес аналізу і оцінки ризиків може бути тривалим, що може вимагати значних часових та людських ресурсів. Крім того, оцінка ризиків проводиться лише за трирівневою шкалою, що може обмежувати точність та детальність отриманих результатів і виявитися недостатньою для

деяких організаційних потреб. Такі обмеження можуть потребувати додаткових уточнень або використання додаткових методів оцінки ризиків.

Методика CRAMM (CCTA Risk Analysis and Management Method), базується на стандартах управління інформаційною безпекою серії BS7799, які наразі перероблені в ISO 27000. Вона описує підхід до якісної оцінки ризиків, при якому перехід до шкали значень якісних показників відбувається за допомогою спеціальних таблиць, що визначають відповідність між якісними та кількісними показниками. Оцінка ризику проводиться на основі аналізу цінності IT-активу для бізнесу, вразливостей, загроз і ймовірності їх реалізації. Методика CRAMM поєднує якісні та кількісні методи оцінки ризиків, що робить її універсальною для різних типів організацій. Вона існує у версіях, спеціально адаптованих для комерційних та державних установ. Використання CRAMM дозволяє економічно обґрунтувати витрати на інформаційну безпеку, забезпечуючи фінансову ефективність та уникнення непотрібних витрат.

Методика CRAMM розбиває процедуру оцінки ризиків на три етапи. Перший етап визначає, чи потрібен детальний аналіз захисту системи. На другому етапі ідентифікуються та оцінюються ризики. Третій етап включає вибір контрзаходів. Кожен етап має свій набір інструментів та документів, що забезпечують систематичний та всеосяжний підхід до управління ризиками. Методика CRAMM допомагає організаціям ефективно розподіляти ресурси та мінімізувати ризики, забезпечуючи безперервність та стійкість їхньої діяльності. Високорівнева структура методології CRAMM представлена на рис. 2.2.

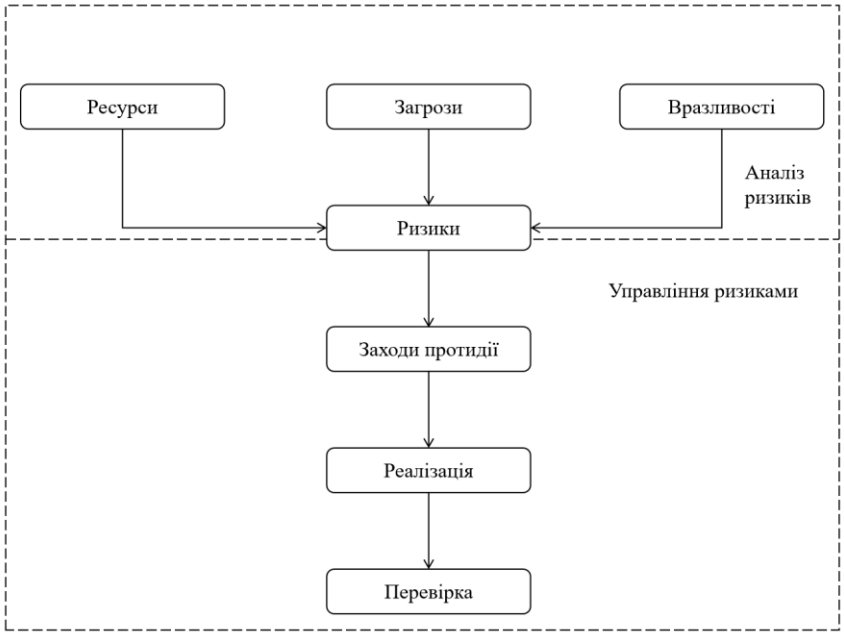

Рис. 2.2 – Високорівнева структура методології CRAMM.

Методологія ґрунтується на трьох основних етапах:

1. Оцінка цінності інформації та ідентифікація активів, що підтримують бізнес-процеси.

2. Визначення загроз, які можуть вплинути на систему, і оцінка вразливості системи до цих загроз. Наступним кроком є виведення показників ризику на основі поєднання загрози, вразливості та цінності активу. Показники ризику масштабуються, щоб встановлені вимоги до безпеки відповідали ступеню ризику.

3. Визначення можливих контрзаходів для зменшення ризиків, включаючи необхідні поліпшення існуючих контрольних заходів [22].

Метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), широко використовується як у комерційних, так і державних організаціях для оцінки ризиків інформаційної безпеки та управління ними. Ця методика передбачає проведення серії внутрішніх семінарів для оцінки критичних загроз, активів і вразливостей [23].

Організаційна методика OCTAVE складається з трьох основних фаз, які зображені на рис. 2.3:

1. Команда аналізує важливість активів для організації, визначає критичні активи та розробляє вимоги безпеки для них. Потім вона ідентифікує загрози для кожного критичного активу, створюючи профілі загроз.

2. Аналізується мережевий доступ та стійкість компонентів інформаційної інфраструктури до мережевих атак.

3. На основі аналізу ризиків для критичних активів команда розробляє стратегію захисту та плани пом'якшення наслідків для усунення ризиків [24].

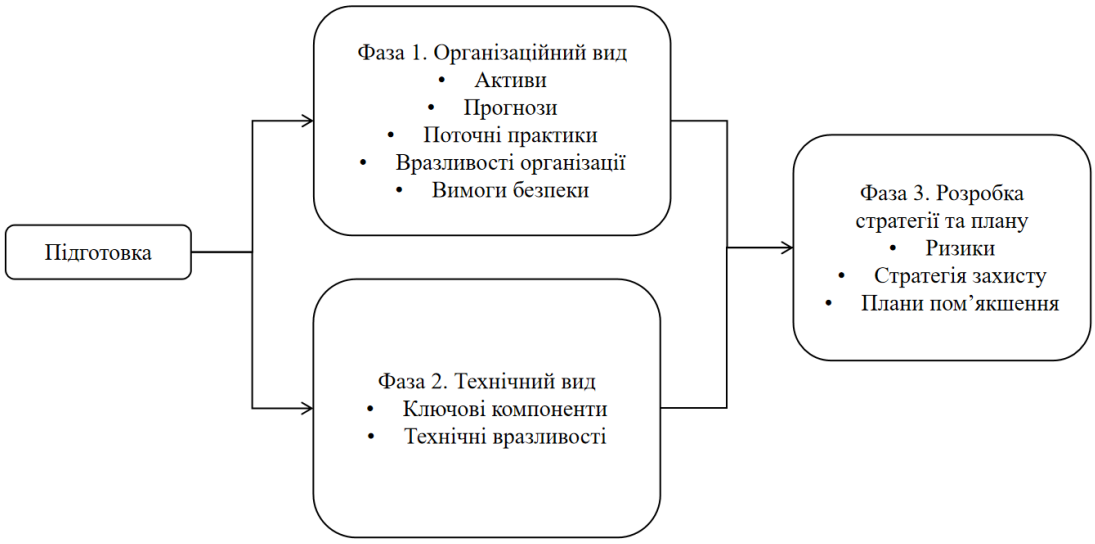

Рис. 2.3 – Процес управління ризиками OCTAVE

Метод COBIT 5 for Risk, розроблений ISACA, базується на передових стандартах управління ризиками, таких як COSO ERM, ISO 31000 та ISO\IEC 27000. Ця методологія спрямована на управління ризиками інформаційних технологій та пов'язаними з ними аспектами, детальна структура оформлена на рис. 2.4.

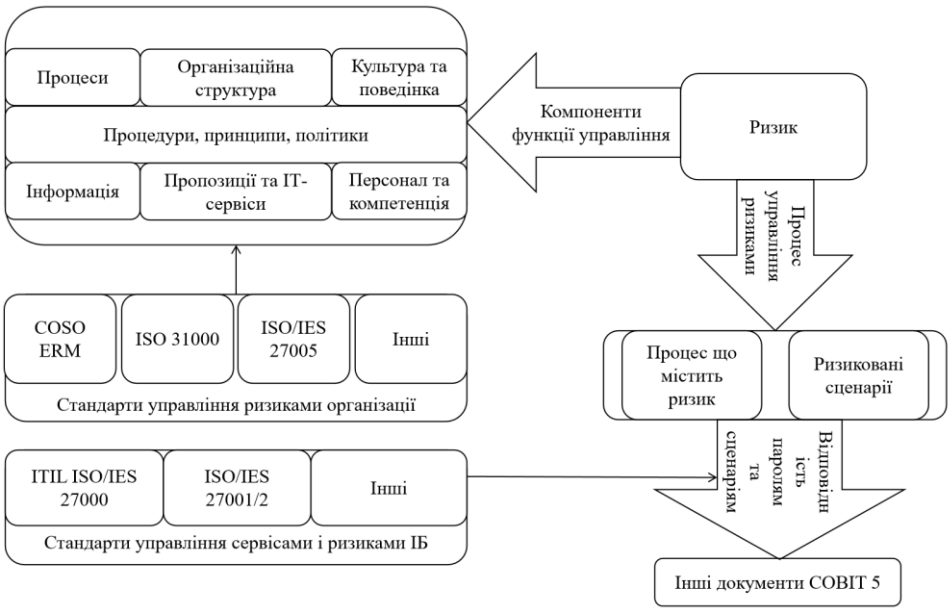

Рис. 2.4 – Структура методології COBIT 5

COBIT аналізує ризики інформаційної безпеки в контексті основної діяльності установи та надає підходи до впровадження управління цими ризиками в рамках процесів якісного аналізу та управління ризиками. Структура методології COBIT включає компоненти установи, які описують функції та процеси управління ризиками, можна побачити на рис. 2.4.

Рис. 2.4 – Компоненти установи опису функції та процесів управління ризиками за методологією COBIT

Ці компоненти включають процеси, організаційну структуру, культуру та поведінку, принципи політики, процедури, інформацію, пропозиції та IT-сервіси, персонал і компетенції.

В рамках процесу управління ризиками за методологією COBIT важливо враховувати різні компоненти, які впливають на ризики інформаційної безпеки та процес їх управління. Серед них:

1. Принципи політики та процедури організації.

2. Процеси, які відображають основні діяльності управління ризиками.

3. Організаційна структура, яка визначає ролі та відповідальності управління ризиками в установі.

4. Корпоративна культура, етика та правила поведінки, що впливають на сприйняття та управління ризиками.

5. Інформація, яка використовується для аналізу та прийняття рішень щодо ризиків.

6. IT-сервіси, інфраструктура та додатки, які можуть бути вразливими перед ризиками і потребують захисту.

7. Персонал з його досвідом і компетенціями, який відіграє ключову роль у виявленні та управлінні ризиками.

Ризикові сценарії стають основним елементом аналізу та управління ризиками за методологією COBIT. Кожен сценарій представляє собою опис події, яка, якщо вона виникне, може мати невизначений вплив, який може бути як позитивним, так і негативним, на досягнення цілей організації.

Метод COBIT містить більше 100 ризикових сценаріїв, які охоплюють різноманітні аспекти впливу, включаючи IT-проекти, управління програмами, інвестиції в IT, навички персоналу, інформацію, а також різні типи ризиків. Кожен сценарій класифікується за типами ризиків і містить інформацію про джерела, типи та можливі наслідки загроз. Аналізуючи ці ризики, організація приймає рішення про уникнення, прийняття, передачу або зниження ризиків.

Методика FRAP (процес аналізу ризиків за допомогою фасилітованого підходу), - це методологія аналізу та оцінки ризиків. Цей процес спрощений, але має структуровану форму, розроблену за допомогою знань проектних команд, які активно обговорюють шляхи протидії ризикам. Участь менеджерів або власників бізнесу є ключовою, оскільки вони володіють необхідними знаннями для мінімізації впливу на бізнес [25].

FRAP є методом аналізу ризиків у бізнесі та проектах, що ґрунтується на стандартах 17799/27002. Включає три етапи: Pre-FRAP (попередній аналіз та формування команди), FRAP (ідентифікація загроз, вразливостей та контрольних заходів) та Post-FRAP (аналіз результатів). На рис. 2.5 зображено основні частини FRAP, які допомагають у керуванні ризиками [26].

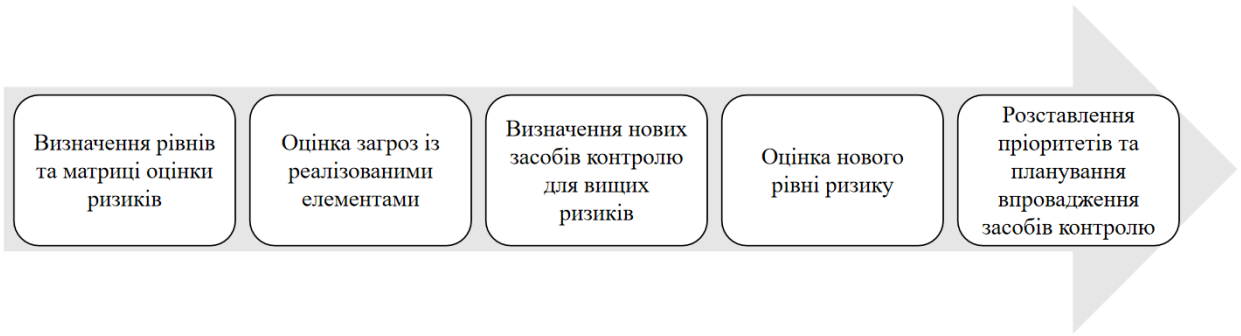

Рис. 2.5 – Основні частини FRAP для встановлення рівня ризику

Методика FRAP ґрунтується на проведенні сеансів виявлення загроз, які організовані командою з усієї організації. Перед FRAP проводиться підготовча зустріч для формування команди, під час сесії FRAP виявляються можливі загрози, а після неї проводиться аналіз та підготовка звіту. У підсумковому звіті команда FRAP визначає загрози та рекомендує заходи контролю для їх пом'якшення. Методика Facilitated Risk Analysis Process (FRAP) включає оцінку рівня ризику для незахищеної інформаційної системи, а також показує потенційний ефект від впровадження системи захисту інформації (СЗІ). Оцінка проводиться з урахуванням ймовірності виникнення загрози та її потенційного збитку за такими шкалами:

Ймовірність:

- висока - існує велика ймовірність, що загроза станеться у наступному році;
- середня - можливо, що загроза станеться у наступному році;
- низька - малоймовірно, що загроза станеться у наступному році.

Збиток:

- високий - можливість зупинки критичних бізнес-процесів, що призведе до значних втрат для організації, втрати репутації або значного зменшення прибутку;
- середній - короткочасне переривання критичних процесів або систем, що може призвести до обмежених фінансових втрат;
- низький - переривання в роботі, яке не спричиняє значних фінансових втрат.

Оцінка ризику визначається за допомогою матриці ризику. Дана матриця відображена в табл. 2.1.

Таблиця 2.1

Матриця ризику за методом FMEA

	Високий	Середній	Низький
Висока	A	B	C
Середня	B	B	C
Низька	B	C	D

Зверху відображен збиток, а з ліва його ймовірність.

A - виправлення має бути виконане миттєво.

B - виправлення слід виконати у найближчий час.

C - необхідно проводити моніторинг ситуації.

D - в ближайший час, виправлення не потрібне.

Метод FMEA є структурованим інструментом аналізу ризиків, спрямованим на виявлення потенційних відмов у процесах, продуктах або послугах та розробку стратегій для зменшення їхніх негативних наслідків. Він

використовується для планування дій з метою мінімізації ризиків. FMEA є однією з перших систематичних методик аналізу відмов і часто відома як PFMEA (Process Failure Mode and Effects Analysis) або FMEA процесу.

Налаштування FMEA включає кілька етапів:

1. Чітке визначення мети, обсягу, графіку та скласти команду для аналізу.

2. Розглядання структур систем, її елементи та функції.

3. Аналіз можливих несправностей, їх наслідків та причин.

4. Оцінка ризику для кожної виявленої несправності, враховуючи серйозність, виникнення та виявлення.

5. Визначення заходів контролю над важливими ризиками та оцінюється їх ефективність.

6. Узагальнюються даниі аналізу та повідомляються зацікавленим сторонам.

Під час оцінки ризику на п'ятому етапі враховуються три фактори: серйозність, виникнення та виявлення. Кожен фактор оцінюється від 1 до 10, і їх множення дає "число пріоритету ризику".

Загалом FMEA використовує три основних критерії для оцінки потенційних відмов:

1. **Тяжкість**: Визначає серйозність можливих наслідків для клієнта чи кінцевого користувача, рейтинг оцінюється від 1 до 10, де 1 - мінімальний ефект, а 10 - критичний результат.

2. **Частота**: Вимірює ймовірність виникнення відмови протягом терміну служби, рейтинг також від 1 до 10, де 1 - рідкісна подія, а 10 - майже певна.

3. **Виявлення**: Вказує на здатність виявлення або передбачення відмови перед її виявленням, також рейтингується від 1 до 10, де 1 - висока ймовірність виявлення, а 10 - майже непомічена.

Команда FMEA повинна досягти консенсусу щодо цих критеріїв для кожної відмови, використовуючи наявні дані для обґрунтування рішень. Головна мета - визначити пріоритетність ризиків і розробити ефективні стратегії управління ними [27].

Аналіз режимів і наслідків FMEA широко використовується для управління ризиками в різних галузях, спрямований на точне визначення джерел ризику та способів їх пом'якшення. FMEA ідентифікує потенційні збої системи та їх наслідки, оцінює вплив на якість або безпеку продукту і розробляє рекомендації для зниження ризику. Використання FMEA дозволяє уникнути збоїв та підвищити якість продукту чи процесу, формуючи культуру запобігання. Рис. 2.6. ілюструє процес FMEA, спрямований на виявлення можливих збоїв та їх наслідків [28].

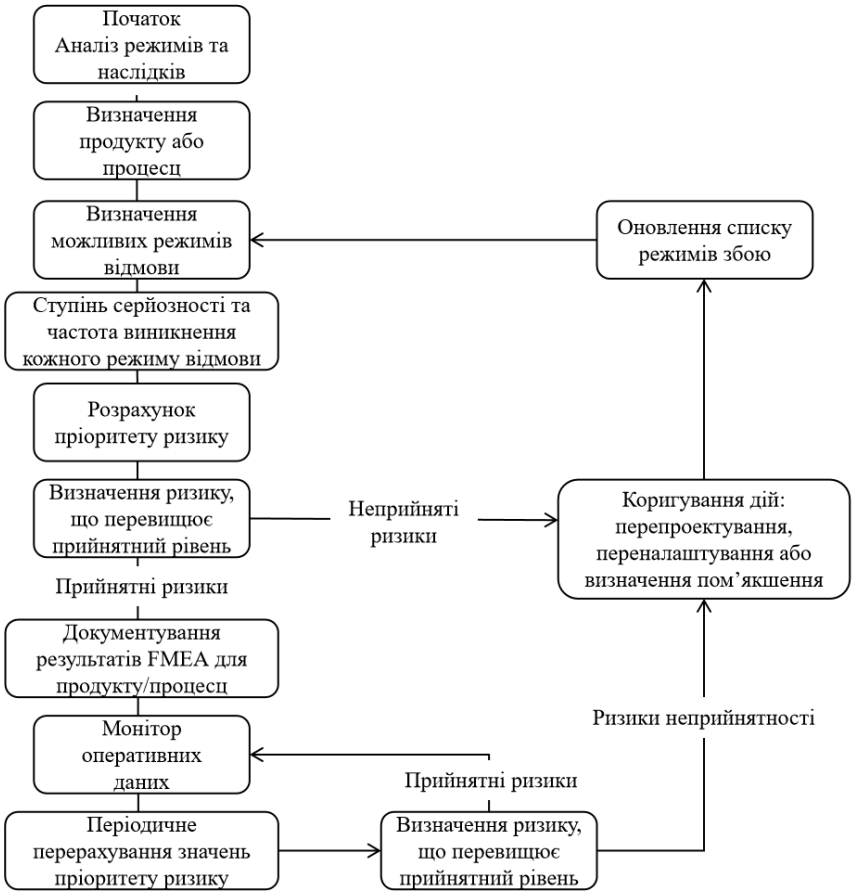

Рис. 2.6 – Виявлення можливих збоїв та їх наслідків при використанні методу FMEA

FMEA надає метод для ідентифікації можливих несправностей, їх наслідків та оцінки важливості. Ось детальна інструкція:

1. Вибір процесу для аналізу, де обертається проблемний процес.

2. Формування команди FMEA, де призначається завдання та мета проекту.

3. Опис процесу, де ретельно описується кожен етап.

4. Виявлення можливих несправностей, відображає збір ідей від команди про можливі проблеми на кожному етапі процесу.

5. Встановлення пріоритетів проблем, виконується оцінка того, які проблеми є найважливішими для вирішення.

6. Розробка та впровадження заходів, таких як планування і виконання змін для зменшення ризиків або наслідків несправностей.

7. Оцінка ефективності змін, зазвичай це перевірка того, чи були внесені зміни успішними у зменшенні ризиків.

Після завершення аналізу команда створює таблицю FMEA, де описані потенційні проблеми, їхні наслідки та рейтинги серйозності, виникнення та виявлення. Ці рейтинги використовуються для визначення пріоритетів у виправленні проблем.

FMEA визначає пріоритетність потенційних збоїв, враховуючи їхню виявленість, серйозність і частоту. Виявленість визначає складність виявлення несправностей, серйозність - важливість наслідків в разі невдачі, а частота - ймовірність того, що збій трапиться.

Основна мета FMEA - або усунути різні рівні ризику через пріоритетні заходи для усунення збоїв, або зменшити їх частоту та серйозність. Процес FMEA також допомагає у виборі заходів для пом'якшення наслідків і наслідків невдачі [29].

FAIR - це потужний інструмент для оцінки і управління ризиками, який допомагає організаціям ефективно захищати свою інформацію, також він надає кількісну оцінку ризиків, є стандартом для багатьох організацій і допомагає в управлінні ризиками, конвертуючи їх у грошові еквіваленти. Його використання сприяє ефективному виявленню та управлінню ризиками в будь-якій сфері бізнесу.

Методологія FAIR допомагає організаціям аналізувати кіберризики, встановлюючи зв'язок між експертами з кібербезпеки, бізнес-менеджерами та керівництвом. Вона дозволяє фінансово оцінювати ризикові сценарії,

створюючи таксономію ризиків і визначаючи ключові поняття. Методологія забезпечує кількісну оцінку ризику, аналіз взаємозв'язків між факторами ризику, відповідаючи на питання щодо ймовірності кіберподій, вартості шкоди, основних кіберризиків, ефективності контролю та страхування. FAIR також сприяє ефективному розподілу бюджету на кібербезпеку та вибору оптимальних заходів для зниження ризиків.

Модель оцінки ризиків FAIR складається з чотирьох етапів:

1. Ідентифікація активів і потенційних загроз.

2. Оцінка частоти виникнення збитків.

3. Аналіз основних і вторинних втрат.

4. Артикуляція ризиків і класифікація факторів ризику [30].

Методологія проекту USAID FAIR ґрунтується на моделі «частоти х величини», яка застосовна до всіх ситуацій і може бути експортована для всіх підприємств Ця модель ризику залишає особам, які приймають рішення, два способи зменшити схильність до збитків:

- зменшення LEF – кількості разів, коли відбуваються події втрат;
- зменшення розміру фінансових втрат, які можуть виникнути в результаті таких подій.

Таксономія ризиків, на основі якої можна схематизувати стандарт проекту USAID FAIR, показана на рис. 2.7. Факторний аналіз інформаційного ризику FAIR - єдина міжнародна стандартна кількісна модель інформаційної безпеки та операційного ризику

Загалом методологія FAIR розглядає ризик як невизначену подію, вимірюючи ймовірність та наслідки. Її фактори включають частоту виникнення загроз, уразливість та розмір втрат. USAID "FAIR" корисний для організацій, що мають інформаційні ризики, проте, варто пам'ятати, що це лише концепція, і власний аналіз також важливий [31].

Рис. 2.7 – Схема аналізу ризиків інформаційної безпеки за методикою FAIR

Аналізуючи всі методи, можна зазначити їх переваги та недоліки, які представлені в табл. 2.2.

Таблиця 2.2

Порівняння методик управління ризиками інформаційної безпеки

Методика	Переваги	Недоліки
NIST (Національний інститут стандартів і технологій)	1. Висока надійність та авторитетність 2. Сумісність з іншими стандартами 3. Придатна для організацій різного розміру 4. Детально описує всі можливі ризики для інформаційних активів	1. Складність та багатогранність 2. Необхідність адаптації до потреб організації 3. Довгостроковий процес аналізу
CRAMM (CCTA Risk Assessment and Management Method)	1. Простота та зрозумілість. 2. Використовує кількісні і якісні способи оцінки ризиків. 3. Можливість адаптації до потреб організації.	1. Недостатня гнучкість та деталізація. 2. Необхідність доопрацювання для деяких галузей. 3. Довгостроковий процес аналізу

Продовження таблиці 2.2

Методика	Переваги	Недоліки
OCTAVE (Operational Control Through Active Threat and Vulnerability Evaluation)	1. Можливість адаптації до потреб організації. 2. Сприяє прийняттю обґрунтованих рішень щодо захисту активів. 3. Придатна для організацій різного розміру та галузей зайнятості. 4. Швидке впровадження	1. Складність та трудомісткість впровадження. 2. Вимогливість до якості та повноти даних. 3. Необхідність залучення кваліфікованих фахівців. 4. Не дає кількісної оцінки ризиків.
FRAP (Framework for the Application of Risk Management to Information Security)	Простота та зрозумілість. 2. Наявність чіткої структури та етапів оцінки ризиків. 3. Можливість адаптації.	1. Недостатня гнучкість та деталізація. 2. Необхідність доопрацювання для деяких галузей.
FMEA (Failure Mode and Effects Analysis)	1. Приймає високий рівень складності. 2. Можна застосовувати єдину кількісну оцінку ризиків. 3.Вплив різних методів пом’якшення/виявлення можна легко змоделювати. 4. Простота та зрозумілість. 5. Підвищення надійності та безпеки.	1. Не враховує ймовірність виникнення відмов. 2. Не дає кількісної оцінки наслідків відмов. 3. Може бути трудомістким для складних систем. 4. Вимагає значних зусиль для встановлення чіткого виявлення термінів.
FAIR (Factor Analysis of Information Risk)	1. Висока точність та об'єктивність оцінки ризиків. 2. Можливість порівняння ризиків з різних категорій. 3. Сприяє прийняттю обґрунтованих рішень щодо управління ризиками. 4. Забезпечує значний захист від загроз.	1. Складність та трудомісткість впровадження. 2. Вимогливість до якості та повноти даних. 3. Необхідність залучення кваліфікованих фахівців. 4. Погано прогнозує та припускає ризики.

Загалом, кожна з цих методик має свої переваги та може бути адаптована відповідно до специфічних потреб організації. Вибір методики залежить від конкретних вимог та умов, але всі вони сприяють підвищенню рівня інформаційної безпеки через систематичний та обґрунтований підхід до управління ризиками.

2.2 Функціональна структура системи управління ризиками інформаційної безпеки організації і оцінка ефективності її функціонування

Інформаційна система управління ризиками організації складається з різних компонентів, включаючи програмне забезпечення, технічні засоби, бази даних, методології та кваліфікований персонал. Цей комплексний підхід дозволяє забезпечити захист інформаційних ресурсів, зберегти цілісність даних та забезпечити стійкість функціонування організаційних процесів.

У виробничому контексті підприємства важливо аналізувати потреби в робочій силі, структуру кадрів та кваліфікацію працівників для ефективного управління ризиками. При цьому важливо формувати організаційну структуру з урахуванням принципів ефективного управління, забезпечуючи оптимальний розподіл обов'язків, високу інформаційну забезпеченість керівництва та забезпечуючи взаємодію між виконавцями та керівництвом. Крім того, необхідно враховувати потреби підприємства у персоналі та оптимізувати систему заробітної плати та стимулювання працівників, забезпечуючи справедливе винагородження за виконану роботу [32].

Основна мета функціонування інформаційної системи управління ризиками організації полягає у підвищенні якості процесів управління ризиками та забезпеченні ризик-менеджерів необхідною та своєчасною інформацією для прийняття обґрунтованих рішень. Ця система допомагає організаціям ідентифікувати, оцінювати та керувати ризиками, мінімізуючи можливі негативні наслідки для бізнесу [33].

Головними завданнями інформаційної системи управління ризиками організації включають:

1. Ідентифікація ризиків, коли система дозволяє виявляти потенційні ризики на різних етапах бізнес-процесів.

2. Аналіз ризиків, передбачає що інформаційна система управління ризиками надає інструменти для оцінки ймовірності виникнення ризиків та їх потенційного впливу на діяльність організації.

3. Моніторинг ризиків, за допомогою нього виконується постійне відстеження виявлених ризиків та оновлення даних про їх статус.

4. Планування заходів, яке передбачає розробку та впровадження планів заходів для мінімізації або усунення ризиків.

5. Інформування та звітність, для цього інформаційна система управління ризиками забезпечує оперативне доведення інформації до користувачів (керівників, спеціалістів) у зручній формі, що дозволяє їм ефективно виконувати свої функції з управління ризиками [34].

Впровадження інформаційної системи управління ризиками сприяє покращенню загального управління організацією, підвищенню її стійкості до зовнішніх і внутрішніх загроз, а також забезпечує відповідність нормативним вимогам і стандартам. Мета впровадження системи управління ризиками на підприємстві полягає в підвищенні ефективності управління шляхом вчасного виявлення загроз загальній безпеці підприємства та досягнення конкретних цілей шляхом впровадження запобіжних заходів для нейтралізації ідентифікованих ризиків [35].

Результатом функціонування системи є надання кожному користувачеві релевантної інформації, яка за змістом, часом подання та методами відображення дозволяє ефективно виконувати свої функції та процедури управління ризиками. Це забезпечує проактивне управління ризиками, що є ключовим фактором успішної та безпечної діяльності організації в сучасному динамічному бізнес-середовищі.

Загалом функція управління ризиками - це ключовий елемент в системі управління організацією, спрямований на забезпечення того, щоб ризики, пов'язані з інформаційними системами, були розглянуті в контексті загальних стратегічних цілей і завдань організації. Ця функція співпрацює з керівництвом для розробки стратегії управління ризиками, обміну інформацією про ризики та забезпеченням належного контролю за діяльністю управління ризиками всередині організації. Основні завдання функції управління ризиками включають в себе розробку стратегії управління ризиками, надання консультацій та рекомендацій з управління ризиками, сприяння обміну інформацією про ризики всередині організації. Хоча функція управління ризиками не передбачає конкретної організаційної структури або формально призначеної відповідальності, керівництво має забезпечити, щоб ця функція була належно впроваджена та контрольована всередині організації.

Функціональна модель (див. рис. 2.8) є головним елементом створення інформаційної системи для автоматизації інформаційних процесів. Її аналіз надає результати у вигляді функціональної моделі, яка враховує контекст конкретної системи. Усі аспекти функціональної моделі, включаючи процеси, елементи і функції, виникають у результаті управлінських рішень та можуть бути представлені за допомогою різноманітних документів.

Рис. 2.8 – Функції управління ризиками в СУІБ

Система управління інформаційною безпекою є передусім системою документації, яка охоплює всі процеси, пов'язані з інформаційною діяльністю та інформаційними відносинами в організації. Ця документаційна система відповідає вимогам міжнародних стандартів серії ISO/IEC 27к і адаптується до структури організації, форми власності (приватної чи державної) та сфери її діяльності. Загалом використовується стандарт ISO/IEC 27001 який встановлює процеси для створення, впровадження та підтримки ефективної системи управління інформаційною безпекою. Цей процес охоплює розробку, впровадження, моніторинг, аналіз та підтримку системи управління інформаційною безпекою, яка враховує ризики, що виникають у контексті бізнесу організації. Використання системи управління інформаційною безпекою за стандартом ISO/IEC 27001 дозволяє організації зробити свої

інформаційні активи більш зрозумілими для менеджменту, виявити ключові загрози безпеки для бізнес-процесів та приймати обґрунтовані рішення на основі бізнес-цілей. При цьому система допомагає ефективно управляти інформаційною безпекою під час критичних ситуацій, забезпечує виконання політики безпеки та чітко визначає особисту відповідальність за її здійснення. Ця функціональна модель зображена на рис. 2.9.

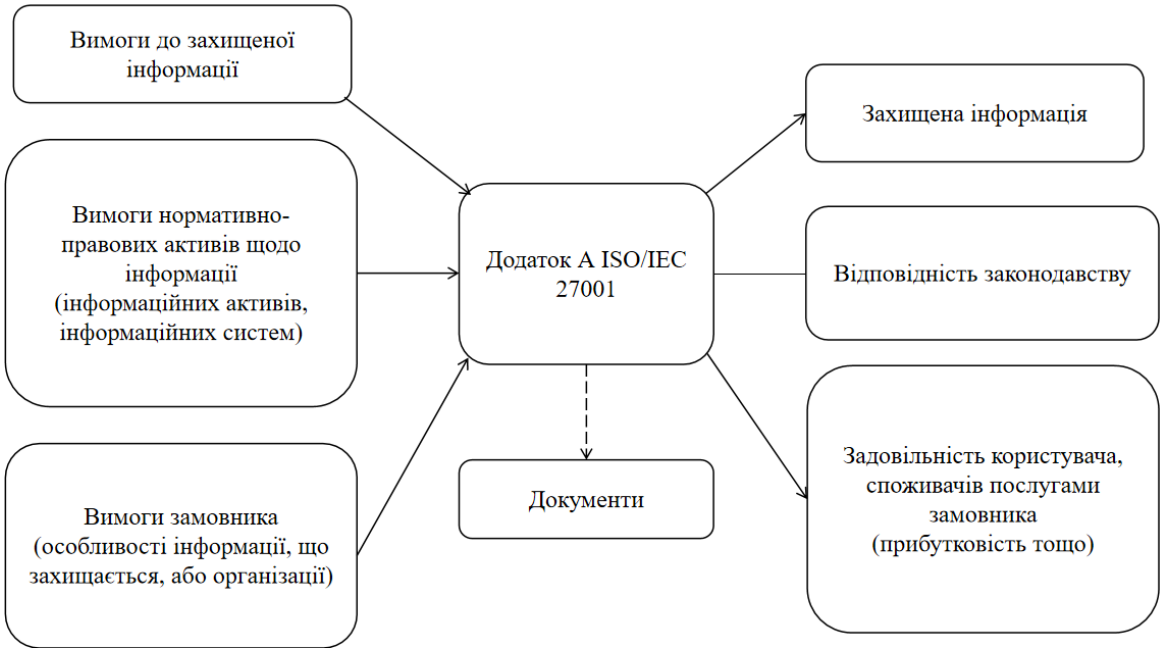

Рис. 2.9 – Функціональна схема забезпечення ІБ

Усі ці моделювання інформаційних процесів виникли від необхідності організацій створювати власні інформаційні системи для покращення забезпечення інформаційної безпеки. Вони дозволяють наочно відобразити всі компоненти інформаційного процесу в єдиній схемі функціонування організації. Для цього використовується ефективна та зручна методологія моделювання, яка забезпечує широкі можливості охоплення діяльності організації за допомогою моделювання всього технологічного процесу. Зокрема, запропонована функціональна модель використовує стандарти серії

ISO/IEC 27к, та додаток А ISO/IEC 27001 є системоутворювальним чинником, який поєднує елементи системи забезпечення інформаційної безпеки

організації. Також важливо зазначити що інформаційна безпека досягається завдяки впровадженню відповідного комплексу управлінських елементів, таких як політики, процеси, процедури, організаційна структура, програмне забезпечення та апаратні засоби. Ці елементи управління повинні бути ретельно розроблені, впроваджені, моніторені, переглянуті та, при необхідності, покращені, щоб забезпечити досягнення безпеки та виконання бізнес-цілей організації.

Побудова ефективної системи ІБ орієнтована на зниження зовнішніх та внутрішніх загроз, при цьому враховуються обмежені ресурси і час. Систему інформаційної безпеки організації можна розглядати як процес управління ризиками. Цей процес включає такі етапи:

1. Опис бізнес-процесів, включаючи коригування та аналіз їх. На основі критеріїв, визначених під час формування політики з управління ризиками, проводиться ідентифікація цих процесів.

2. Збір ризиків з метою виявлення загроз, які можуть призвести до значних негативних наслідків для підприємства. Для цього проводиться аналіз бізнес-діяльності.

3. Оцінка ризиків включає визначення характеристик ризиків та ресурсів інформаційної системи. Результатом є перелік потенційних ризиків з їх кількісними та якісними оцінками збитку і можливості реалізації, а також перелік ризиків, які не будуть відслідковуватися.

4. Планування заходів з мінімізації ризиків включає визначення термінів та переліку робіт. Виділяються організаційні, правові, організаційно-технічні, програмні та інженерно-технічні заходи.

5. Реалізація заходів передбачає виконання запланованих робіт, контроль якості результатів та виконання згідно з установленим графіком.

6. Оцінка ефективності полягає в системному процесі отримання та оцінки об'єктивних даних про поточний стан системи та рівень відповідності її дій певним критеріям.

Процес управління ризиками в системі ІБ організації, який зображений на рис. 2.10 включає в себе не лише опис бізнес-процесів та збір ризиків, але і опитування експертів предметної області. Цей етап спрямований на систематичне збирання експертних оцінок та думок фахівців щодо потенційних загроз і ризиків, які можуть вплинути на діяльність організації. Результатом даного процесу є класифікаційний перелік всіх потенційних ризиків, що дозволяє організації краще зрозуміти їхню природу та масштаби, а також визначити стратегії їх управління [36].

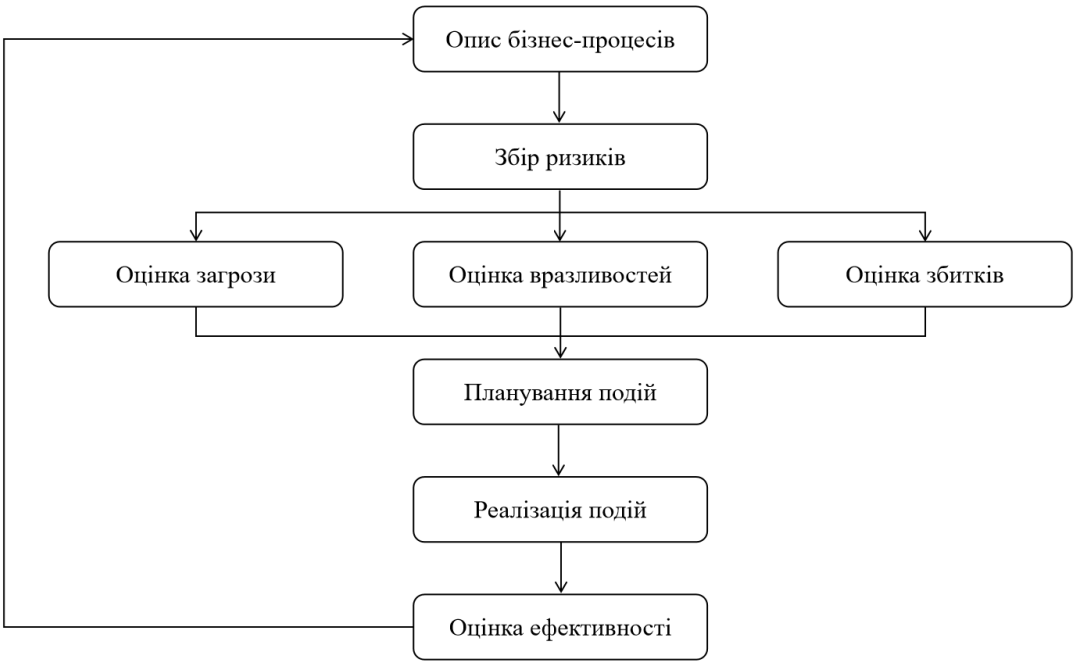

Рис. 2.10 – Схема процесу управління ризиками для ІБ

Система управління безпекою входить у загальну систему управління, яка ґрунтується на підприємницькому ризику та орієнтована на встановлення, впровадження, використання, моніторинг, підтримку та підвищення безпеки організації. Головною метою підсистеми управління безпекою організації є забезпечення необхідного рівня безпеки для функціональної повноти організації рис. 2.11 та захисту чутливих матеріалів. Цю мету можна досягти шляхом систематичного контролю виконавчої підсистеми безпеки.

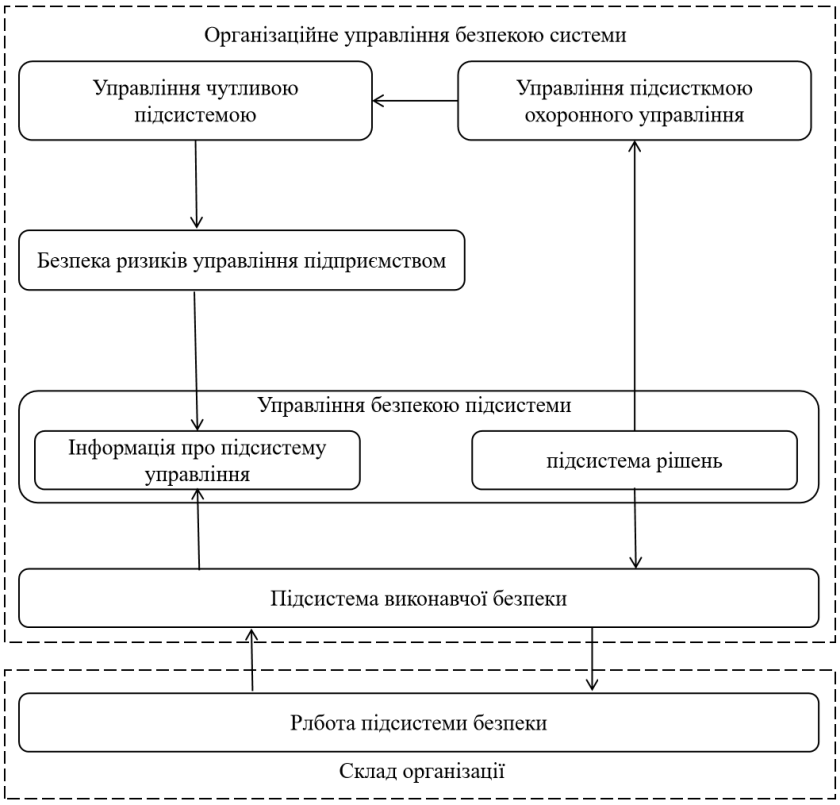

Рис. 2.11 – Функціональна структура системи безпеки

Підсистема управління безпекою організації складається з різних компонентів, таких як підсистема управління безпекою, виконавча підсистема, підсистема управління чутливими матеріалами, підсистема управління ризиками, технічна система та IT-системи. Процес управління безпекою має бути постійним, безперервним та постійно вдосконалюватися відповідно до плану, що включає в себе визначення рівня ризику та розробку стратегій управління цими ризиками.

Отже, ефективність системи управління ризиками інформаційної безпеки в організації є критично важливою для забезпечення безпеки даних та збереження довіри клієнтів і партнерів. Ця система базується на ретельній ідентифікації потенційних загроз і вразливостей, оцінці їх впливу на бізнес-процеси та розробці стратегій для мінімізації ризиків [37].

Ефективність цієї системи вимірюється її здатністю вчасно виявляти, запобігати та вирішувати потенційні загрози та інциденти безпеки. Постійний аналіз результатів та удосконалення процесів дозволяють підтримувати

високий рівень захисту інформації в умовах постійно змінюючогося оточення. Активна участь всіх структурних підрозділів організації є ключовою для успішної реалізації стратегій безпеки та мінімізації ризиків. Такий підхід забезпечує ефективне функціонування системи управління ризиками інформаційної безпеки та підвищує відповідальність організації перед своїми клієнтами та партнерами.

2.3 Оцінка можливостей використання організаційних і технічних засобів захисту інформаційної безпеки в процесах управління ризиками

Захист інформаційних ресурсів стає актуальною проблемою для багатьох підприємств. Розв'язання цієї проблеми вимагає комплексного підходу, що об'єднує організаційні та технічні заходи [38].

Для ефективного управління інформаційною безпекою в організаціях використовується комбінація технічних і організаційних рішень, що забезпечує надійний моніторинг стану системи захисту інформації. Інформаційний моніторинг являє собою процес безперервного спостереження за появою нових даних про діяльність об'єкта за визначеними інформаційними індикаторами у конкретній сфері. Його мета полягає у аналізі, управлінні і прогнозуванні розвитку ситуації на основі реальної інформації. Основною метою інформаційного моніторингу є оцінка поточного стану проблеми та моделювання варіантів її розвитку [39].

Організаційний захист інформації охоплює ряд заходів, спрямованих на налагодження взаємодії між співробітниками та забезпечення необхідного рівня моніторингу ІТ-систем і підсистем інформаційної безпеки. Ці заходи дозволяють формувати групи реагування на інциденти, складені з експертів різного рівня, і сприяють створенню операційного центру безпеки. Основними організаційними заходами в СУІБ, які забезпечують достатній рівень захисту будь-якого підприємства, є:

1. Організаційне використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації.

2. Організаційна робота з аналізу внутрішніх і зовнішніх (гібридних) загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту [40].

Організаційні засоби охоплюють різноманітні завдання, починаючи від розробки внутрішніх документів, які встановлюють правила роботи з технікою та комерційною інформацією, до проведення інструктажу та перевірки персоналу. Також вони включають в себе визначення зон відповідальності для уникнення неправомірного розголошення та використання даних та впровадження програмних засобів для захисту даних від копіювання або знищення. Крім того, організаційні засоби допомагають складати плани з відновлення систем у разі їхнього виходу з ладу. У свою чергу, організаційна оцінка - це процес, під час якого збирається інформація для виявлення сильних та слабких сторін організації, а також можливих можливостей та ризиків. Ця процедура допомагає зрозуміти першопричини проблем і допомагає організації рухатися вперед, підвищуючи ефективність та надійність захисту інформації та уникнення потенційних загроз і втрат. Переваги організаційної оцінки включають:

1. Оцінка допомагає виявити основні проблеми, які виникають у роботі організації.

2. Розуміння сильних і слабких сторін допомагає керівникам приймати більш обґрунтовані рішення для подальшого розвитку.

3. Оцінка допомагає зосередити ресурси на вирішенні основних проблем, що дозволяє ефективніше використовувати час і гроші.

4. Розуміння очікуваних показників та фактичних даних допомагає підвищити продуктивність співробітників шляхом оптимізації робочих процесів.

Організаційну оцінку можна проводити, залучаючи зовнішніх консультантів або коучів, які мають досвід у цій галузі. Вони детально

вивчають організацію, ідентифікують сильні та слабкі сторони та допомагають зосередитися на вирішенні проблем. Загалом основна мета полягає у вирішенні основної причини проблеми, що дозволяє досягти тривалих покращень, а не тимчасових заходів.

Організаційна оцінка починається з встановлення мети, чітко формулюючи цілі та результати, які потрібно досягти через оцінку. Розробляється план проведення оцінки з графіком та описом обов'язків і дій. Ключовий етап - збір даних про організацію, через опитування, інтерв'ю, аналіз фінансових та операційних даних, перевірку документів. Важливо звернути увагу на різні аспекти діяльності, включаючи стратегічні цілі, внутрішні процеси, комунікаційну культуру та ефективність управління. Після збору даних проводиться аналіз та оцінка, де визначаються основні сильні та слабкі сторони, а також можливості для поліпшення. На основі результатів аналізу розробляються рекомендації та плани дій. Для збору даних та отримання зворотного зв'язку можна використати програмне забезпечення для опитувань, провести інтерв'ю та фокус-групи. SWOT-аналіз допоможе виявити сильні та слабкі сторони, а також можливості та загрози. Фінансовий аналіз та порівняння з найкращими практиками інших компаній у секторі нададуть цінну інформацію для покращення продуктивності та ефективності.

Підсумовуючи, організаційна оцінка є ключовим інструментом для оцінки ефективності та результативності бізнесу. Вона допомагає виявити сильні та слабкі сторони організації, а також зрозуміти, які аспекти потребують уваги та покращень. Здійснення організаційної оцінки може включати різні методи, такі як опитування, інтерв'ю, фінансовий аналіз і SWOT-аналіз. Ці методи дозволяють зібрати різноманітні дані та отримати об'єктивну картину стану справ у компанії. Важливими етапами організаційної оцінки є визначення мети та завдань, збір і аналіз даних, розробка рекомендацій та плану дій, а також оцінка ефективності проведеної оцінки. Опитування виявляється одним з ефективних методів отримання відгуків та думок від співробітників організації. Такі інструменти, як QuestionPro, надають широкі можливості для проведення

онлайн-опитувань та оцінок, сприяючи у покращенні процесу організаційної оцінки [41].

В той час як, технічні рішення представляють собою комплекс інструментів, спрямованих на збір інформації щодо стану компонентів інформаційних систем і впливу на їх функціонування. Ці засоби допомагають виявляти та контролювати різноманітні аспекти безпеки інформації, включаючи виявлення шкідливого програмного забезпечення та реагування на інциденти безпеки. Один з головних аспектів технічних рішень є системи моніторингу, які слідкують за активністю в мережі та на комп'ютерах користувачів з метою виявлення потенційно шкідливих дій або програм. Ці системи забезпечують постійний контроль інформаційного середовища та можуть реагувати на виявлені загрози автоматично або за допомогою оповіщень. Крім того, важливим елементом є системи управління подіями і ризиками інформаційної безпеки. Ці системи спрямовані на виявлення, реєстрацію та аналіз ризиків, що відбуваються в інформаційній системі, і реагування на них. Вони допомагають вирішувати проблеми безпеки шляхом вчасного виявлення та оцінки ризиків, що можуть загрожувати безпеці даних та інфраструктурі організації. Технічні засоби захисту інформації включають як програмні, так і апаратні засоби, призначені для забезпечення безпеки даних та інформаційних систем. Основні з них включають:

1. Створення резервних копій найважливіших даних та їх збереження віддалено від основної мережі або комп'ютерної системи. Це забезпечує можливість відновлення даних у разі втрати або пошкодження основної копії.

2. Створення дубльованих копій важливих підсистем мережі, що відповідають за зберігання даних. Це дозволяє забезпечити доступність даних навіть у випадку відмови одного з обладнання.

3. Автоматичний перерозподіл ресурсів мережі в разі виникнення проблем з працездатністю окремих елементів.

4. Постачання електроенергії в разі відмови основного джерела живлення, що дозволяє уникнути втрати даних через непередбачувані перерви в електропостачанні.

5. Установка систем автоматичної пожежної сигналізації, вогнегасних систем та систем виявлення води для захисту обладнання та даних від пожежі та водяних пошкоджень.

6. Використання ПЗ для захисту баз даних та іншої конфіденційної інформації від несанкціонованого доступу.

До технічних заходів також входить забезпечення фізичної безпеки об'єктів, що може включати обладнання приміщень камерами спостереження, контроль доступу та системи сигналізації для виявлення потенційних загроз.

В організаціях, технічні рішення стають не просто важливою, а навіть невід'ємною частиною забезпечення безпеки інформації. Вони не лише виявляють потенційні загрози, а й дозволяють аналізувати та оперативно реагувати на них, забезпечуючи ефективний контроль і захист цінних інформаційних активів.

У критичних системах, де безпека інформації має основне значення, використання технічних засобів захисту інформації стає обов'язковим кроком для ефективного управління ризиками і гарантії безпеки даних. Власники критичних систем або уповноважені суб'єкти визначають комплекс таких засобів, забезпечуючи, щоб вони відповідали високим стандартам технічного захисту. Такий підхід є запорукою створення надійної системи захисту інформації, що відповідає сучасним вимогам безпеки [42].

На практиці, технічні засоби захисту інформації включають в себе широкий спектр апаратних рішень, таких як фільтри, міжмережеві екрани для апаратури, системи регулярного тестування безпеки, оновлення програмного забезпечення та інше. Однак, не завжди встановлення таких засобів призводить до автоматичного підвищення рівня безпеки в організації. Часто це стає результатом недостатньої інтеграції між ними. Важливо, щоб всі технічні

засоби працювали як єдина система, спільно діючи для захисту інформації в організації.

Загалом технічні засоби контролю інформаційної безпеки є важливим компонентам, який допомагає забезпечити ефективне управління та моніторинг доступу до інформаційних систем. Вони повинні бути чітко визначеними, зрозумілими і дотримуваними для забезпечення надійного контролю. У контексті управління ризиками, технічні засоби контролю, такі як системи контролю доступу, є одними з найбільш очевидних і важливих. Також моніторинг технічного контролю є важливим аспектом підзвітності керівництва і технічною проблемою, яка потребує постійної уваги. З управлінської точки зору, моніторинг технічного контролю часто асоціюється з аудиторськими процедурами, що включають регулярну перевірку і аналіз системних журналів і хронологічних записів, які є доказами належного контролю. Ще один прикладом технічного контролю є використання системних журналів для моніторингу поведінки системи. Системні журнали ведуть хронологічний запис подій, що відбуваються в системі, включаючи входи і виходи користувачів, спроби доступу до конфіденційних даних, зміни в конфігураціях системи та інші важливі події. Це дозволяє адміністраторам безпеки відстежувати будь-які підозрілі або несанкціоновані дії, аналізувати потенційні загрози і реагувати на інциденти в реальному часі. Таким чином, технічні засоби контролю не тільки забезпечують захист інформаційних систем, але й підвищують підзвітність і прозорість управління, що є критично важливим для ефективного управління інформаційною безпекою на підприємстві [43].

Загалом технічні та організаційні заходи представлені в табл. 2.3 в сфері інформаційної безпеки взаємодоповнюють один одного, утворюючи комплексну систему захисту. Організаційні заходи, такі як чітка структура управління, розробка політик та навчання персоналу, створюють основу для ефективного функціонування системи безпеки. Технічні заходи, у свою чергу, забезпечують безпосередній захист інформації за допомогою моніторингу, захисту та контролю. Завдяки взаємодії цих двох компонентів ефективна

система інформаційної безпеки забезпечує надійний захист інформаційних активів підприємства від різноманітних загроз.

Таблиця 2.3

Організаційні та технічні заходи захисту

Організаційні засоби захисту	Технічні засоби захисту
1. Розробка політик безпеки	1. Антивірусне програмне забезпечення
2. Проведення навчань та тренінгів з питань інформаційної безпеки	2. Системи виявлення та запобігання вторгненням (IDS/IPS)
3. Встановлення процедур управління доступом до інформації	3. Мережеві і міжмережеві екрани (Firewall)
4. Аудит і ревізія систем безпеки	4. Системи криптографічного захисту
5. Впровадження політики резервного копіювання та відновлення даних	5. Системи управління подіями та інцидентами (SIEM)
6. Моніторинг та аналіз подій	6. Системи спостереження за діями користувачів
7. Розробка та впровадження процедур реагування на інциденти	7. Системи захисту електронної пошти
8. Управління життєвим циклом інформаційної системи з точки зору безпеки	8. Системи контролю доступу (Access Control Systems)

Ця таблиця демонструє, як організаційні та технічні засоби можуть доповнювати один одного для забезпечення повного спектру захисту інформації та управління ризиками.

2.4 Методика проведення дослідження впливу процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки організації

Проведення досліджень управління ризиками є важливим інструментом, який дозволяє організаціям ідентифікувати, оцінювати та мінімізувати потенційні загрози. Цей процес не тільки підвищує рівень захисту інформації, але й сприяє оптимізації ресурсів та покращенню загальної ефективності управління.

Визначення ризиків та їх управління є ключовими аспектами у будь-якій сфері діяльності організації (див. рис. 2.12).

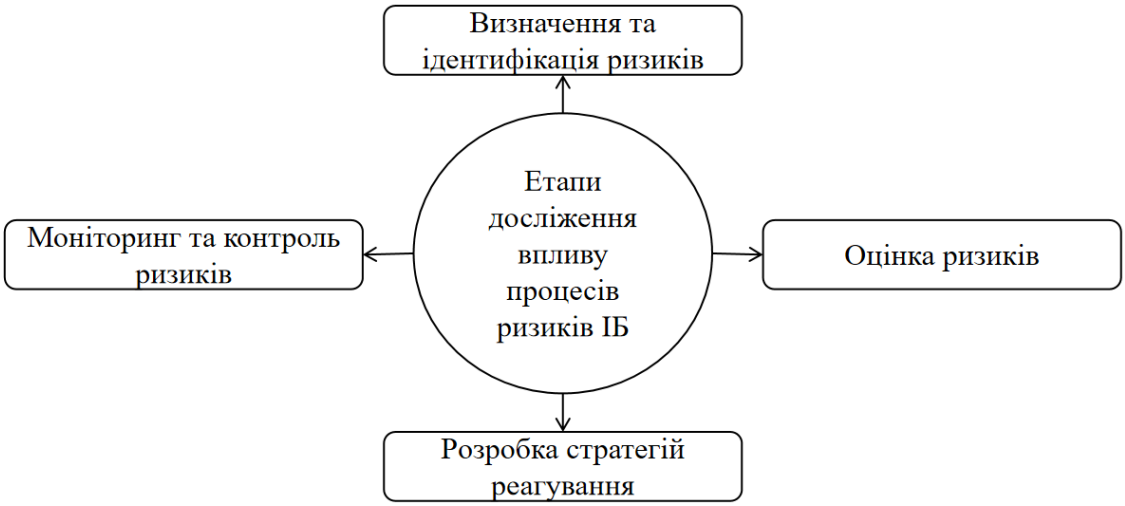

Рис. 2.12 – Етапи впливу процесів ризиків ІБ

Цей процес включає кілька етапів від ідентифікації потенційних загроз до розробки стратегій реагування та моніторингу їх ефективності:

1. Першим кроком являється виявлення всіх можливих загроз, які можуть вплинути на організацію. Це може включати зовнішні фактори, такі як економічні коливання, політичні зміни, природні катастрофи, а також внутрішні чинники, такі як недоліки в управлінні, втрати персоналу тощо.

2. Після ідентифікації потенційних ризиків проводиться оцінка їх ймовірність виникнення та вплив на організацію. Це допомагає визначати, які ризики є найбільш серйозними та потребують найбільшої уваги.

3. Після оцінки ризиків організація має розробити стратегії реагування на них. Це може включати різні підходи, такі як уникнення ризиків, зменшення їх впливу, передача ризиків іншим сторонам за допомогою страхування або контрактів, або прийняття ризику та його припинення.

4. Постійний моніторинг ризиків та ефективність застосованих стратегій управління ними. Організація повинна мати систему, яка дозволяє вчасно реагувати на зміни в зовнішньому середовищі та внутрішніх умовах.

Ці етапи управління ризиками допомагають організаціям адаптуватися до змін у зовнішньому середовищі та ефективно управляти потенційними загрозами, що дозволяє їм забезпечити стійкість та успішність у довгостроковій перспективі [44].

Обов’язкове створення належної системи управління ризиками в організації є важливим фактором для її успішного функціонування та стійкості в умовах непередбачуваності. Ця система повинна ґрунтуватися на чіткому розумінні ролей та відповідальностей на всіх рівнях управління. Кожен працівник повинен бути осведомленим про свої обов'язки щодо ідентифікації, оцінки та управління ризиками у своїй діяльності. Застосування логічних та систематичних методів важливо для ефективного управління ризиками. Це дозволяє не лише ідентифікувати потенційні загрози та оцінювати їх вплив на діяльність організації, але й розробляти ефективні стратегії для їх мінімізації або усунення. Наприклад, застосування методів аналізу ризиків дозволяє ідентифікувати найбільш імовірні та найбільш серйозні загрози, а далі розробляти конкретні заходи для їх зменшення. Моніторинг та перегляд управління ризиками є ще однією важливою складовою. Цей процес дозволяє своєчасно виявляти зміни у рівні ризиків, нові загрози або зміни в умовах діяльності, що може вплинути на організацію. За допомогою моніторингу організація може адаптувати свої стратегії управління ризиками та приймати своєчасні рішення для забезпечення стійкості та успішності в умовах невизначеності.

Отже, створення належної системи управління ризиками, яка базується на чіткому розумінні ролей, застосуванні логічних методів та постійному моніторингу, є ключовим елементом для успішного управління ризиками в будь-якій організації [45].

Також документування процесів управління ризиками в організації відіграє ключову роль у забезпеченні можливості аналізу ефективності вжитих заходів. Чітко визначені процедури і кроки дозволяють керівництву та працівникам організації розуміти, які кроки потрібно вжити в разі виникнення ризикових

ситуацій, які критерії оцінки ризиків та які стратегії реагування відповідають цим ситуаціям. Крім того, наявність документації дозволяє проводити аналізи, ідентифікувати та аналізувати шаблонні або повторювані ризики, що сприяє вдосконаленню процесів управління ризиками та зменшенню ймовірності їх виникнення в майбутньому. Використання накопиченого досвіду дозволяє уникнути повторення помилок, швидше виявляти нові загрози та ефективніше реагувати на них. Крім того, розвиток навичок управління ризиками серед персоналу сприяє створенню культури безпеки та свідомого ставлення до ризиків у всіх сферах діяльності організації. Впровадження інструментів для роботи з інформацією також має вирішальне значення для успішного управління ризиками. Автоматизовані системи управління ризиками дозволяють ефективно виявляти, оцінювати та відстежувати ризики на всіх рівнях організації. Вони також сприяють збору та аналізу даних, необхідних для прийняття обґрунтованих рішень з питань управління ризиками. Оцінка впливу процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки потребує комплексного підходу. Це означає аналіз середовища, в якому функціонує організація, оцінку специфіки виконуваних завдань, визначення цілей та аналізу впроваджених заходів. Тільки такий підхід дозволяє не лише оцінити поточний стан системи управління ризиками, але й виявити шляхи її оптимізації та покращення, що є критичним для забезпечення стійкості та безпеки організації [46].

Методика проведення дослідження управління ризиками в організації повинна бути систематичною та комплексною, щоб забезпечити об'єктивність та надійність результатів. Це включає розробку чітких критеріїв оцінки, які дозволяють визначити ефективність інтегрованих процесів управління ризиками. Такі критерії можуть включати рівень відповідності до стандартів, рівень захищеності інформаційних активів, ефективність виявлення та управління ризиками тощо. Крім того, важливо визначити методи збору та аналізу даних, які дозволять отримати об'єктивну інформацію про стан управління ризиками. Це може включати аудити, опитування персоналу, аналіз

інцидентів, а також використання спеціалізованих програмних засобів для оцінки ризиків. Формування рекомендацій щодо вдосконалення процесів управління ризиками є головним кроком в дослідженні. На основі отриманих даних та аналізу зачасту розробляються конкретні рекомендації щодо вдосконалення системи управління ризиками, враховуючи специфіку організації та її бізнес-потреб. Залучення всіх зацікавлених сторін до процесу управління ризиками є важливим аспектом, який сприяє підвищенню обізнаності та відповідальності за інформаційну безпеку на всіх рівнях організації. Це може включати навчання персоналу та регулярні оновлення знань з питань управління ризиками. Використання міжнародних стандартів, таких як ISO/IEC 27001, може слугувати основою для розробки ефективної системи управління ризиками ІБ. Цей стандарт надає зрозумілу та уніфіковану базу для впровадження процесів управління ризиками, забезпечуючи високий рівень захисту інформаційних активів та відповідність міжнародним стандартам безпеки. Для максимальної ефективності системи управління ризиками важливо:

1. Забезпечити підготовку та досвід керівництва в цій області.

2. Впровадити ефективні підходи та механізми для виконання процесів управління ризиками.

3. Розробити порядки та процедури для складання та подання звітів про результати діяльності у цій сфері.

Впровадження систематичного підходу до управління ризиками є невідмінною дією для сучасних організацій, оскільки воно дозволяє їм ефективно впоратися з потенційними загрозами та використовувати ризики як можливості для розвитку та інновацій.

Як протидія ризикам, управління ризиками відображається як стратегічний інструмент, який допомагає організаціям досягати своїх цілей та забезпечує стійкий розвиток у динамічному бізнес-середовищі. Одним з ключових аспектів цього підходу є перетворення ризиків на можливості. Замість того, щоб реагувати на загрози виключно у відвертому форматі захисту, організації

активно шукають способи використання ризиків як можливостей для покращення своєї діяльності. Підводячи приклад, можна визначити що виявивши ризик змін у вимогах споживачів, компанія може впровадити інноваційні рішення або виробляти нові продукти, що відповідають цим змінам, що в результаті дозволяє їй збільшити конкурентоспроможність та ринкову частку. Крім того, систематичний підхід до управління ризиками допомагає організаціям приймати обґрунтовані та стратегічні рішення. Шляхом аналізу ризиків на всіх рівнях діяльності компанії, керівництво може мати повну картину стану ризиків і відповідно планувати майбутні дії. Це дозволяє знизити ризик та підвищити ефективність стратегічного управління. Отже, впровадження систематичного підходу до управління ризиками не лише забезпечує захист від потенційних загроз, але і перетворює ризики на можливості для розвитку та створення конкурентних переваг. Такий стратегічний підхід сприяє стійкому розвитку організації та підвищує її конкурентоспроможність в глобальному бізнес-середовищі [47].

Висновок до розділу 2

У цьому розділі був проведений детальний аналіз зв’язаний з управлінням ризиків. Були детально проаналізовані методи управління ризиками ІБ організації, такі як NIST, CRAMM, OCTAVE, FRAP, FMEA, FAIR, були визначене їх виконання, переваги, недоліки. Загалом всі ці методики надають структурований підхід до аналізу та управління ризиками інформаційної безпеки. Вони допомагають ідентифікувати загрози, оцінювати вразливості та визначати ефективні контрміри для зниження ризиків. Також була детально досліджена структура системи управління ризиків ІБ, де були надані моделі СУІБ, та функціонального управління ризиками ІБ. Крім того були визначені організаційні та технічні засоби захисту ІБ, та обумовлена їхня головна мета для організацій. Додатково була відображена методика проведення впливу на

ІБ, де були визначені її головні етапи, та як досягти максимальної ефективності їх використання.

Розділ 3. ДОСЛІДЖЕННЯ ЩОДО ВПЛИВУ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ НА ЕФЕКТИВНІСТЬ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ (ДЛЯ ОБРАНОГО ПРИКЛАДУ)

У цьому розділі досліджується вплив ефективності управління ризиками на інформаційну безпеку в конкретній компанії. На основі аналізу формулюються рекомендації з покращення цих процесів для досягнення оптимального рівня захисту даних інформаційної системи організації.

3.1 Оцінка впливу процесів управління ризиками на ефективність системи управління ризиками інформаційної безпеки

Оцінка ризику є основним етапом управління ризиками. Вона включає визначення, аналіз та оцінку можливих загроз, а також вибір стратегій реагування. Після визначення ризиків важливо розробити плани дій та забезпечити постійний моніторинг їх реалізації. Цей процес допомагає організаціям зменшити негативний вплив ризиків та забезпечити досягнення поставлених цілей. На рис. 3.1 можна побачити детально описаний алгоритм оцінювання ризиків інформаційних ризиків [48].

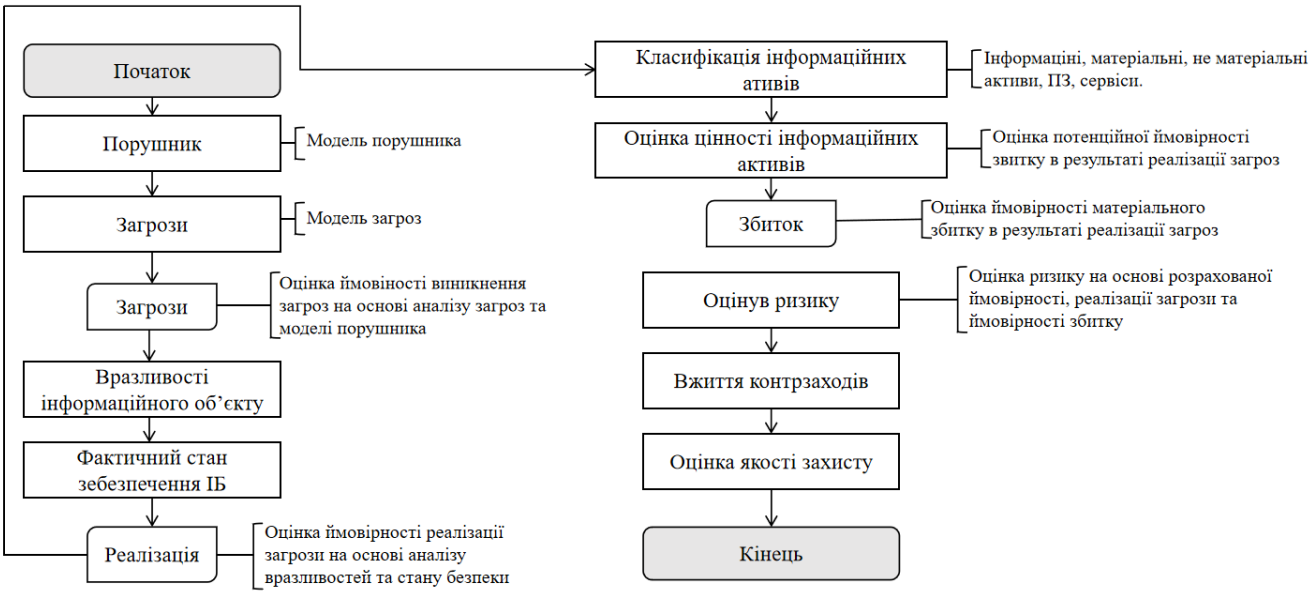

Рис. 3.1 – Схема алгоритму оцінювання інформаційних ризиків

Для більш детального опису оцінки впливу на ефективність системи, для прикладу буде проведений аналіз як на практиці впроваджується стандарт ISO 27001 в організацію У цілях конфіденційності, назва компанії не розголошується, і для цілей цього прикладу використовується назва "Visual".

Зараз безпека інформації є найважливішим аспектом для будь-якої компанії, впровадження стандарту ISO 27001 є стратегічно важливим кроком для забезпечення захищеності даних та підвищення довіри клієнтів. Компанія "Visual", яка спеціалізується на автоматизації та оптимізації бізнес-процесів, усвідомлює важливість безпеки інформації як ключового елементу своєї діяльності. Перед впровадженням стандарту ISO 27001 компанія мала ряд процесів безпеки, але більшість з них не були достатньо структурованими або не враховували всі потенційні загрози. У зв'язку зі стрімким ростом компанії та зростанням кількості загроз кібербезпеці, виникала необхідність у впровадженні стандартизованої моделі управління інформаційною безпекою. Впровадження стандарту ISO 27001 мало стати стратегічним кроком для компанії "Visual" у забезпеченні стабільної та ефективної системи управління безпекою інформації. Перший етап впровадження стандарту ISO 27001 передбачав підготовку, аналіз потреб компанії та формування проектної групи.

Після цього було розроблено політику та процедури безпеки, що відповідали вимогам стандарту. Важливою частиною процесу була реалізація та впровадження системи управління безпекою. інформації, включаючи впровадження технічних засобів та навчання персоналу [49]. Для забезпечення ефективності системи управління безпекою інформації, в компанії "Visual" проводилися регулярні аудити та аналіз ефективності. Отримані результати дозволили виявити слабкі місця та внести необхідні зміни для покращення системи управління безпекою. Впровадження стандарту ISO 27001 позитивно позначилося на безпеці інформації компанії, зменшивши ризики витоку даних та підвищивши рівень довіри клієнтів.Загалом, впровадження стандарту ISO 27001 у компанії "Visual" стало ключовим кроком для забезпечення безпеки інформації та підвищення конкурентоспроможності на ринку. Цей процес відображає стратегічний підхід компанії до управління ризиками та забезпечення стабільності своєї діяльності в умовах постійно зростаючих загроз кібербезпеці. Рис. 3.2 демонструє процес, використовуваний компанією для впровадження та оцінки СУІБ.

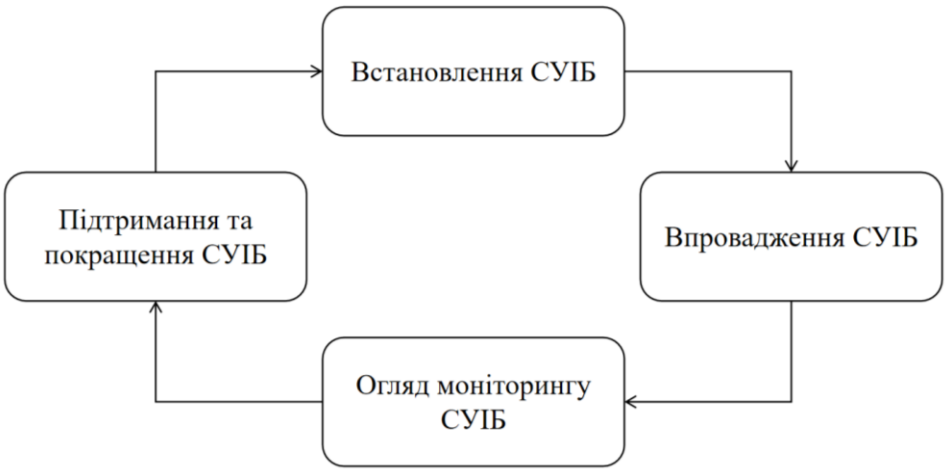

Рис. 3.2 – Процес для впровадження та оцінки СУІБ компанії

Впровадження стандарту ISO 27001 в компанії "Visual" було спрямоване на створення надійної ділової та технічної основи для оцінки та забезпечення безпеки інформаційної системи. Компанія ретельно розглянула всі аспекти свого бізнесу, включаючи ідентифікацію власників інформаційної системи,

класифікацію конфіденційності інформації, аналіз підтримуваних бізнес-процесів, вимог безпеки та відповідності. Під час оцінки ризиків, була проведена глибока аналітика важливості інформаційних активів компанії. Кожен актив був ретельно проаналізований на наявність вразливостей та можливі ризики для досягнення бізнес-цілей "Visual". Результати оцінки ризиків надали керівництву чітке уявлення про пріоритетність заходів щодо адміністрування ризиків та впровадження відповідних механізмів контролю. Зокрема, процедура оцінки ризиків включала систематичне оцінювання шкали ризику та визначення їх важливості в контексті бізнес-цілей компанії. Після цього були прийняті відповідні рішення щодо обробки ризиків, включаючи впровадження механізмів контролю, прийняття ризиків та їх передачу третім сторонам. Важливою частиною процесу було також забезпечення систематичного перегляду і оновлення процедур безпеки, оскільки змінюються умови та обставини. Такий підхід дозволяв компанії постійно удосконалювати свою систему управління безпекою інформації та ефективно протистояти ризикам кібербезпеки.

На рис. 3.3 зображено блок-схему дій, що здійснюються в процесі оцінки ризику.

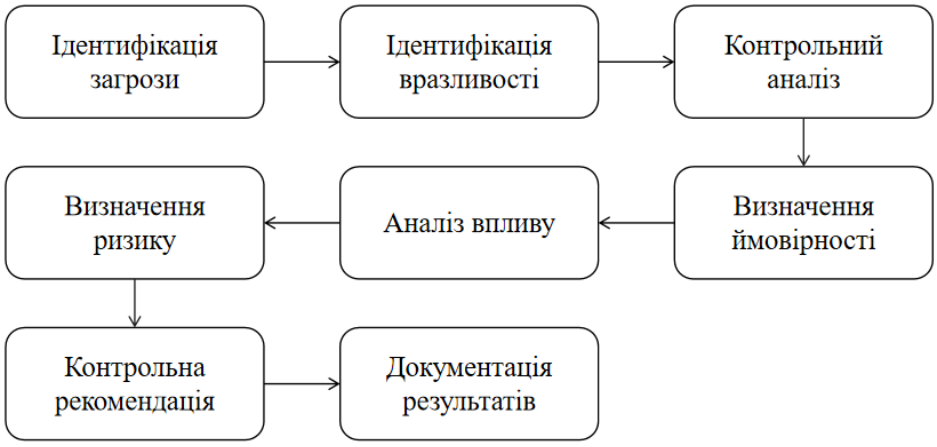

Рис. 3.3 – Блок-схема заходів в процесі оцінки ризиків

Процес оцінки ризиків для компанії "Visual" включав аналіз різних категорій небезпек, які можуть впливати на безпеку інформаційних активів. Наприклад, ці категорії включають загрози з боку зловмисників, технічні

помилки, природні катастрофи та інші потенційні загрози для інформаційної безпеки.

Для кожної категорії небезпеки визначалися критерії впливу, що дозволяли визначити ймовірність виникнення конкретного ризику та рівень частоти подій [50]. Наприклад, для категорії "злам системи" критеріями впливу можуть бути доступність зловмисників, рівень захисту системи та кількість виявлених потенційних загроз.

Далі, рівні впливу оцінювалися в контексті можливих наслідків для компанії "Visual". Це включало оцінку можливого збитку для бізнесу, втрату конфіденційної інформації, репутаційні ризики та інші аспекти. Наприклад, якщо виявлено порушення конфіденційності клієнтських даних, це може призвести до великих фінансових втрат і втрати довіри клієнтів.

Для кожного рівня впливу були визначені рівні наслідків, які дозволили оцінити серйозність можливих наслідків для компанії. Наприклад, можливі наслідки можуть бути розподілені на категорії "невеликий", "помірний", "серйозний" та "критичний", залежно від потенційного впливу на бізнес та інформаційну безпеку.

Усі ці аспекти оцінюються для кожної конкретної ситуації та ризику, що дозволяло компанії "Visual" ретельно аналізувати та управляти своїми ризиками в контексті їх важливості та потенційних наслідків.

Також план обробки ризиків для "Visual" включав заходи з мінімізації та контролю ризиків інформаційної безпеки. Це включало встановлення механізмів контролю, прийняття ризиків в межах умов та критеріїв, запобігання загрозам через політики безпеки та навчання персоналу, а також передачу ризиків страховим компаніям. Такий план допоміг зменшити ймовірність та наслідки можливих загроз для компанії [51].

Загалом впровадження стандарту ISO 27001 в компанії "Visual" виявилося ключовим кроком у забезпеченні безпеки інформації та зниженні ризиків. Цей процес дозволив компанії створити ділову та технічну основу для оцінки інформаційної системи, ідентифікувати ризики та прийняти відповідні заходи їх

обробки. Аналіз категорій небезпек, критеріїв впливу та ймовірності наслідків допоміг керівництву прийняти обґрунтовані рішення з управління ризиками. План обробки ризиків включав широкий спектр заходів, спрямованих на мінімізацію та контроль ризиків інформаційної безпеки. У результаті цього плану компанія змогла знизити ймовірність та наслідки можливих загроз, що позитивно позначилося на стабільності та ефективності її діяльності.

3.2 Рекомендації щодо вдосконалення процесів управління ризиками інформаційної безпеки організації

Ефективне управління ризиками інформаційної безпеки стає важливою потребою для кожної організації. Захист даних від несанкціонованого доступу, втрати чи пошкодження є пріоритетним завданням, оскільки це впливає на якість роботи, репутацію та навіть існування організації. Розробка та вдосконалення процесів управління ризиками стає основною стратегічною метою будь-якої організації, що передбачає впровадження цілісних систем управління, використання передових технологій і стандартів, а також постійне навчання персоналу та моніторинг ефективності впроваджених заходів. Враховуючи важливість ефективного управління ризиками інформаційної безпеки для стабільної діяльності будь-якої організації, пропонуються рекомендації, відображені у табл. 3.1.

Таблиця 3.1

Рекомендації щодо вдосконалення процесів управління ризиками ІБ

Рекомендація	Очікувані перемоги	Очікуваний вплив
Провести глибокий аналіз існуючих процесів управління ризиками	Виявлення слабких місць у існуючих процесах. Зниження ймовірності витоків даних.	Зниження часу виявлення та реагування на загрози. Оптимізація процесів управління ризиками.

Продовження таблиці 3.1

Рекомендація	Очікувані перемоги	Очікуваний вплив
Розробити план дій для усунення виявлених слабких місць.	Покращення ефективності управління ризиками. Збільшення рівня захисту інформації.	Підвищення стійкості до потенційних загроз. Збільшення швидкості виявлення та реагування на ризики.
Розробити та впровадити інтегровану систему управління ризиками.	Створення структурованої та цілісної системи управління ризиками. Забезпечення комплексного підходу до ідентифікації, оцінки, контролю та моніторингу ризиків. Мінімізація вразливостей і підвищення стійкості до атак.	Зниження ймовірності витоків та несанкціонованого доступу. Оптимізація процесів управління ризиками. Збільшення продуктивності та швидкості реагування на потенційні загрози.
Оновлювати інформаційну базу про загрози та методи їх виявлення регулярно.	Мінімізація можливих втрат та ризиків через своєчасне реагування. Підвищення готовності до виявлення потенційних загроз та їхнього усунення.	Покращення захищеності інформації. Зменшення впливу потенційних загроз.
Розробка програм навчання та підвищення обізнаності персоналу щодо ІБ.	Збільшення рівня обізнаності з питань інформаційної безпеки. Покращення вмінь персоналу виявляти, оцінювати та управляти ризиками інформаційної безпеки.	Зменшення ризику людських помилок та необережності. Підвищення конкурентоспроможності.

Продовження таблиці 3.1

Рекомендація	Очікувані перемоги	Очікуваний вплив
Впровадити стандарти та практики у сфері ІБ	Спрощення розуміння та виконання вимог щодо безпеки даних. Запобігання можливим загрозам та вразливостям за допомогою застосування стандартів безпеки.	Забезпечення швидкості реагування на виявлення ризиків. Вдосконалення захисту інформації.
Використовувати автоматизовані інструменти для моніторингу та аналізу безпеки	Забезпечення постійного та систематичного моніторингу стану інформаційної безпеки. Швидке виявлення потенційних загроз та вразливостей.	Зниження часу, потрібного для виявлення загроз. Покращення точності та об'єктивності моніторингу.

Вдосконалення процесів управління ризиками інформаційної безпеки нині є дуже важливим. Загальна мета цих рекомендацій полягає в створенні і підтримці ефективної системи управління ризиками інформаційної безпеки, що відповідає потребам сучасного бізнесу. Впровадження запропонованих заходів сприятиме забезпеченню безпеки даних та збереженню довіри стейкхолдерів до організації.

Висновок до розділу 3

У цьому розділі було проведено глибоке дослідження процесів управління ризиками та їх впливу на ефективність системи управління ризиками ІБ. Встановлено, що належне управління ризиками є дуже важливим для забезпечення ІБ. Систематичний підхід до ідентифікації, аналізу, оцінки та моніторингу ризиків показав, що може значно підвищити рівень захисту інформаційних активів організації. На основі проведеного аналізу були розроблені рекомендації щодо вдосконалення процесів управління ризиками.

Загалом, результати дослідження підтверджують, що ефективне управління ризиками є ключовим елементом у забезпеченні інформаційної безпеки організації та може бути основою для створення міцної та надійної системи управління ризиками. Впровадження запропонованих рекомендацій дозволить організації не тільки підвищити ефективність існуючої системи, але й забезпечити кращу підготовку до можливих майбутніх загроз.

ВИСНОВКИ

У кваліфікаційній роботі проведено обширне дослідження процесів управління ризиками інформаційної безпеки в організації. Результати цього аналізу виявили, що ефективне управління ризиками є основною складовою успішної діяльності будь-якої організації в сучасному інформаційному середовищі.

Мета цього дослідження полягає в аналізі процесів управління ризиками інформаційної безпеки організації, що є основною складовою успішного забезпечення інформаційної безпеки. Як результат, була виявлена необхідность захисту від різноманітних загроз та забезпечення стабільності функціонування організації, що є головною метою системи інформаційної безпеки. Крім того, було визначено, що стандарти, такі як ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, відображають головні аспекти управління ризиками інформаційної безпеки та відповідають цілям дослідження.

Також були сформульовані основні вимоги щодо управління ризиками в системі забезпечення інформаційної безпеки. Виявлено, що активна участь всіх підрозділів організації є важливою для забезпечення високого рівня безпеки даних та відповідальності перед клієнтами і партнерами. Дослідження також вказало на різноманітні методи та підходи до управління ризиками, що створюють можливість ідентифікувати загрози та розробляти ефективні контрміри, такі як NIST, CRAMM, OCTAVE, FRAP, FMEA, FAIR.

На прикладі впровадження стандарту ISO 27001 у компанію "Visual" було підкреслено важливість систематичної оцінки ризиків та розробки стратегій для забезпечення інформаційної безпеки. Цей процес не лише допомагає ідентифікувати потенційні загрози, але й сприяє підвищенню стабільності та ефективності діяльності організації.

Розроблені рекомендації щодо вдосконалення її процесів включають:

- проведення глибокого аналізу існуючих процесів управління ризиками;

- розробку плану дій для усунення виявлених слабких місць;
- впровадження інтегрованої системи управління ризиками;
- оновлення інформаційної бази про загрози та методи їх виявлення регулярно;
- розробку програм навчання та підвищення обізнаності персоналу щодо інформаційної безпеки;
- впровадження стандартів та практик у сфері інформаційної безпеки;
- використання автоматизованих інструментів для моніторингу та аналізу безпеки.

Проведення досліджень та обробка їх результатів для компанії "Visual" показало можливості по вдосконаленню процесу управління в системі управління безпекою організації.

Загалом дослідження підтвердило важливість ефективного управління ризиками інформаційної безпеки для успішної діяльності будь-якої сучасної організації. Рекомендації, розроблені на основі результатів аналізу, надають практичні кроки для підвищення рівня безпеки та стабільності функціонування організації в умовах постійно зростаючих загроз інформаційній безпеці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. Darby. Information Security Risk Management Explained – ISO 27001 URL: https://www.isms.online/iso-27001/information-security-risk-management-explained/

2. Ю.Р. Гарасим, В.А. Ромака, М.М. Рибій. АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ ЗАБЕЗПЕЧЕННЯ ВЛАСТИВОСТІ ЖИВУЧОСТІ СИСТЕМ. 2013. URL: file:///D:/%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B8/VNULP_2013_753_17%20(1).pdf

3. Z. Jourdan, R. Rainer, T. E. Marshall, A. University. An Investigation Of Organizational Information Security Risk Analysis. URL: https://www.researchgate.net/publication/287663997_An_Investigation_Of_Organizational_Information_Security_Risk_Analysis

4. WHAT IS INFORMATION RISK MANAGEMENT IN CYBERSECURITY? URL: https://blog.rsisecurity.com/what-is-information-risk-management-in-cybersecurity/

5. Information Security Risk Management – Definition, Steps & Roles URL: https://phoenixnap.com/blog/security-risk-management

6. Ю.М. Якименко, В.А. Савченко, С.В. Легомінова. Системний аналіз інформаційної безпеки: сучасні методи управління. Київ: Державний університет телекомунікацій, 2022. 135-136 с.

7. О.І. Волот. Інформаційна та кібернетична безпека мучасного підприємства: заббезпечення та моделювання. 239-242 с. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/8ec3397a-956a-4255-a474-dd6b501ce437/content

8. Концепція інформаційної безпеки України URL: https://www.osce.org/files/f/documents/0/2/175056.pdf

9. ISO/IEC 27001 - Інформаційні технології. Методи безпеки. Системи менеджменту інформаційною безпекою. Вимоги. URL: https://iso-

certify.com/ua/publikatsii/iso-iec-27001-informatsiyni-tekhnolohiyi-metodymbezpeky-systemy-menedzhmentu-informatsiynoyu-bezpekoyu-vymohy/

10. Meeba Gracy. List of ISO 27002 Controls (Complete Overview). URL:https://sprinto.com/blog/iso-27002-controls/

11. ISO 27005:2022 ISMS Risk Management - it's important. URL:https://info.degrandson.com/blog/iso-27005-2022-info

12. Brad Kelechava. ISO/IEC 27005:2022 – Information Security Risk Management. URL: https://blog.ansi.org/iso-iec-27005-2022-security-risk-management/

13. Інформаційна безпека: види, загрози і захист. URL: https://moyaosvita.com.ua/ekonomika/informacijna-bezpeka-vidi-zagrozi-i-zaxist/

14. В.М. Гранатуров, І.В. Литовченко. Методи якісного аналізу підприємницьких ризиків. Одеса: Одеська національна академія зв'язку ім. О. С. Попова, 2005. 5 с.

15. Information security risk management: Understanding the components. URL: https://www.techtarget.com/searchsecurity/tip/Information-security-risk-management-Understanding-the-components

16. І.М. Карпович, О.М. Гладка, В.І. Калашніков. МОДЕЛЮВАННЯ ПРОЦЕСІВ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СПОСІБ ОПТИМІЗАЦІЇ ВИТРАТ. 93-94 с. URL: http://tech.vernadskyjournals.in.ua/journals/2022/5_2022/13.pdf

17. Information Security: Principles, Threats, and Solutions. URL:https://www.hackerone.com/knowledge-center/principles-threats-and-solutions

18. INTERNAL VS EXTERNAL THREATS- HERE’S ALL YOU NEED TO KNOW. URL: https://securetriad.io/internal-vs-external-threats/

19. What is NIST SP 800 30? URL: https://cyvatar.ai/nist-csf-sp-800-30/

20. M. Ghazouani, S. Faris, H. Medromi, A. Sayouti. Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. 2014, 38 c.

21. Top 10 types of information security threats for IT teams. URL:https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams

22. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation). URL:https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation)

23. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/

24. О.В. ПОТІЙ, Ю.І. ГОРБЕНКО, О.А. ЗАМУЛА, К.В. ІСІРОВА. МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ. 10-15 с. URL: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdf

25. Сидоркін П.Г., Горліченко С.О.,Некоз В.С., Шилан М.В. МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ CRAMM ТА COBIT 5 FOR RISK. URL: https://sit.nuou.org.ua/article/view/286348/281460

26. FRAP – Facilitated Risk Analysis Process. URL: https://pdfslide.tips/documents/frap-facilitated-risk-analysis-process.html?page=20

27. Є.С. РОДІН. ПРОЦЕСНІ ПІДХОДИ ДО МОДЕЛЮВАННЯ У СФЕРІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/83786/16-Rodin.pdf?sequence=1

28. Guide to Failure Mode and Effects Analysis (FMEA). URL: https://reliability.com/resources/articles/guide-to-failure-mode-and-effects-analysis/

29. FAILURE MODE AND EFFECT ANALYSIS (FMEA). URL: http://surl.li/tveeu

30. What Is Factor Analysis Of Information Risk (FAIR)? URL: https://www.wallarm.com/what/what-is-factor-analysis-of-information-risk-fair

31. The FAIR™ Methodology for Cyber Risks. URL: https://www.c-risk.com/blog/fair-analysis

32. Л.О. Бескровна. Бізнес-планування підприємства. Одеса: ОНАЗ, 2012. 96 с.

33. О. М. Герасименко. ФОРМУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ РИЗИК-МЕНЕДЖМЕНТУ З ВРАХУВАННЯМ ЧУТЛИВОСТІ КОМПАНІЇ ДО РИНКОВИХ РИЗИКІВ. URL: file:///D:/%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B8/efek_2013_5_21%20(1).pdf

34. В.І. Котецька. Аналіз процесів управління ризиками інформаційної безпеки організації. Матеріали НПК. ДУІКТ, 2023. 161-163 с.

35. М.А. Дядюк. Управління ризиками. Харків: Харківський державний університет харчування та торгівлі, 2017. 23 с

36. В. Коняхин. Система управління інформаційною безпекою підприємства. URL: https://stud.com.ua/43080/ekonomika/sistema_upravlinnya_informatsiynoyu_bezpekoyu_pidpriyemstva

37. Romuald Hoffmann, Maciej Kiedrowicz, Jerzy Stanik. Risk management system as the basic paradigm of the information security management system in an organization. URL: https://www.researchgate.net/publication/309367195_Risk_management_system_as_the_basic_paradigm_of_the_information_security_management_system_in_an_organization#pf3

38. І.М. Карпович, О.М. Гладка, Ю.А. Наконечна. АНАЛІЗ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІТ-ПІДПРИЄМСТВА. URL: https://www.tech.vernadskyjournals.in.ua/journals/2020/5_2020/14.pdf

39. О.П. Ващенкою. ІНФОРМАЦІЙНИЙ МЕНЕДЖМЕНТ. Київ: ДУІКТ, 2024. 102 с.

40. Політика інформаційної безпеки. URL: https://kitsoft.ua/ua/politika-informacijnoyi-bezpeki

41. СИСТЕМНИЙ АНАЛІЗ ТЕХНІЧНИХ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ВІД КОМПАНІЇ FIREEYE. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/251

42. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Київ. 2000. 3 с.

43. Organizational Assessment: What It Is, Benefits + How to Conduct. URL: https://www.questionpro.com/blog/organizational-assessment/

44. Л.А. Сарана, О.В. Білан, І.М. Бітюк. УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВА В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ URL: http://www.psae-jrnl.nau.in.ua/journal/2_82_2021_ukr/17.pdf

45. WHAT IS RISK MANAGEMENT & WHY IS IT IMPORTANT? URL: https://online.hbs.edu/blog/post/risk-management

46. Risk Management Automation: What it is and how it can improve your cybersecurity? URL: https://reciprocity.com/blog/what-is-risk-management-automation/

47. N. Zakharova. Risk Management in the Enterprise: The Essence, Approaches, and Methods. URL: https://www.researchgate.net/publication/369219239_Risk_Management_in_the_Enterprise_The_Essence_Approaches_and_Methods

48. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮНА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO. URL: https://ela.kpi.ua/server/api/core/bitstreams/ec7ce023-c4f9-4730-9fb1-4aee988d223c/content

49. РОЗРОБКА ОСНОВИ СТРАТЕГІЇ АНАЛІЗУ РИЗИКІВ ДЛЯ ОЦІНКИ ВПЛИВУ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРИКЛАД З ІНДУСТРІЇ IT-КОНСАЛТИНГУ. ЧАСТИНА 1. URL: https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informaczijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltyngu-chastyna-1/

50. В.І. Котецька. Вплив ризиків на ефективність інформаційної безпеки в організаціях, підходи до аналізу. Матеріали НПК. ДУІКТ, 2024. 65-67 с.

51. РОЗРОБКА ОСНОВИ СТРАТЕГІЇ АНАЛІЗУ РИЗИКІВ ДЛЯ ОЦІНКИ ВПЛИВУ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРИКЛАД З ІНДУСТРІЇ IT-КОНСАЛТИНГУ. ЧАСТИНА 2. URL: https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informaczijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltyngu-chastyna-2/