Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Метод аналізу ризиків в системах управління інформаційною безпекою

Виконавець: студент IV курсу, групи КБ-41

_____ **Артем Макушенко**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Олександр ЛАПТЄВ	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студента **КБ-41** **Макушенка Артема Ігоровича**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Метод аналізу ризиків в системах управління інформаційною безпекою

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Аналіз ризиків, методи аналізу ризиків

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомлення з основними концепціями аналізу ризиків включає розуміння ризиків, загроз і вразливостей в інформаційних системах, ознайомлення з різними методами аналізу ризиків, вивчення прикладів існуючих методів, огляд огляд стандартів і відповідної літератури

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Підвищення ефективності проведення потенційних загроз та вразливостей в системах управління інформаційною безпекою.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Артем МАКУШЕНКО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 26.10.2022	*виконано*
2	Аналіз літератури	27.10.2022 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Збір даних	16.02.2023 – 05.03.2023	*виконано*
5	Аналіз ризиків в системах управління інформаційною безпекою	06.03.2023 – 27.03.2023	*виконано*
6	Аналіз методів виявлення та ідентифікації ризиків в системах управління інформаційною безпекою	28.03.2023 – 15.04.2023	*виконано*
7	Метод аналізу ризиків в системах управління інформаційною безпекою	16.04.2020 – 8.05.2023	*виконано*
8	Оформлення пояснювальної записки	9.05.2023 – 24.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	25.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Артем МАКУШЕНКО
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 73 сторінки основного тексту, 7 таблиць та 2 рисунки. Список використаних джерел містить 20 найменування і займає 2 сторінки.

Метою роботи підвищення ефективності проведення аналізів ризиків в системах управління інформаційною безпекою.

Об'єктом дослідження є процеси аналізу ризиків в системах управління інформаційною безпекою.

Предметом дослідження методи аналізу ризиків в системах управління інформаційною безпекою.

Методи дослідження:

- теоретичний аналіз;
- структурний аналіз;
- синтез, моделювання;

Практичною цінністю є підвищення ефективності проведення потенційних загроз та вразливостей в системах управління інформаційною безпекою.

Ключові слова: аналіз ризиків, системи управління інформаційною безпекою, методи аналізу ризиків, інформаційна безпека, загрози, вразливості, оцінка ризиків, управління ризиками, методології оцінки ризиків, ідентифікація ризиків, запобігання інцидентам безпеки, моделі ризику.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

ЗЗІ – засоби захисту інформації;

ЗІ – захист інформації;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

КСЗІ – комплексна система захисту інформації;

КЦД – конфіденційність, цілісність, доступність;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмні засоби, програмне забезпечення;

СЗІ – система захисту інформації;

ІБ – інформаційна безпека;

СУІБ – система управління інформаційною безпекою;

APT – сучасні постійні загрози;

GDPR – загальний регламент Європейського Союзу про захист даних;

CCPA – закон про конфіденційність споживачів;

RMF – NIST Risk Management Framework;

OCTAVE – оперативна оцінка критичних загроз, активів та вразливостей;

FAIR – факторний аналіз інформаційних ризиків;

CRAMM – метод аналізу та управління ризиками ССТА;

ІТ – інформаційних технологій;

HACCP – аналіз ризиків і критичн контрольні точки

ККТ – критичні контрольні точки.

ВСТУП

У сучасну цифрову епоху інформаційна безпека стала ключовим питанням для організацій по всьому світу. Зі зростанням залежності від інформаційних технологій та все більш витончених кіберзагроз, захист конфіденційних даних та інформаційних активів став головним пріоритетом. СУІБ надає організаціям основу для створення, впровадження, функціонування, моніторингу, перегляду, підтримки та постійного вдосконалення заходів інформаційної безпеки.

Аналіз ризиків відіграє важливу роль в ефективному управлінні інформаційною безпекою. Аналіз ризиків - це виявлення, оцінка та зменшення ризиків, які можуть вплинути на конфіденційність, цілісність та доступність інформаційних активів. Систематично аналізуючи та оцінюючи ризики, організації можуть приймати обґрунтовані рішення, ефективно розподіляти ресурси та впроваджувати відповідні засоби контролю для мінімізації впливу потенційних загроз.

У дослідженні спочатку надається огляд поточних загроз та вразливостей інформаційної безпеки шляхом вивчення різних методологій аналізу ризиків, що використовуються в галузі.

Тож ***актуальність роботи*** полягає в тому, що в сучасну цифрову епоху інформаційна безпека стала критично важливою для організацій по всьому світу. Зростаюча залежність від інформаційних технологій призводить до збільшення кіберзагроз, які суттєво ставлять під загрозу конфіденційність, цілісність та доступність інформаційних активів.

Метою роботи є підвищення ефективності проведення аналізів ризиків в системах управління інформаційною безпекою.

Для досягнення зазначеної мети дипломної роботи поставлено наступні **завдання**:

- Провести аналіз ризиків інформаційної безпеки
- Дослідити методи аналізу ризиків інформаційної безпеки
- Запропонувати метод аналізу ризиків в системах управління інформаційною безпекою

Об'єктом дослідження є процеси аналізу ризиків в системах управління інформаційною безпекою.

Предметом дослідження методи аналізу ризиків в системах управління інформаційною безпекою.

Методи дослідження:

- теоретичний аналіз;
- структурний аналіз;
- синтез, моделювання;

Практична цінність роботи полягає в наступному:

- підвищення ефективності проведення потенційних загроз та вразливостей в системах управління інформаційною безпекою**.**

РОЗДІЛ 1
АНАЛІЗ РИЗИКІВ БЕЗПЕКИ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В СУІБ аналіз ризиків - це важливий процес, коли виявляється та оцінюється потенційні загрози для інформаційних активів. Головна мета ефективного аналізу ризиків, зрозуміти, що може погрожувати конфіденційності, цілісності та доступності інформації. Тому люди намагаються запровадити відповідні заходи контролю, для зменшення ризиків.

1.1 Принципи аналізу ризиків

Визначення принципів аналізу ризиків є важливою частиною системи управління інформаційною безпекою і включає методи, спрямовані на оцінку та управління ризиками. Відповідно до ISO/IEC 27000:2018, ризик - це втрата або пошкодження активів або порушення цілісності, конфіденційності або доступності інформації. Він визначається як потенційна загроза.

До аналізу ризиків застосовуються такі принципи:

1. Оцінка ризиків повинна бути систематичною, повторюваною та прозорою.

2. Визначати конкретні критерії для оцінки ймовірності та впливу на активи інформаційної системи.

3. Аналіз ризиків повинен включати оцінку технічних, організаційних та людських аспектів безпеки інформаційної системи.

4. Ризики повинні оцінюватися з урахуванням поточних загроз і вразливостей інформаційних систем та можливих майбутніх подій.

5. Аналіз ризиків повинен включати оцінку ймовірності реалізації ризику та потенціалу управління ризиками [1].

Відповідно до спеціальної публікації NIST 800-53, аналіз ризиків включає наступні етапи:

1. Виявлення вразливостей та загроз, пов'язаних з інформаційною системою.

2. Оцінка ймовірності та впливу потенційних ризиків.

3. Визначення рівня ризику та пріоритетів управління.

4. Розробка плану дій з управління ризиками та моніторинг його виконання.

Ці принципи підтверджені в чинних українських стандартах інформаційної безпеки, таких як ДСТУ ISO/IEC 27000:2015, ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO/IEC 27005:2015. Таким чином, ефективне управління ризиками в інформаційних системах вимагає дотримання принципів аналізу ризиків та орієнтації на відповідні стандарти [2].

1.2 Основні терміни

1. Ризик - це вплив невизначеності на цілі організації; в контексті СУІБ ризик означає потенційну можливість шкоди або збитків, які можуть виникнути в результаті порушення безпеки або іншої події, що впливає на конфіденційність, цілісність або доступність інформації організації.

2. Загроза - це потенційне джерело шкоди інформації або інформаційним системам організації. Загрози можуть бути спричинені природними явищами (наприклад, повені або землетруси), діями людей (наприклад, крадіжки або саботаж) або технічними збоями (наприклад, збої в роботі апаратного або програмного забезпечення).

3. Вразливості - це слабкі місця або прогалини в системі захисту інформаційної безпеки організації. Вразливості можуть бути наслідком поганого

захисту системи, неправильної конфігурації, застарілого програмного забезпечення або неадекватних процедур безпеки. Вразливості створюють можливості для загроз використати їх і завдати шкоди організації. Наприклад, вразливості у веб-додатках дозволяють хакерам отримати несанкціонований доступ до конфіденційної інформації.

4. Активи - це все, що має цінність для організації. Вони включають в себе ряд предметів і ресурсів, таких як інформація, обладнання, програмне забезпечення та персонал. Наприклад, інформація, що міститься в базі даних клієнтів, є активом, оскільки вона цінна для організації і може бути використана для прийняття рішень та розвитку бізнесу. Те ж саме стосується обладнання, яке підтримує діяльність організації, наприклад, комп'ютерів і серверів, а також програмного забезпечення, яке використовується для виконання необхідних завдань. Люди також є активами, оскільки їхні знання, досвід та навички сприяють підвищенню ефективності роботи організації. Всі ці активи є цінними і потребують належного захисту для забезпечення безпеки та стабільності організації.

5. Засоби контролю - це заходи та процедури, створені для зменшення ризику порушень безпеки та інцидентів в організації. Їх основна мета - запобігти або зменшити загрози та вразливості, які можуть поставити під загрозу конфіденційність, цілісність та доступність інформації.

6. Аналіз ризиків - це процес ідентифікації та оцінки потенційних ризиків, які можуть вплинути на інформаційні активи організації. Основна мета аналізу ризиків - виявити загрози, визначити вразливості та оцінити потенційний вплив цих ризиків на організацію.

7. Оцінка ризиків - це процес аналізу та оцінки ймовірності та впливу ідентифікованих ризиків на організацію.

Оцінка ризиків є важливим елементом процесу аналізу ризиків в системі управління інформаційною безпекою. Вона передбачає виявлення та оцінку

потенційних ризиків для інформаційних активів організації, а також визначення ймовірності та впливу цих ризиків.

8. Управління ризиками - це процес виявлення, оцінки, визначення пріоритетності та зменшення ризиків для інформаційних активів організації.

Управління ризиками - це комплексний процес, що включає в себе виявлення, оцінку, визначення пріоритетів і зниження ризиків для інформаційних активів організації. Метою управління ризиками є зменшення загального впливу та ймовірності потенційних ризиків шляхом застосування відповідних засобів контролю та контрзаходів.

9. Обробка ризиків - це процес оцінки різних доступних варіантів і вибору найбільш прийнятного способу дій.

Обробка ризиків є важливим кроком у процесі управління ризиками і передбачає вибір і впровадження засобів контролю для зменшення виявлених ризиків. Після того, як ризики ідентифіковані та оцінені, організація повинна вирішити, як на них реагувати [3].

1.3 Принципи оцінки ризиків у системах управління інформаційною безпекою

Принципи оцінки ризиків в системах управління інформаційною безпекою визначають підходи та принципи, якими слід керуватися при оцінці ризиків.

Дотримуючись цих принципів, організації можуть виявити та оцінити потенційні ризики для своїх інформаційних активів і захистити себе від впливу цих ризиків [4].

1.3.1 Постійність

Оцінка ризиків - це не разовий захід, а постійний процес, який слід проводити регулярно, щоб забезпечити захист інформаційних активів організації від ризиків, що виникають.

Регулярно проводячи оцінку ризиків, організація може переконатися, що вона має необхідні засоби контролю для захисту своїх інформаційних активів від потенційних загроз та ефективного зниження ризиків. Це також дозволяє відстежувати ефективність стратегій управління ризиками та вносити необхідні корективи.

1.3.2 Пристосування до конкретних організацій

Загалом, проведення оцінки ризиків відповідно до бізнес-цілей, стратегії, операцій та інфраструктури управління ризиками організації допомагає гарантувати, що організація може ефективно та результативно виявляти ризики та управляти ними. Проведення регулярних оцінок ризиків також може допомогти організаціям уникнути нових ризиків і забезпечити захист інформаційних активів.

1.3.3 Ретельний аналіз загроз

Процес управління ризиками слід регулярно переглядати, щоб переконатися, що він є актуальним та ефективним. Це може включати оновлення аналізу загроз і вразливостей, переоцінку ризиків і перегляд засобів контролю, щоб переконатися, що вони ефективно знижують ризики. Регулярний перегляд процесів оцінки та контролю ризиків допоможе забезпечити захист інформаційних активів організації від потенційних загроз.

1.3.4 Ретельний аналіз вразливості

Необхідно провести комплексний аналіз вразливості, який виявить слабкі місця та вразливості в інформаційних активах, системах та процесах організації. Аналіз вразливостей повинен враховувати як технічні, так і нетехнічні вразливості, включаючи людські фактори, такі як помилки працівників, атаки соціальної інженерії та внутрішні загрози. Аналіз вразливостей також повинен враховувати потенційний вплив вразливостей на інформаційні активи організації.

1.3.5 Використання методології аналізу ризику

Оцінка ризиків повинна ґрунтуватися на комплексній методології аналізу ризиків, яка узгоджується з системою управління ризиками організації. Методологія аналізу ризиків повинна ґрунтуватися на визнаних галузевих стандартах і найкращих практиках, таких як ISO/IEC 27005:2018 "Інформаційні технології - Практики безпеки - Управління ризиками інформаційної безпеки". Методологія аналізу ризиків повинна бути адаптована до конкретних потреб організації. Методологія аналізу ризиків повинна бути адаптована до конкретних потреб організації та враховувати апетит до ризику і толерантність організації.

Використовуючи комплексну методологію аналізу ризиків, організація може забезпечити виявлення та оцінку потенційних ризиків для інформаційних активів, а також запровадити відповідні засоби контролю для зменшення цих ризиків. Це допоможе захистити організацію від порушень безпеки та інших інцидентів, які можуть завдати шкоди інформаційним активам.

1.3.6 Залучення всіх підрозділів

Залучення всіх зацікавлених підрозділів може призвести до більшої відповідальності та підтримки процесу оцінки ризиків і стратегії управління ризиками. Зацікавлені сторони з більшою ймовірністю підтримають реалізацію стратегії управління ризиками і візьмуть на себе відповідальність за свою роль в управлінні ризиками, якщо відчують, що їхні погляди і занепокоєння враховані.

1.3.7 Документація

Документація повинна бути чіткою, стислою і зрозумілою, а також містити стислий виклад основних висновків і рекомендацій. Документація повинна також включати припущення та обмеження процесу оцінки ризиків, такі як доступність даних, ресурсні обмеження та невизначеності в аналізі ризиків. Це забезпечить належну інтерпретацію результатів оцінки ризиків і прийняття відповідних рішень з управління ризиками на основі наявної інформації.

1.4 Ризики інформаційної безпеки

Оскільки ризики відрізняються за ймовірністю виникнення та потенційним впливом на інформаційну безпеку організації, важливо проводити комплексний аналіз ризиків для виявлення та визначення пріоритетності потенційних ризиків [5].

1.4.1 Людська помилка або навмисні дії

Людські помилки або навмисні дії можуть призвести до порушень безпеки. Випадкові дії, такі як неправильна конфігурація систем або необережне

поводження з конфіденційною інформацією, можуть призвести до інцидентів безпеки. Навмисні дії, такі як крадіжка, хакерські атаки або соціальна інженерія, можуть призвести до несанкціонованого доступу до інформації.

Людські помилки є поширеними причинами порушень безпеки в організаціях. Випадкові помилки можуть бути спричинені працівниками, підрядниками або сторонніми постачальниками послуг. Такі помилки включають неправильну конфігурацію систем, неправильне встановлення програмного забезпечення, випадкове видалення даних і необережне поводження з конфіденційною інформацією. Такі помилки можуть призвести до витоку даних і завдати значної фінансової та репутаційної шкоди організації.

1.4.2 Шкідливе програмне забезпечення

Шкідливе програмне забезпечення, таке як віруси, хробаки та троянські програми, може потрапляти в інформаційні системи через електронну пошту, веб-перегляди та знімні носії. Шкідливе програмне забезпечення може пошкодити дані, системи та програми і навіть призвести до повної зупинки системи.

Також може спричинити низку проблем, включаючи крадіжку конфіденційних даних, таких як паролі, номери кредитних карток та іншу особисту інформацію. Шкідливе програмне забезпечення також може втручатися в роботу системи, спричиняючи низьку продуктивність або навіть повний збій системи. Крім того, шкідливе програмне забезпечення може використовуватися для дистанційного керування зараженими системами і може бути використане для подальших атак шляхом створення мереж заражених комп'ютерів, відомих як ботнети.

1.4.3 Зовнішні атаки.

Зовнішні атаки можуть походити з різних джерел, включаючи хакерів, кіберзлочинців та державних суб'єктів. Метою цих атак може бути викрадення конфіденційної інформації, виведення з ладу або знищення систем чи отримання несанкціонованого доступу.

Зовнішні атаки - це кібератаки, які відбуваються поза мережею або системами організації. Зовнішні атаки стають все більш поширеними, а кіберзлочинці та хакери постійно вдосконалюють свою тактику використання вразливостей і слабких місць в системах. Зовнішні атаки можуть набувати різних форм, зокрема

1. Фішингові атаки: Фішингові атаки передбачають надсилання користувачам фальшивих електронних листів, щоб змусити їх надати конфіденційну інформацію, таку як імена користувачів та паролі. Фішингові атаки можуть бути використані для отримання доступу до систем або викрадення конфіденційних даних.

2. Атаки на відмову в обслуговуванні (DoS-атаки): DoS-атака - це атака, яка перевантажує систему або мережу надмірним трафіком, роблячи її непридатною для законних користувачів; DoS-атаки можуть бути використані для порушення роботи служб або пограбування організацій.

3. Атаки "людина посередині" (MITM): MITM-атаки перехоплюють комунікацію між двома сторонами з метою викрадення даних або доступу до систем; MITM-атаки можуть бути використані для викрадення конфіденційних даних, таких як номери кредитних карток або облікові дані для входу в систему.

4. Атаки за допомогою паролів: Атаки на паролі - це спроби вгадати або розшифрувати паролі, щоб отримати доступ до систем або даних. Атаки на паролі можуть бути автоматизованими і можуть швидко скомпрометувати системи зі слабкими паролями або паролями, які легко вгадати.

5. Атаки з використанням програм-вимагачів: Атаки з вимогою викупу шифрують дані в системі або мережі і вимагають оплату в обмін на ключ для розшифрування. Атаки вірусів-здирників можуть спричинити значні збої в роботі та фінансові втрати.

6. Сучасні постійні загрози (APT): APT - це цілеспрямована атака, метою якої є отримання несанкціонованого доступу до системи протягом тривалого періоду часу; APT часто важко виявити і вони можуть завдати значної шкоди системам і даним.

Зовнішні атаки є серйозною загрозою для організацій будь-якого розміру, тому важливо мати надійні заходи безпеки для захисту від них. Такі заходи безпеки включають брандмауери, системи виявлення та запобігання вторгненням, антивірусне програмне забезпечення, а також програми навчання та підвищення обізнаності співробітників [6].

1.4.4 Стихійні лиха

Стихійні лиха, такі як повені, пожежі, землетруси та урагани, можуть пошкодити центри обробки даних, системи та обладнання, що призводить до втрати даних та перебоїв у роботі.

1.4.5 Технічні збої

Технічні збої, такі як несправності апаратного та програмного забезпечення, перебої в електропостачанні або збої в мережі, можуть призвести до втрати даних.

1.4.6 Інсайдерські загрози.

Внутрішні загрози можуть надходити від нинішніх або колишніх співробітників, підрядників або партнерів, які мають доступ до конфіденційної інформації. Ці загрози можуть включати крадіжку, саботаж і навмисне або ненавмисне розголошення конфіденційної інформації.

1.4.7 Відповідність нормативним вимогам.

Недотримання регуляторних вимог, таких як правила захисту даних, може призвести до штрафів, юридичних наслідків та шкоди для репутації.

1.4.8 Ризики ланцюга постачання.

Ризики ланцюга поставок включають такі вразливі місця, як незахищене програмне та апаратне забезпечення, а також слабкі практики безпеки в продуктах, послугах і процесах, що надаються сторонніми постачальниками та продавцями.

1.5 Аналіз причин виникнення ризиків в ІБ

Аналіз ризиків у системі управління інформаційною безпекою (СУІБ) визначає та оцінює потенційні ризики для інформаційних активів організації (наприклад, обладнання, програмного забезпечення, мереж, даних). Причини цих ризиків можуть відрізнятися залежно від конкретної ситуації в організації, але зазвичай вони поділяються на кілька широких категорій.

1.5.1 Людський фактор.

Одним з найважливіших джерел ризику в СУІБ є людські помилки. Це можуть бути як навмисні дії, такі як хакерство та соціальна інженерія, так і ненавмисні дії, такі як випадкове видалення важливих файлів або неправильне налаштування параметрів. Людський фактор також включає в себе такі фактори, як неналежне навчання, недостатня обізнаність та ненавмисна або зловмисна поведінка працівників, підрядників або сторонніх постачальників.

Людські фактори можуть бути значним джерелом ризику в СУІБ, оскільки їх важко контролювати і вони непередбачувані. Співробітники та сторонні постачальники часто є найслабшою ланкою в системі інформаційної безпеки, оскільки вони можуть ненавмисно або навмисно наражати організацію на ризик. Наприклад, працівник може випадково натиснути на фішинговий електронний лист або залишити свій пароль у незахищеному місці, тоді як зловмисник може навмисно викрасти конфіденційну інформацію або пошкодити системи.

Недостатня підготовка та недостатня обізнаність також можуть призвести до людських помилок. Працівники можуть не знати найновіших протоколів безпеки або не розуміти важливості дотримання встановлених процедур. Крім того, недбала або зловмисна поведінка працівників також може призвести до інцидентів безпеки. Наприклад, працівник, який завантажує несанкціоноване програмне забезпечення або використовує особистий пристрій для доступу до конфіденційної інформації, може поставити організацію під загрозу [7].

Для усунення людського фактору в СУІБ організації повинні впроваджувати комплексні програми навчання та підвищення обізнаності, щоб роз'яснити співробітникам і стороннім постачальникам важливість інформаційної безпеки. Вони також повинні впровадити надійні системи контролю доступу та моніторингу для виявлення та запобігання несанкціонованому доступу до інформації. Нарешті, організації повинні мати

чітку політику та процедури для реагування на інциденти безпеки та усунення потенційних загроз.

1.5.2 Технічні фактори.

Технологічні фактори є одними з основних факторів ризику в СУІБ. Ця категорія включає ризики, пов'язані з апаратними та програмними компонентами інформаційних систем організації, такими як сервери, бази даних, додатки та мережі. Технічні ризики виникають через недоліки проектування, помилки впровадження та недоліки конфігурації, які можуть призвести до збоїв у роботі системи, витоку даних та інших інцидентів, пов'язаних з безпекою.

Апаратні збої, такі як збій жорсткого диска, перебої в електропостачанні та збої в роботі мережевого обладнання, можуть призвести до перебоїв у роботі системи та втрати даних. Збої в програмному забезпеченні, такі як баги та програмні помилки, можуть призвести до збоїв у роботі системи, пошкодження даних та несанкціонованого доступу. Вразливості в програмних додатках та операційних системах також становлять значний ризик, оскільки вони можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем та викрадення конфіденційної інформації.

Щоб зменшити вплив технічних ризиків, організації повинні впроваджувати надійні заходи безпеки, включаючи брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення, а також надійні механізми шифрування та автентифікації. Вони також повинні регулярно моніторити та тестувати свої системи для виявлення та виправлення вразливостей і недоліків. Крім того, організації повинні мати плани аварійного відновлення та безперервності бізнесу, щоб забезпечити швидке відновлення після системних збоїв і катастроф.

1.5.3 Фактори навколишнього середовища

Екологічні фактори включають природні небезпеки, такі як повені, землетруси та урагани, а також техногенні небезпеки, такі як пожежі, відключення електроенергії та саботаж. Фактори навколишнього середовища також можуть включати зовнішні загрози, такі як кібератаки, крадіжки та промислове шпигунство.

1.5.4 Юридичні та регуляторні фактори

Правові та регуляторні фактори також можуть впливати на ризики СУІБ. Вони можуть включати вимоги щодо конфіденційності даних, безпеки та захисту інтелектуальної власності. Недотримання цих вимог може призвести до значних фінансових і репутаційних втрат для організації.

На додаток до нормативно-правових вимог, законодавчі та регуляторні фактори також включають ризик судових розглядів, штрафів і санкцій за недотримання галузевих норм. Наприклад, галузь охорони здоров'я зобов'язана дотримуватися вимог Закону про переносимість і підзвітність у сфері медичного страхування (HIPAA), який встановлює стандарти захисту медичної інформації про пацієнтів; недотримання вимог HIPAA може призвести до значних штрафів і юридичних наслідків.

Інші правові та регуляторні фактори, які можуть становити ризики для СУІБ, включають міжнародні нормативні акти, такі як Загальний регламент Європейського Союзу про захист даних (GDPR), який встановлює стандарти захисту даних і конфіденційності, і Каліфорнійський закон про конфіденційність споживачів (CCPA), який встановлює вимоги щодо захисту особистої інформації жителів Каліфорнії в США [7].

Організації повинні знати закони та правила, які застосовуються до їхньої галузі, і вживати відповідних заходів для забезпечення їх дотримання. Це може включати впровадження заходів із захисту даних, проведення регулярних аудитів та оцінок, а також розробку політик і процедур для забезпечення дотримання вимог. Невиконання цих вимог може мати серйозні юридичні та фінансові наслідки і зашкодити репутації організації.

1.5.5 Бізнес-фактори

Бізнес-фактори відіграють важливу роль у системі управління інформаційною безпекою (СУІБ) і можуть суттєво впливати на ризики, пов'язані з СУІБ.

1. Злиття та поглинання: Злиття та поглинання передбачають інтеграцію різних ІТ-систем, що може призвести до проблем інтероперабельності та ризиків для безпеки. Придбання нових активів або впровадження нових процесів також може створити нові вразливості.

2. Реорганізація. Реорганізація може передбачати зміни в посадових ролях, обов'язках та підпорядкуванні, що може призвести до помилок у протоколах безпеки. Вона також може включати консолідацію або децентралізацію ІТ-інфраструктури, що може призвести до нових ризиків.

3. Швидке зростання. Швидке зростання може призвести до перевантаження існуючої ІТ-інфраструктури, що може спричинити збої в роботі системи та втрату даних. Це також може призвести до нестачі кваліфікованого персоналу та неналежних заходів безпеки.

4. Скорочення штату: Скорочення штату збільшує навантаження на інших працівників і може призвести до помилок, упущень і збоїв у протоколах безпеки. Зміни в правах доступу та скорочення штату також можуть створити нові вразливості.

5. Зміни в бізнес-стратегії: зміни в бізнес-стратегії, такі як вихід на нові ринки або впровадження нових продуктів, можуть створювати нові ризики для безпеки. Такі зміни можуть вимагати використання нових технологій, які, можливо, не були належним чином протестовані або інтегровані з існуючими системами. Зміни у нормативно-правових вимогах також можуть вимагати впровадження нових засобів контролю безпеки.

Висновки до розділу 1

По-перше, кожен метод аналізу ризиків має свої переваги та недоліки, і організаціям слід обирати той метод, який найкраще відповідає їхнім потребам та ресурсам.

По-друге, аналіз причин виникнення ризиків в СУІБ є важливим кроком у розробці ефективної стратегії управління ризиками. Визначивши конкретні причини ризиків, організації можуть розробити цілеспрямовані рішення для усунення цих ризиків та мінімізації їхнього потенційного впливу.

По-третє, організаціям важливо враховувати потенційні ризики, пов'язані з цими бізнес-чинниками, і вживати превентивних заходів для їхнього зменшення. Це може включати впровадження надійних протоколів безпеки, проведення регулярних оцінок ризиків та забезпечення дотримання відповідних норм і стандартів.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ РИЗИКІВ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Аналіз наявних методів аналізу ризиків

Методи аналізу ризиків відіграють важливу роль у створенні ефективної системи управління інформаційною безпекою (СУІБ) організації. Існує багато методів аналізу ризиків, які були розроблені та застосовуються різними організаціями. Цей розділ містить огляд і порівняльний аналіз деяких з них.

2.1.1 Методологія оцінки ризиків ISO 27001

ISO 27001 є широко визнаним стандартом СУІБ; методологія оцінки ризиків ISO 27001 включає етапи ідентифікації активів, ідентифікації загроз, ідентифікації вразливостей, оцінки ризиків та вибору засобів контролю.

Методологія використовує формулу для розрахунку рівня ризику на основі ймовірності та впливу ризику. Методологія ISO 27001 є всеосяжною, гнучкою та підходить для всіх типів організацій. Однак вона може зайняти багато часу і бути складною для впровадження в невеликих організаціях.

ISO 27001 є міжнародним стандартом для СУІБ і забезпечує системний підхід до управління та захисту конфіденційної інформації Методологія оцінки ризиків, викладена в ISO 27001, є важливим компонентом його структури і включає в себе ряд кроків для виявлення та управління ризиками для інформаційних активів [8].

Першим кроком в методології оцінки ризиків ISO 27001 є визначення активів, які необхідно захистити, включаючи апаратне забезпечення, програмне забезпечення та дані. Наступним кроком є визначення потенційних загроз для

цих активів, таких як людські помилки, стихійні лиха та кібератаки. Після того, як загрози визначені, виявляються та оцінюються вразливості системи. Це передбачає вивчення потенційних слабких місць у заходах безпеки, впроваджених для захисту активів.

Після виявлення вразливостей наступним кроком є оцінка ризиків, пов'язаних з кожною загрозою, з огляду на ймовірність реалізації ризику та потенційний вплив ризику. Зазвичай це робиться за допомогою формули, яка розраховує рівень ризику на основі ймовірності та впливу ризику.

Методологія ISO 27001 також рекомендує набір засобів контролю для управління та пом'якшення виявлених ризиків. Ці засоби включають технічні рішення, такі як брандмауери та шифрування, а також адміністративні засоби, такі як політики та процедури. Засоби контролю слід обирати на основі їхньої ефективності в управлінні виявленими ризиками, а також їхньої здатності впроваджувати та підтримувати.

Методологія ISO 27001 є всеосяжною і підходить для всіх типів організацій, але може зайняти багато часу і бути складною для впровадження в невеликих організаціях. Слід зазначити, що відповідність стандарту ISO 27001 не гарантує повну безпеку, а скоріше забезпечує основу для управління ризиками і створення ефективних засобів контролю безпеки.

2.1.2 Структура управління ризиками NIST:

NIST Risk Management Framework (RMF) - це структурований підхід до управління ризиками. Вона складається з шести етапів: категоризація інформаційних систем, вибір засобів контролю безпеки, впровадження засобів контролю безпеки, оцінка засобів контролю безпеки, авторизація інформаційних систем і моніторинг засобів контролю безпеки. Однак його впровадження може бути складним і трудомістким, особливо для невеликих організацій.

Система управління ризиками Національного інституту стандартів і технологій (NIST) - це структурований підхід до управління ризиками для інформації та систем організації. Це широко визнаний підхід, який використовується багатьма організаціями, в тому числі урядом США, для управління ризиками інформаційної безпеки.

NIST RMF складається з шести етапів

1. Класифікація інформаційних систем: на цьому етапі визначаються та класифікуються інформаційні системи відповідно до їх важливості та впливу на місію та цілі організації. Цей крок допомагає визначити ризики, пов'язані з кожною системою.

2. Вибір засобів контролю безпеки: Цей крок передбачає вибір відповідних засобів контролю безпеки на основі ризиків, виявлених на попередньому кроці. Засоби контролю обираються на основі низки критеріїв, включаючи класифікацію системи, толерантність організації до ризиків та інші фактори.

3. Впровадження засобів контролю безпеки: На цьому етапі відбувається впровадження обраних засобів контролю безпеки. Засоби контролю можуть бути технічними, адміністративними або фізичними за своєю природою.

4. Оцінка засобів контролю безпеки: На цьому етапі оцінюється ефективність впроваджених засобів контролю безпеки. Це може бути зроблено шляхом тестування, аудиту або іншими методами.

5. Авторизація інформаційної системи: на цьому етапі надається дозвіл на експлуатацію інформаційної системи на основі результатів оцінки заходів контролю безпеки. Дозвіл може бути наданий тільки в тому випадку, якщо ризики, пов'язані з системою, знаходяться в прийнятних межах.

6. Моніторинг засобів контролю безпеки: Цей крок передбачає безперервний моніторинг засобів контролю безпеки для підтримки їх ефективності, а також для виявлення та усунення ризиків, що виникають.

NIST RMF - це комплексна методологія, яка забезпечує структурований підхід до управління ризиками інформаційної безпеки. Однак її впровадження може бути складним і трудомістким, особливо для невеликих організацій. Воно вимагає значних витрат часу, кадрових і фінансових ресурсів.

2.1.3 OCTAVE

Оперативна оцінка критичних загроз, активів та вразливостей (OCTAVE) - це метод оцінки ризиків, який фокусується на виявленні та усуненні організаційних вразливостей. Метод OCTAVE складається з трьох етапів: виявлення, оцінка та впровадження. Метод OCTAVE - це комплексний і гнучкий підхід, який можна адаптувати до потреб різних організацій. Однак його ефективне застосування вимагає значних ресурсів і досвіду.

Оперативна критична оцінка загроз, активів та вразливостей (OCTAVE) - це методологія оцінки ризиків, розроблена Інститутом інженерії програмного забезпечення (SEI) Університету Карнегі-Меллона. Метод OCTAVE - це комплексний та гнучкий підхід до оцінки інформаційних активів та вразливостей організації, призначений для виявлення та усунення вразливостей у критичних бізнес-процесах [9].

Метод OCTAVE складається з трьох етапів:

1. Ідентифікація: На цьому етапі організація визначає свої критичні активи та бізнес-процеси, а також існуючі політики та процедури безпеки. Також визначаються потенційні загрози для активів і процесів.

2. Оцінка: на цьому етапі організація оцінює ризики, пов'язані з критично важливими активами та бізнес-процесами. Це включає виявлення вразливостей і визначення потенційного впливу загроз.

3. Реалізація: на цьому етапі організація впроваджує заходи контролю безпеки для зменшення виявлених ризиків. Це включає вибір і впровадження відповідних заходів контролю безпеки та моніторинг їхньої ефективності.

Однією з сильних сторін Закону OCTAVE є його зосередженість на вразливих місцях організації. Виявляючи та усуваючи вразливі місця, організації можуть зменшити свій загальний ризик. Метод OCTAVE також є гнучким і може бути адаптований до потреб різних організацій.

Однак метод OCTAVE є ресурсномістким і вимагає значного досвіду для ефективного застосування. Він також може бути менш придатним для невеликих організацій з обмеженими ресурсами.

2.1.4 Метод FAIR:

Факторний аналіз інформаційних ризиків (FAIR) - це метод кількісного аналізу ризиків, який визначає та оцінює фактори, що впливають на ризик настання події: визначення сфери застосування, збір даних, аналіз, фактори ризику, аналіз ризику та обробка ризику Метод FAIR забезпечує комплексний і кількісний аналіз ризику, але вимагає значних знань і ресурсів для його реалізації.

FAIR (Factor Analysis of Information Risk - факторний аналіз інформаційного ризику) - це методологія кількісної оцінки ризиків, яка має на меті визначити та оцінити фактори, що впливають на ризик настання події. Методологія покликана забезпечити всебічний кількісний аналіз ризиків, щоб допомогти організаціям приймати обґрунтовані рішення щодо стратегій управління ризиками та їх зниження.

Методологія FAIR включає наступні шість кроків

1. Сфера застосування: на цьому етапі визначається сфера застосування оцінки ризиків, включаючи активи та процеси, що підлягають оцінці, залучених осіб та схильність організації до ризику

2. Збір даних: на цьому етапі збираються дані про потенційні загрози, вразливості та впливи, пов'язані з визначеними активами та процесами.

3. Аналіз: Дані, зібрані на цьому етапі, аналізуються для визначення факторів, що сприяють ризику виникнення інциденту, включаючи ймовірність виникнення загрози, вразливість активу або процесу та потенційний вплив інциденту.

4. Фактори ризику: на цьому етапі визначені фактори оцінюються з метою визначення їх відносної важливості для загального ризику.

5. Аналіз ризиків: на цьому етапі виявлені фактори об'єднуються та аналізуються за допомогою математичних моделей для розрахунку ймовірності та впливу ризикових подій.

6. Обробка ризиків: На цьому завершальному етапі результати аналізу ризиків використовуються для розробки стратегій управління ризиками, таких як передача ризику, уникнення ризику, зниження ризику та прийняття ризику.

Аналіз ризиків є важливим процесом у розробці ефективної системи управління інформаційною безпекою (СУІБ). Аналіз ризиків передбачає виявлення потенційних ризиків, оцінку їхньої ймовірності та впливу, а також розробку стратегій управління ними. Процес аналізу ризиків, як правило, складається з декількох етапів, включаючи визначення обсягу, збір даних, аналіз, фактори ризику, аналіз ризиків та управління ризиками [11].

На етапі визначення сфери застосування визначається обсяг оцінки ризиків, включаючи активи та процеси, що підлягають оцінці, залучених осіб та схильність організації до ризику. Цей етап допомагає забезпечити цілеспрямованість процесу аналізу ризиків та його адаптацію до конкретних потреб організації.

Етап збору даних передбачає збір даних про потенційні загрози, вразливості та впливи, пов'язані з визначеними активами та процесами. Це може

включати перегляд наявної документації, проведення інтерв'ю або інші методи збору відповідної інформації.

На етапі аналізу зібрані дані аналізуються для виявлення факторів, що сприяють підвищенню ризику виникнення інциденту. Це може включати визначення ймовірності виникнення загрози, вразливості активу або процесу та потенційного впливу події.

На етапі визначення факторів ризику ідентифіковані фактори оцінюються для визначення їхньої відносної важливості у формуванні загального ризику. Це дозволяє розставити пріоритети в управлінні ризиками та розподілити ресурси належним чином.

На етапі аналізу ризиків виявлені фактори об'єднуються та аналізуються за допомогою математичних моделей для розрахунку ймовірності та впливу ризикових подій. Це дає змогу кількісно оцінити ризики та прийняти обґрунтовані рішення щодо управління ризиками.

На етапі обробки ризиків результати аналізу ризиків використовуються для розробки стратегій обробки ризиків, таких як передача ризиків, уникнення ризиків, зменшення ризиків і прийняття ризиків. Ці стратегії допомагають управляти виявленими ризиками і гарантують, що організація належним чином підготовлена до протидії потенційним загрозам.

Методологія FAIR забезпечує структурований і систематичний підхід до аналізу ризиків, який допомагає організаціям визначати пріоритети і розподіляти ресурси для ефективного управління ризиками. Однак її впровадження вимагає значних знань і ресурсів і може не підходити для невеликих організацій або організацій з обмеженими ресурсами.

2.1.5 CRAMM:

Метод аналізу та управління ризиками ССТА (CRAMM) - це метод аналізу ризиків для виявлення та оцінки ризиків для IT-систем. Метод CRAMM складається з семи етапів: ідентифікація активів, ідентифікація загроз, ідентифікація вразливостей, оцінка ризиків, ідентифікація засобів контролю, оцінка засобів контролю та огляд. Він включає в себе наступні кроки: Метод CRAMM - це комплексний і структурований підхід, який підходить для великих організацій. Однак його впровадження може бути складним і трудомістким.

Метод CRAMM складається з семи кроків:

1. Ідентифікація активів: На цьому етапі визначаються IT-системи та активи, які потребують захисту, в тому числі обладнання, програмне забезпечення, дані та мережі.

2. Ідентифікація загроз: На цьому етапі визначаються потенційні загрози для IT-систем та активів, такі як кібератаки, стихійні лиха та людські помилки.

3. Виявлення вразливостей: на цьому етапі виявляються слабкі місця в IT-системах та активах, які можуть бути використані виявленими загрозами.

4. Оцінка ризиків. На цьому етапі оцінюється ступінь ризику, пов'язаного з кожною комбінацією загрози та вразливості.

5. Визначення засобів контролю: На цьому етапі визначаються засоби контролю, які можуть бути впроваджені для зменшення або усунення виявлених ризиків.

6. Оцінка контролів: на цьому етапі оцінюється ефективність визначених контролів у зменшенні або усуненні виявлених ризиків.

7. Перегляд: на цьому етапі процес оцінки та управління ризиками переглядається, щоб переконатися, що він залишається ефективним та актуальним.

Метод CRAMM - це метод аналізу та управління ризиками, який широко використовується в галузі інформаційних технологій (IT). Метод CRAMM включає сім кроків, які допомагають організаціям ідентифікувати та управляти ризиками для своїх IT-систем та активів.

Першим кроком методу CRAMM є визначення активів, які потребують захисту. Ці активи включають в себе обладнання, програмне забезпечення, дані та мережі. На цьому етапі створюється список всіх активів і систем, які необхідно захистити, який використовується на наступному етапі.

Другий крок - визначення потенційних загроз для IT-систем та активів. Ці загрози можуть включати кібератаки, стихійні лиха, людські помилки та інші потенційні ризики. Цей крок передбачає оцінку зовнішнього та внутрішнього середовища та виявлення загроз, які можуть завдати шкоди IT-системам та активам організації.

Третій крок - виявлення вразливостей в IT-системах та активах. Виявлені загрози можуть використовувати ці вразливості, такі як застаріле програмне забезпечення, слабкі паролі та неадекватні налаштування безпеки. Цей крок передбачає оцінку IT-систем та активів з метою виявлення слабких місць, які можуть бути використані потенційними загрозами.

Четвертий крок - оцінка рівня ризику, пов'язаного з кожною комбінацією загрози та вразливості. Кожному ризику, виявленому на цьому етапі, присвоюється оцінка ймовірності та впливу, а також визначається загальний рівень ризику, пов'язаний з поєднанням потенційної загрози та вразливості.

На п'ятому етапі визначаються заходи контролю, які можуть бути впроваджені для зменшення або усунення виявлених ризиків. Ці заходи можуть включати технічні, адміністративні та фізичні засоби контролю, такі як брандмауери, системи виявлення вторгнень, контроль доступу та політики безпеки.

Шостий крок - оцінка ефективності визначених засобів контролю для зменшення або усунення виявлених ризиків. На цьому етапі здійснюється тестування засобів контролю та оцінюється їхня ефективність для зменшення ймовірності та впливу виявлених ризиків.

Останнім кроком є аналіз процесу оцінки та управління ризиками, щоб переконатися, що він є ефективним і доцільним. Цей крок передбачає регулярну переоцінку ризиків і засобів контролю, щоб переконатися, що вони залишаються актуальними та ефективними у зменшенні ризиків, пов'язаних з IT-системами та активами організації.

Загалом, методологія CRAMM - це комплексний та структурований підхід до аналізу та управління ризиками, який допомагає організаціям виявляти та управляти ризиками для своїх IT-систем та активів. Однак її впровадження може бути складним і трудомістким, особливо в невеликих організаціях.

Метод CRAMM - це комплексний і структурований підхід до аналізу та управління ризиками. Він підходить для великих організацій зі складними IT-системами та активами. Однак його впровадження є складним і трудомістким і може вимагати значних ресурсів і досвіду. Крім того, технології постійно розвиваються, і для підтримки ефективності методів CRAMM можуть знадобитися регулярні оновлення.

Таким чином, кожен метод аналізу ризиків має свої сильні та слабкі сторони, і організаціям слід обирати той метод, який найкраще відповідає їхнім потребам. Комплексна та добре впроваджена методологія аналізу ризиків має важливе значення для розробки та підтримки ефективної СУІБ в організації.

2.2 Опис методів аналізу ризиків

Аналіз ризиків є важливим процесом для виявлення, оцінки та управління ризиками в системі управління інформаційною безпекою. Для аналізу ризиків в

ІБ використовуються різні методи, кожен з яких має свої переваги та недоліки. У цьому розділі проаналізовано переваги та недоліки використання різних методів аналізу ризиків у сфері інформаційної безпеки.

2.2.1 Якісний аналіз ризику:

Якісний аналіз ризиків - це суб'єктивний метод, який оцінює ризики відповідно до їхньої ймовірності та впливу. Він включає ідентифікацію ризиків, аналіз їхньої ймовірності та впливу, а також оцінку ризиків відповідно до їхньої значущості. Він простий, економічно ефективний і не вимагає особливих експертних знань. Однак цей метод має кілька обмежень. Оцінки є суб'єктивними і залежать від сприйняття особи, яка проводить оцінку, що може призвести до непослідовних результатів. Метод не забезпечує точного вимірювання ризику, що ускладнює визначення пріоритетності ризиків.

Якісний аналіз ризиків є поширеним методом оцінки ризиків у системах управління інформаційною безпекою. Це суб'єктивний підхід, який фокусується на ймовірності та впливі ризиків.

Першим кроком у якісному аналізі ризиків є виявлення ризиків, які можуть становити загрозу інформаційній безпеці організації. Після визначення ризиків експерт аналізує ймовірність настання кожного ризику та вплив на організацію в разі його настання. Потім експерт оцінює кожен ризик відповідно до його серйозності, як правило, за шкалою низького, середнього або високого рівня.

Переваги якісного аналізу ризиків полягають у тому, що він простий, економічно ефективний і не вимагає спеціальних знань. Він підходить для організацій з обмеженими ресурсами та низькою толерантністю до ризиків. Крім того, він забезпечує широкий огляд ризиків і допомагає визначити сфери, які потребують додаткової уваги [12].

Однак цей метод має кілька обмежень. Оцінки є суб'єктивними і залежать від сприйняття експерта, що робить результати непослідовними. Крім того, різні експерти можуть надавати різний ступінь важливості одному й тому ж ризику, що може призвести до плутанини та непорозумінь. Крім того, цей метод не забезпечує точного вимірювання ризику і ускладнює визначення пріоритетності ризиків. Як наслідок, сферам високого ризику може бути надано недостатньо уваги, тоді як сферам низького ризику може бути надано занадто багато уваги.

Загалом, якісний аналіз ризиків може бути корисною відправною точкою для організацій з обмеженими ресурсами та низькою толерантністю до ризиків. Однак важливо доповнити його іншими методами аналізу ризиків, щоб забезпечити всебічну і точну оцінку ризиків.

2.2.2 Кількісний аналіз ризику:

Кількісний аналіз ризиків забезпечує більш об'єктивний підхід до оцінки ризиків. Він використовує математичні моделі для вимірювання ймовірності та впливу ризиків. Застосування цього методу вимагає більше технічних знань і ресурсів, але забезпечує більш точне вимірювання ризику. Він полегшує визначення пріоритетності ризиків і забезпечує більш надійну основу для прийняття рішень. Однак цей метод є трудомістким і дорогим, а також вимагає значної кількості даних для точного аналізу.

Кількісний аналіз ризиків - це структурований метод вимірювання ймовірності та впливу ризиків за допомогою числових даних. Він передбачає збір та аналіз даних для визначення ймовірності та серйозності потенційних ризиків. Статистичні моделі, симуляції та інші математичні інструменти використовуються для оцінки ймовірності та впливу кожного сценарію ризику.

Однією з переваг кількісного аналізу ризиків є його точність. Використання математичних моделей забезпечує більш точне та об'єктивне вимірювання

ризику. Це дозволяє визначати пріоритети ризиків та ефективно розподіляти ресурси. Це також дає більш точну картину потенційного впливу різних ризиків, створюючи більш надійну основу для прийняття рішень.

Ще однією перевагою кількісного аналізу ризиків є те, що він допомагає виявити прогалини в існуючому середовищі контролю. Систематично аналізуючи ризики, цей метод може виявити сфери, де контроль є неефективним або потребує вдосконалення. Це може допомогти організаціям приймати обґрунтовані рішення про те, куди інвестувати, щоб покращити контролі.

Однак кількісний аналіз ризиків має певні обмеження. Він займає багато часу, оскільки вимагає великих обсягів даних і досвіду для проведення точного аналізу. Він також може бути дорогим у впровадженні, особливо в малих і середніх організаціях з обмеженими ресурсами. Крім того, результати цього методу можуть залежати від якості та точності вхідних даних, і завжди існує ризик помилок моделювання та припущень, що впливають на точність результатів.

Таким чином, кількісний аналіз ризиків забезпечує більш точне та об'єктивне вимірювання ризиків і дозволяє організаціям приймати більш обґрунтовані рішення щодо визначення пріоритетності ризиків та розподілу ресурсів. Однак застосування цього методу вимагає значних ресурсів і досвіду, а точність результатів залежить від якості та достовірності вхідних даних.

2.2.3 Аналіз ризиків Дельфі:

Метод Дельфі - це метод, заснований на консенсусі, в якому група експертів дає зворотний зв'язок кілька разів. Цей метод дозволяє розглянути різні точки зору і більш точно оцінити ризик.

Це ефективний метод для комплексного аналізу ризиків і може надати більш детальну інформацію, ніж інші методи. Однак цей метод є трудомістким і

дорогим, а також може бути складно керувати зворотним зв'язком від декількох експертів і об'єднувати їхні думки.

Метод Дельфі - це структурований підхід, який використовується для групової комунікації та прийняття рішень у ситуаціях, коли експертам необхідно надати зворотний зв'язок на основі консенсусу. Анкети або опитування надсилаються групі експертів у кілька раундів. Експерти залишаються анонімними, а після кожного раунду зворотний зв'язок узагальнюється і передається групі. Членам групи надається можливість коригувати свої відповіді на основі зворотного зв'язку з попередніх раундів, доки не буде досягнуто консенсусу.

Метод Дельфі особливо корисний для складних аналізів ризиків, які вимагають участі великої кількості експертів з різними точками зору. Експерти можуть надавати зворотний зв'язок, не піддаючись впливу групової динаміки або думок інших. Це також сприяє чесному і відкритому спілкуванню, оскільки учасники є анонімними.

Перевагою методу Дельфі є те, що він надає більш детальну інформацію, ніж інші методи аналізу ризиків. Експерти можуть давати більш детальні відповіді, а кілька раундів зворотного зв'язку можуть прояснити і уточнити певні моменти.

Однак метод Дельфі вимагає багато часу і є дорогим. Процес збору відгуків від великої кількості експертів і зіставлення їхніх відповідей може зайняти значний час. Крім того, експерти можуть мати конкуруючі пріоритети, що ускладнює координацію їхньої участі в процесі.

Ще одним недоліком методу Дельфі є складність управління та об'єднання зворотного зв'язку від великої кількості експертів. Процес потребує кваліфікованого фасилітатора, який керуватиме комунікацією та гарантуватиме, що зворотний зв'язок буде правильно зрозумілий і відображений у кінцевому результаті.

Незважаючи на ці виклики, метод Дельфі є ефективним інструментом для комплексного аналізу ризиків, що вимагає участі багатьох експертів. Він може забезпечити детальну і точну оцінку ризиків та уможливити прийняття рішень на основі консенсусу.

2.2.4 Аналіз ризиків на основі сценарію

Сценарний аналіз ризиків передбачає створення сценаріїв потенційних ризиків та оцінку їхньої ймовірності та впливу. Цей метод забезпечує більш проактивний підхід до управління ризиками і дозволяє виявити потенційні ризики до того, як вони виникнуть. Він також забезпечує краще розуміння ризиків та їхнього потенційного впливу. Однак цей підхід обмежений кількістю створених сценаріїв і точністю даних, що використовуються в оцінці.

Сценарний аналіз ризиків - це метод створення та оцінки потенційних сценаріїв ризиків для організації. Розглядаються ймовірність і потенційний вплив кожного сценарію, а також визначаються найбільш значущі ризики і встановлюється їх пріоритетність. Аналіз ризиків на основі сценаріїв є проактивним і дозволяє організаціям виявляти потенційні ризики до того, як вони виникнуть, що дає можливість для раннього втручання та пом'якшення наслідків.

Однією з переваг сценарного аналізу ризиків є те, що він забезпечує більш глибоке розуміння ризиків та їх потенційних наслідків. Метод дозволяє оцінити різні сценарії ризиків і дає розуміння того, як конкретний ризик може вплинути на організацію. Метод допомагає організаціям передбачати вплив різних ризиків і приймати обґрунтовані рішення щодо стратегій управління ризиками.

Однак аналіз ризиків на основі сценаріїв обмежений кількістю згенерованих сценаріїв і точністю даних, які використовуються для оцінки сценаріїв. Організаціям необхідно розробити широкий спектр сценаріїв, щоб забезпечити врахування всіх потенційних ризиків, що може зайняти багато часу

та ресурсів. Крім того, точність даних, що використовуються для оцінки кожного сценарію, є критично важливою, оскільки вона впливає на надійність результатів.

Загалом, аналіз ризиків на основі сценаріїв є ефективним способом виявлення потенційних ризиків та розробки відповідних стратегій управління ризиками. Цей підхід дозволяє організаціям застосовувати проактивний підхід до управління ризиками та приймати обґрунтовані рішення на основі оцінки різних сценаріїв. Однак важливо розробити широкий спектр сценаріїв, щоб забезпечити надійність результатів і точність даних, які використовуються в оцінці.

2.2.5 Аналіз ризиків і критичні контрольні точки (HACCP):

HACCP - це системний підхід, який використовується для виявлення, оцінки та контролю ризиків для безпеки харчових продуктів. Він передбачає визначення критичних контрольних точок у процесі та розробку засобів контролю для зменшення ризиків. Цей підхід може бути застосований до інформаційної безпеки і є корисним для виявлення та управління ризиками в конкретних процесах. Однак він не забезпечує повного аналізу всіх ризиків в організації і може не підходити для складних систем.

Аналіз ризиків та критичні контрольні точки (HACCP) - це систематичний метод, який використовується в харчовій промисловості для виявлення, оцінки та контролю ризиків для безпеки харчових продуктів. Метод визначає потенційні небезпеки в процесі та розробляє засоби контролю для зменшення небезпеки в певних точках процесу, які називаються критичними контрольними точками (ККТ).

HACCP також може застосовуватися до інформаційної безпеки і є корисним для виявлення та управління ризиками в конкретних процесах і сферах діяльності організації. Процес визначає критичні точки в системі, де можуть виникати ризики, і розробляє засоби контролю для управління цими ризиками.

Метод забезпечує структурований підхід до управління ризиками та гарантує, що ризики систематично ідентифікуються та контролюються.

Перевага методу HACCP полягає в тому, що він зосереджений на запобіганні ризикам, а не на реагуванні на них. Цей проактивний підхід також може бути застосований до інформаційної безпеки і допомагає організаціям заздалегідь виявляти потенційні ризики та вживати заходів для їх пом'якшення. Метод HACCP також забезпечує послідовність і повторюваність, запроваджуючи стандартизований підхід до управління ризиками.

Однак метод HACCP не забезпечує повного аналізу всіх ризиків в організації і може не підходити для складних систем, де взаємодіє багато ризиків. Крім того, для належного впровадження методу HACCP може знадобитися значний час і ресурси. Слід також зазначити, що метод HACCP не є панацеєю і повинен бути адаптований до конкретних потреб і обставин кожної організації.

Висновки до розділу 2

Таким чином, кожен метод аналізу ризиків має свої переваги та недоліки. Вибір методу залежить від потреб організації, її ресурсів і складності системи, що аналізується. Більш повний і точний аналіз ризиків може бути досягнутий шляхом поєднання декількох методів.

РОЗДІЛ 3
КОМБІНОВАНИЙ МЕТОД АНАЛІЗУ РИЗИКІВ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1 Роль Системи управління інформаційною безпекою

Організації повинні надавати пріоритет конфіденційності, доступності та цілісності інформації, щоб виконувати свої юридичні та регуляторні зобов'язання і підтримувати довірливі ділові відносини. Система управління інформаційною безпекою (СУІБ) може надати цінну допомогу в подоланні ризиків інформаційної безпеки та кібератак. Існують різні підходи до впровадження СУІБ, але етап оцінки ризиків виділяється як найбільш важливий і трудомісткий. Цей розділ має на меті показати систему аналізу та оцінки ризиків для використання інформаційно-технологічними компаніями, щоб відповідати вимогам стандарту Міжнародної організації зі стандартизації (ISO) 27001. У ньому розглядаються фактори, які мотивують організації інвестувати в інформаційну безпеку, а також переваги, які можна отримати від цього процесу.

3.2 Роль стандарту ISO 27001 у впровадженні систем управління інформаційною безпекою.

Інформація завжди була важливим активом підприємств, і потребувала, і потребує захисту. У сучасному світі більшість інформації зберігається в цифровому вигляді та доступна онлайн, що полегшує доступ до неї та мінімізує час, витрачений на архівування. Однак, це має і свій недолік. Будь-яка інформація може піддаватися різним ризикам і загрозам залежно від її важливості. Зростання компанії робить її привабливою мішенню для кібератак, а витік даних може

завдати шкоди репутації, доходам і довірі до компанії. З цих причин система управління інформаційною безпекою (СУІБ) має важливе значення для залучення нових клієнтів та утримання існуючих. Всі клієнти повинні знати, що інформація, якою вони діляться, захищена та належним чином управляється.

Стандарт Міжнародної організації зі стандартизації (ISO) 27001 - це система управління, яка знаходить механізми для виявлення, оцінки та подолання ризиків. Стандарт може слугувати керівництвом для розробки ефективної СУІБ, адаптованої до потреб організації, а впровадження СУІБ означає, що кожна компанія повинна розробити стратегію для кращого реагування на ризики та загрози інформаційній безпеці і в кінцевому підсумку створити СУІБ, яка відповідає стандарту ISO 27001. Стандарт не визначає конкретних процедур для реалізації вимог; натомість, вони повинні бути встановлені та впроваджені відповідно до компанії.

Існує багато різних підходів до того, як успішно впровадити СУІБ на підприємстві, бажаний результат є однаковим: забезпечити безпеку інформації та знайти оптимальне рішення, що відповідає потребам компанії. Крім того, однією з найбільш важливих і трудомістких частин створення СУІБ в компанії є оцінка ризиків. Всі можливі ризики повинні бути ідентифіковані, оцінені та класифіковані. Оскільки кожна компанія відрізняється від іншої, ризики також можуть відрізнятися, і не існує єдиного підходу, який кожна компанія може використовувати для оцінки ризиків.

Політика компаній гарантує, що інформація, з якою вона працювала як в електронному, так і в паперовому вигляді, буде належним чином захищена від наслідків порушення конфіденційності, порушення цілісності або обмеження доступу до цієї інформації. В компаніях є багато процесів. Однак більшість з них не фіксуються регулярно або взагалі не фіксувалися. Іншими словами, багато загроз не були ідентифіковані.

3.3 Переваги систем управління інформаційною безпекою

На мою думку, інформаційна безпека є частиною управління ІТ. Виходячи з цього, можна зрозуміти важливість інформаційної безпеки в бізнес-стратегії сучасних конкурентоспроможних компаній. Компанії можуть обробляти або зберігати дані, які можна віднести до різних типів інформації. Від записів про клієнтів і співробітників до бухгалтерських даних - вся ця інформація повинна бути доступною, щоб компанія могла нормально функціонувати. Вся ця інформація повинна бути захищена, і компанії, акції яких котируються на біржі, повинні вибрати і впровадити відповідні заходи для захисту своїх фізичних і фінансових активів, репутації, юридичного статусу, персоналу та інших матеріальних і нематеріальних активів. Саме тут у гру вступає СУІБ.

У літературі існують певні дискусії щодо цілей СУІБ. Основною метою інформаційної безпеки є захист цінних ресурсів організації (інформації, програмного забезпечення та обладнання). Плани, практики та процеси СУІБ повинні бути здатні зупинити та захистити обладнання, програмне забезпечення та інформацію користувачів від зовнішніх та внутрішніх загроз, навіть якщо компанія або організація знаходиться під загрозою.

З вищесказаного можна зрозуміти, що СУІБ є необхідною, оскільки вона здатна захистити критичні активи. Однак, впровадження СУІБ є непростим завданням, і погане планування може мати негативний вплив на компанію. Зокрема, при впровадженні СУІБ компанії можуть прийняти процеси та політики, які перешкоджають її функціонуванню. Перевірки інформаційної безпеки можуть забирати багато часу і можуть ускладнювати або забирати багато часу у персоналу при виконанні своїх щоденних завдань. Це також збільшує робоче навантаження, оскільки доступ до інформації обмежується. Крім того, може погіршитися якість роботи, оскільки неможливо підтримувати операційні стандарти, які існували до впровадження СУІБ. Нарешті, наявний персонал

повинен буде виділити час для проведення додаткових аудитів інформаційної безпеки або залучити до виконання цих завдань іншу команду.

З вищезазначених причин, організація та економічна ефективність є важливими компонентами ефективної СУІБ. Процедури СУІБ, які є важливим компонентом кожної СУІБ, повинні бути узгоджені з цілями та місією організації.

Щоб уникнути додаткових витрат, збільшення робочого навантаження та зниження якості, це слід враховувати на етапі розробки, а не на етапі впровадження успішної СУІБ. Основна концепція СУІБ полягає в забезпеченні конфіденційності, цілісності та доступності всієї інформації та даних. Конфіденційність - це ідея про те, що інформація та дані не повинні бути доступними для неавторизованих осіб. Компанії мають справу з фінансовими документами, комерційними кодами, даними клієнтів та особистою інформацією. Цілісність стосується несанкціонованих змін даних та інформації; СУІБ не може гарантувати точність збереженої інформації та даних, але включає процеси та інструменти для перевірки того, що зміни є запланованими, належним чином впровадженими, а також відсутності несанкціонованих подій. Доступність стосується інформації та систем, які завжди повинні бути доступними на вимогу. Найпоширенішими загрозами є відмова в обслуговуванні та втрата потужності обробки даних. Відмова в обслуговуванні - це дії користувача або зловмисника, які блокують обчислювальні послуги. Втрата потужності обробки даних - це руйнування обчислювального обладнання або програмних ресурсів фізично (внаслідок стихійних лих, або техногенних катастроф), або через недоступність програмного забезпечення (внаслідок зловмисного доступу до системи або помилки адміністратора).

Хоча компанії впроваджують засоби контролю для захисту свого фізичного, технічного та адміністративного середовища, не можна ігнорувати важливість дотримання балансу між конфіденційністю, цілісністю та

доступністю. Досягнення золотої середини є складним завданням. Наприклад, конфіденційність може бути порушена для забезпечення високої доступності. З іншого боку, акцент компанії на конфіденційності може ускладнити забезпечення доступності.

Бізнес є залежним від підключення до Інтернету. У той же час, підприємства одночасно працюють у дуже складному і мінливому середовищі загроз безпеці, яке наражає їхню інформаційну інфраструктуру на різноманітні ризики. Це змушує підприємства стикатися з безпрецедентними викликами і, зрештою, будувати більш безпечні інформаційно-технологічні (IT) інфраструктури. Кібератаки на компанії можуть серйозно зашкодити їхній репутації та інвестиціям. Незаперечним факт, що одне порушення безпеки може завдати непоправної шкоди компанії з точки зору корпоративної відповідальності, втрати довіри та зменшення доходів.

Від інцидентів безпеки страждають усі зацікавлені сторони, але в той же час, в більшості випадків співробітники не розуміють важливості конфіденційності даних компанії і не вживають необхідних заходів для того, щоб не допустити порушення.

Хоча компанії, організації та фірми визнають важливість аналізу, оцінки та ефективного зменшення ризиків, обов'язки та плани протидії загрозам інформаційній безпеці, як правило, недостатньо чітко визначені Впровадження системи управління інформаційною безпекою, наприклад, ISO 27001, може допомогти забезпечити запобігання цим загрозам і є ефективним і важливим способом забезпечення безпечної та надійної обробки даних.

ISO 27001 може принести численні важливі переваги компаніям та організаціям. Впроваджуючи ISO 27001, компанії встановлюють прозорі процеси управління доступом, контролем та обробкою інформації, а також послідовно захищають та управляють конфіденційними даними. Для цього процеси обробки даних повинні бути чіткими та постійно керованими. Крім того, ISO 27001

покращує репутацію компанії. Це також інтерпретується як збільшення прибутку та частки ринку, оскільки клієнти більш охоче довіряють свої дані компаніям, сертифікованим за стандартом ISO 27001. Таким чином, компанії матимуть впевненість і конкурентну перевагу для залучення більшої кількості клієнтів і зростання. Ще одним фактором, про який варто згадати, є відповідність міжнародним нормам, таким як Загальний регламент про захист даних (GDPR), та дотримання вимог законодавства. Юридичні санкції за порушення конфіденційності інформації можуть призвести до тривалих судових баталій і величезних фінансових втрат.

Компанії, сертифіковані за стандартом ISO 27001, можуть уникнути будь-яких негативних наслідків витоку даних: їм необхідно створити систему реагування на інциденти інформаційної безпеки, засновану на положеннях ISO 27001. Це означає наявність системи, яка дозволяє повідомляти про загрози інформаційній безпеці та реагувати на них якомога раніше. Кібератаки можуть відбуватися щодня, і життєво важливо виявляти їх на ранній стадії. Наприклад, у випадку з витоком даних, компанії може знадобилося більше тижня, щоб дізнатися про атаку. Якби атака була виявлена раніше, масштаб витоку даних міг бути меншим і постраждала б менша кількість клієнтів. Система реагування на інциденти інформаційної безпеки могла б допомогти виявити та протидіяти атаці раніше.

Крім того, ISO-сертифіковані компанії регулярно аналізують першопричини таких атак та інцидентів за допомогою тестів, які виявляють вразливості системи до того, як відбудеться фактична атака. Виявляючи вразливості до фактичної атаки, компанії отримують цінний час для підготовки до сценаріїв витоку даних. Нарешті, компанії, сертифіковані за стандартом ISO 27001, повинні мати план аварійного відновлення.

Він повинен спрацьовувати в разі виникнення надзвичайної ситуації, тобто якщо атака вже відбулася. Важливо мати план відновлення після атаки. Якщо

компанія зможе якнайшвидше продовжити нормальне функціонування, збитки, завдані атакою, будуть незначними. Кожен день, протягом якого компанія не працює, призводить до значних втрат для її доходів та операцій.

3.4 ISO 27001: Оцінка ризиків

В рамках інформаційної безпеки добре структуровані інвестиційні наміри в безпеку надають вищому керівництву багато умов для раціоналізації фінансування корпоративної інформаційної безпеки. Організації можуть враховувати як економічні, так і неекономічні наслідки своїх інвестиційних рішень. Фінансові умови, такі як рентабельність інвестицій (ROI), дозволяють оцінити економічну життєздатність менеджменту по відношенню до вартості активів, які захищає менеджмент, і вартості інвестицій. До неекономічних умов належать співпраця з клієнтами та зосередженість на організаційній та операційній життєздатності. В літературі з організації та управління також зазначається, що чітко визначені стратегічні інвестиційні цілі є важливим елементом процесу розвитку, що веде до організаційного прийняття та змін.

Ризик є ключовим словом, відповіддю на вищезазначені виклики, а управління ризиками визначає пріоритети; відповідно до ISO 27000:2013, СУІБ забезпечує конфіденційність, цілісність та доступність інформації через процес управління ризиками та надає зацікавленим сторонам Запевнення. Оцінка ризиків - це інструмент для аналізу та інтерпретації ризиків. Це означає визнання та оцінку вразливості організації. Це передбачає визначення обсягу та процедур оцінки, збір та аналіз даних, а також перегляд звітів з оцінки ризиків. Група з реалізації повинна зібрати та проаналізувати дані про ризики. Це вимагає визначення всіх активів, ризиків, вразливостей, засобів захисту та їх важливості, залишків і ймовірності успішної атаки [13].

Оцінка ризиків не обмежується існуючими проблемами, але також повинна враховувати майбутні проблеми, беручи до уваги нові системи і винаходи, які вже існують і будуть впроваджені в майбутньому. Проведення оцінки ризиків також призводить до поглиблення знань про організацію та її діяльність. Команди з оцінки ризиків прагнуть зрозуміти, як взаємодіють системи і процедури, щоб компанії могли виявити прогалини у своїх процесах. Важливо зазначити, що особа, яка очолює процес оцінки ризиків, повинна мати чітке, широке бачення та глибокі знання про компанію в цілому.

Управління ризиками є наступним кроком і полягає у виборі та впровадженні відповідних засобів контролю для зниження ризику до рівня, прийнятного для організації. Як і в інших аспектах ISO 27001, не існує прискорювачів або обов'язкових шаблонів, яких слід дотримуватися, коли справа доходить до оцінки ризиків. Команда з інформаційної безпеки може провести оцінку ризиків, яка має сенс для структури організації.

Оцінка ризиків, як описано в ISO 27001, встановлює та підтримує критерії ризиків інформаційної безпеки, дає послідовні, точні та відносні результати, працює з власниками ризиків для виявлення ризиків, а також аналізує та оцінює ці ризики. Оцінка ризиків включає наступні дії: виявлення активів, що піддаються ризику, та визначення їхнього статусу суттєвості за вартістю, конфіденційністю та важливістю; виявлення потенційних загроз; визначення ступеня ймовірності виникнення загроз для конкретних активів; визначення впливу (як правило, включаючи очікувані втрати, пошкодження та витрати на відновлення); зменшення ризиків шляхом впровадження відповідних заходів); зменшення ризиків шляхом включення управління ризиками до проектування активів; обмеження корпоративного контролю над бюджетами, включаючи впровадження нових політик і процедур.

3.5 ISO 31000: Управління ризиками

Стандарт управління ризиками ISO 31000 є одним із стандартів управління ризиками, набором міжнародних стандартів для застосування керівних принципів управління ризиками, опублікованих Міжнародною організацією зі стандартизації. Як і багато інших стандартів управління ISO, ISO 31000 встановлює структуровану систему, призначену для задоволення вимог компаній усіх розмірів і типів. Крім того, пропонується використовувати ISO 31000:2018 як відповідну структуру для вирішення проблеми невизначеності в оцінці ризиків у промисловій діяльності. Структура управління ризиками ISO 31000:2018 нещодавно була затверджена як дійсна основа для ретельного аналізу управління ризиками. Він представлений у вигляді Стандарт в основному використовується учасниками галузі, але є адаптованим і не є специфічним для галузі або сектора. Визначення ризику в ISO 31000:2018 відрізняється від інших визначень ризику, що використовуються в традиційній оцінці ризику, тим, що ризик визначається виключно з точки зору ймовірності поганих або небажаних наслідків. Він не фокусується на ймовірності поганого або небажаного результату, а скоріше на управлінні ризиком.

Відповідно до ISO 31000:2018, управління ризиками - це ітеративний процес, що включає такі етапи: визначення сфери, контексту та критеріїв; оцінка ризиків (включаючи ідентифікацію ризиків, аналіз ризиків та оцінку ризиків); обробка ризиків; збір даних та звітність; моніторинг та огляд; аналіз ризиків; оцінка ризиків; комунікація та консультування. ISO 31000 відрізняє структуру управління ризиками від двох інших компонентів системи управління ризиками організації: принципів управління ризиками та процесів управління ризиками. Архітектура управління ризиками складається з цих трьох компонентів. Система управління ризиками - це сукупність компонентів, які слугують основою та організаційною структурою для розробки, впровадження, моніторингу, аналізу та

постійного вдосконалення управління ризиками в масштабах підприємства. Деякі системи управління ризиками, такі як ISO 31000, є стандартами управління ризиками. також відомі як стандарти. Організації часто використовують ці два позначення як взаємозамінні.

Ризик-менеджмент - це процес, спрямований на управління ризиками, тобто інформування, консультування, визначення контексту, ідентифікацію, оцінку, аналіз, обробку, моніторинг і перегляд ризиків [14].

ISO 31000 встановлює основні принципи, структуру та методи. Він не призначений для створення однаковості в системах управління ризиками, а для визначення процесу управління ризиками в будь-якому бізнесі, включаючи безпеку. Він надає організаціям стандарти управління ризиками, які можуть бути використані для встановлення та досягнення цілей, незалежно від розміру або типу бізнесу. Концепція, структура і процеси застосовні до органів державної влади, приватних компаній, груп, асоціацій і підприємств усіх типів. Вона також встановлює єдиний підхід до управління ризиками, незалежно від галузі чи сектору. За допомогою підходу до управління ризиками можна управляти всіма типами ризиків. Підхід до управління ризиками застосовується протягом усього життя організації і до всіх видів діяльності, включаючи прийняття рішень на всіх рівнях.

Зменшення ризиків, прогнозування ризиків та управління ризиками є елементами управління організацією, в бізнес-плані якої управління ризиками є невід'ємною частиною. Тому компанії часто звертаються до ISO 31000 за допомогою у виконанні цього завдання; ISO 31000 можна використовувати для управління процесами, операціями, проектами, програмами, товарами, послугами та активами, а також для прийняття стратегічних рішень на організаційному рівні.

3.6 Приклад компанії до впровадження ISO

Організація мала політику захисту інформації, яку вона обробляє, як в електронному, так і в паперовому вигляді, щоб захистити її від наслідків порушення конфіденційності, нездатності підтримувати цілісність інформації або припинення доступу до неї. У компанії вже існувала низка процесів. Однак багато з них документувалися нерегулярно або взагалі не документувалися. Це означало, що багато загроз не розпізнавалися, а отже, не усувалися. Було організовано щорічні та початкові тренінги з інформаційної безпеки, а співробітників було ознайомлено з політикою інформаційної безпеки компанії. Було створено групу з інформаційної безпеки. Її члени пройшли навчання, і всі співробітники змогли піднімати питання інформаційної безпеки. Втім, компанія вже має деякі налагоджені процеси, що сприяють дотриманню вимог стандарту ISO 27001. Однак багато загроз і вразливостей не було виявлено [15].

Швидке зростання компанії підказало, що стандартизована модель інформаційної безпеки зробить певні бізнес-аспекти більш функціональними. Швидке зростання також дало зрозуміти, що компанія стала мішенню для кіберзагроз. Як наслідок, компанія поставила собі за мету дотримуватися більш детальної та вдосконаленої політики інформаційної безпеки. Традиційний підхід до захисту інформації не підходив для компанії, що швидко зростає. Зі збільшенням штату компанії ризик людських помилок зростав в геометричній прогресії.

3.7 Метод аналізу ризиків

Для підтримки організації у створенні СУІБ була розроблена стратегічна основа. Рисунок 3.1 ілюструє процес, який має використовувати компанія, організація для впровадження та оцінки своєї СУІБ. На першому етапі компанія

встановила правила безпеки та пов'язані з ними заходи і засоби контролю. Потім вона розробила заяву про сферу застосування, в якій пояснила, чому дозволи є пріоритетними над іншими. Вона також визначила активи та дебіторську заборгованість, оцінила ризики та обрала методи оцінки [16].

На другому етапі було впроваджено політику і процедури безпеки, створено засоби контролю і організовано управління операціями.

На третьому етапі оцінювали та вимірювали ефективність діяльності, а результати доповідали керівництву.

На завершальному етапі компанії вживали відповідних превентивних, прогнозних та коригувальних заходів для підтримки та вдосконалення своїх СУІБ.

Рисунок 3.1 – Процес впровадження СУІБ

Ризик - це негативний вплив вразливостей або загроз, які можуть виникнути на інформаційні системи та активи Організації. Управління ризиками - це систематичне виявлення, оцінка та реалізація кроків і дій, спрямованих на зниження ризиків до прийнятного рівня. У наступних параграфах описано та проаналізовано методи оцінки та обробки інформаційних ризиків для визначення належного рівня ризику згідно з відповідним стандартом безпеки (ISO/IEC

27001:2013), а також надано рекомендації щодо розробки ефективної програми управління ризиками в інфраструктурі організації. [18].

Оцінка ризиків, обробка ризиків та допоміжні засоби контролю і процеси впроваджуються на всіх об'єктах організації і стосуються інформаційних та операційних ризиків усіх активів, що використовуються всередині компанії, які потенційно можуть вплинути на інформаційну безпеку організації. Засоби контролю і процеси застосовуються до всіх оцінок ризиків інформаційної безпеки, що проводяться в рамках СУІБ організації, і охоплюють всі бізнес-процеси і активи організації. Політика оцінки та управління ризиками застосовується до всіх організацій (наприклад, до співробітників, партнерів, підрядників, місцевих партнерів з доставки, постачальників і широкої громадськості).

Управління ризиками - це процес в рамках СУІБ організації, метою якого є сприяння систематичному виявленню, оцінці та управлінню ризиками, а також забезпечення прийнятного рівня інформаційної безпеки в рамках СУІБ. Цілями оцінки та управління ризиками в контексті інформаційної безпеки є чіткий розподіл обов'язків, розробка послідовної методології виявлення ризиків, ідентифікація ризиків, чітке формулювання ризиків та їх оцінок, впровадження кращих засобів контролю безпеки в інформаційних системах організації, а також розробка рішень для оцінки ризиків [19].

В результаті організація створить технічну основу оцінюваної інформаційної системи та забезпечила, щоб бізнес-цілі охоплювали всі внутрішні та зовнішні аспекти, що контролюють виявлені ризики. Також повинно бути враховано ідентифікацію власників інформаційної системи організації, включаючи класифікацію інформації, допоміжні бізнес-процеси, користувачів системи, вимоги до безпеки та відповідності. З технічного боку, організація була визначена як власник послуг інформаційної системи, а також були розглянуті

можливості підтримки та обслуговування інформаційної системи користувачами організації, логічна архітектура та компоненти системи.

Оцінка ризиків враховувала критичність інформаційних систем і активів організації. Якщо інформація була критично важливою для організація або актив був визначений як високо ризикований, для відповідного інформаційного активу проводилася комплексна оцінка ризиків. Це включало в себе поглиблену документацію та перевірку активів, а також оцінку впливу вразливостей і ризиків для цих активів на бізнес.

Оцінка ризиків дозволила виявити, кількісно оцінити та визначити пріоритетність ризиків відповідно до цілей організації, а також встановити критерії прийнятного рівня ризиків. Результати оцінки ризиків допомога керівництву організації у виборі та визначенні пріоритетності відповідних заходів з управління ризиками інформаційної безпеки та впровадженні відповідних засобів контролю для захисту від цих ризиків.

Процедура оцінки ризиків включала метод систематичної оцінки ступеня ризику (аналіз ризику) та визначення значущості ризику шляхом порівняння ризику з умовами ризику (оцінка ризику). Оцінки ризиків проводилися час від часу у відповідь на зміни в припущеннях щодо безпеки та умов ризику (наприклад, активів, загроз, вразливостей, впливів та інших суттєвих змін). Вони проводяться систематично і можуть давати подібні та повторювані результати кілька разів, залежно від ролі та важливості.

Оцінка ризиків повинна проводитися з урахуванням доступу до бізнес-процесів організації та розуміння бізнес-процесів, ризику впливу на активи організації, технологічних систем, що підтримують потреби, законів та нормативних актів, яким повинна відповідати організація, а також поточної оцінки вразливості та загроз. Оцінку ризиків слід проводити для кожної нової системи обробки інформації, принаймні після введення нових інформаційних активів і після змін у системі або процесі. Якщо оцінка не проводилася протягом

відносно тривалого періоду часу (наприклад, три роки), можуть знадобитися зміни, які змінять характер загроз і вразливостей.

Для кожного ризику, виявленого в ході оцінки ризиків, керівництво організація повинно було визначити відповідні методи управління ризиками. Серед можливих способів реагування на ризики - впровадження відповідних засобів контролю для зменшення ризику, прийняття ризикових умов і стандартів, уникнення ризику шляхом уникнення поведінки, яка може створити ризик, а також передача відповідного ризику іншим підрозділам компанії (наприклад, страховим компаніям або постачальникам) [20].

Ідентифікація ризику за допомогою відповідних засобів контролю означає вибір і впровадження засобів контролю відповідно до вимог, що випливають з оцінки ризику. Вибрані засоби контролю впроваджують і використовують засоби контролю, пов'язані зі зниженими та залишковими ризиками, відповідно до національних і міжнародних законів і політик, договірних зобов'язань із замовниками та постачальниками, вимог і цілей компанії організація, потреб і нормативних актів та інших умов і обмежень, умов і обмежень компанії, витрат компанії, важливості збалансування інвестицій, вкладених у впровадження і функціонування засобів контролю, з втратами і необхідністю забезпечення мінімізації ризиків.

Першим кроком процесу оцінки ризиків СУІБ (вплив активів на конфіденційність, цілісність та доступність організаційної інформації) була ідентифікація всіх активів із золотою зіркою. Активи включають документи, програми та бази даних у фізичній або електронній формі, ІТ-обладнання, інфраструктуру, людей, зовнішні та аутсорсингові послуги. Ідентифікація активів також включає визначення власника (відповідальної особи або організаційного підрозділу) кожного активу. Визначення вразливостей та загроз кожного активу є наступним кроком у методології оцінки ризиків. Кожен актив може мати низку вразливостей і загроз.

3.8 Результати аналізу та оцінки ризиків

Організація в результаті починає враховувати всі потенційні вразливості та ризики, пов'язані з конкретною системою, незалежно від того, чи є вони внутрішніми чи зовнішніми, природними чи створеними людиною, випадковими чи навмисними. Інформація про вразливості та загрози була отримана від відповідних робітників організації і, в деяких випадках, від професійних консультантів з безпеки, місцевих і національних правоохоронних органів, охоронних організацій та контактів. У Таблиці 3.1 перераховані категорії загроз, які могли бути виявлені.

Табляця 3.1

Категорії загроз, визначені для організацій

Викрадення	Викрадення, Вандалізм
Помилка ПЗ	Помилка ПЗ, віруси, шкідливі програми, несанкціонований доступ, Помилки при обслуговуванні
Відключення	Відключення електроенергії, зв'язку
Помилка мережі	Атака на мережу
Природний лихо	Землетрус, Повінь, Пожежа
Юридичний	Порушення договірних зв'язків, Порушення законодавства
Помилка людини	Зловживання інформацією, Помилка оператора, Зловживання привілегіями користувача, Знищення записів, Несанкціоноване встановлення програмного забезпечення

продовження табл.3.1

Помилка обладнання	Несправність обладнання, Пошкодження кабелів, Заблокований доступ
Зовнішні носії	Використання неперевірених зовнішніх носіїв

Ризики для інформаційних систем, інформації та операцій організації можуть бути ідентифіковані в наступних категоріях. Якщо ви є робітником організація, ви можете ідентифікувати загрози, пов'язані з активами, що розглядаються. Вичерпний перелік подій, які можуть перешкодити або затримати досягнення цілей організація, задокументовано. Ризики, не включені до цього переліку, можливо, не були оцінені та зменшені. Загрози з існуючих сховищ можуть бути додані після відповідних розслідувань. Для цілей аналізу та оцінки було надано чітке визначення ризиків. Нарешті, до визначення ризиків включено потенційний вплив на інформаційні системи та активи організації. Ризики, які потенційно можуть вплинути на конфіденційність, цілісність і доступність інформаційних систем, інформації, операцій і активів організації, документуються в процесі оцінки ризиків. Критерії оцінки ризиків були розроблені для досягнення загального розуміння тих заходів безпеки, які зменшують потенційний вплив до прийнятного рівня. Критерії впливу визначають рівень шкоди та витрат, спричинених загрозами. У Таблиці 3.2. представлені визначені критерії впливу.

Таблиця 3.2

Критерії впливу

Втрата фінансової цінності	Вплив на відповідні процедури

продовження табл.3.2

Прямий фінансовий вплив	Інциденти безпеки, атаки
Непрямі, довгострокові фінансові наслідки	Порушення законодавчих та регуляторних вимог
Порушення планів і термінів	Проблеми з приватними контрактами
Втручання в корпоративні процедури	Проблеми з недоторканністю приватного життя
Втрата вартості бізнесу	Питання конкуренції
Втрата можливостей	Конфіденційна інформація, персональні дані, шкода репутації
Збої в комерційній діяльності	Проблеми соціальної конфіденційності

Було проведено аналіз для визначення виявлених вразливостей і засобів контролю безпеки, а також ймовірності майбутніх подій і ризиків, які можуть завдати шкоди інформаційним системам і активам організації. Вплив втрати конфіденційності, цілісності та доступності оцінювався за допомогою критеріїв впливу. Ймовірність виникнення була фактором ризику, заснованим на аналізі ймовірності того, що конкретна загроза скористається певною (або набором) вразливостей. Ризик є наслідком ймовірності (вірогідності) того, що певна загроза стане результатом потенційної вразливості та її впливу на інформаційні системи та активи організації. Діяльність з оцінки ризиків надає інформацію, необхідну для розробки відповідних засобів контролю безпеки та заходів для зменшення або усунення ризиків у процесі зменшення ризиків (обробка ризиків).

Етапи, що ведуть до проведення оцінки ризиків, включають такі види діяльності: виявлення загроз, виявлення вразливостей, аналіз засобів контролю, визначення ймовірностей, аналіз впливу, визначення ризиків, рекомендації щодо засобів контролю та документування результатів. Першим кроком є оцінка

ймовірності виникнення потенційних загроз. Ймовірність виникнення загрози (рівень загрози) визначається як ймовірність настання події. Визначаючи ймовірність виникнення загрози, компанія має врахувати причину загрози, можливу вразливість та існуючі засоби контролю. Другий етап включав аналіз загроз для інформаційної системи та аналіз вразливостей, пов'язаних з навколишнім середовищем організації, тобто оцінку рівня вразливості відповідно до сценарію загрози. Впроваджені засоби контролю організації були протестовані. Згодом засоби контролю, впроваджені організації, були переглянуті, щоб спробувати мінімізувати або усунути ймовірність і вірогідність загроз, які можуть виникнути в результаті вразливостей системи. На четвертому етапі організації має врахувати такі ключові фактори: джерело (природу) загрози, наявність та ефективність існуючих засобів контролю. Ймовірність реалізації загрози була вхідним параметром, а рівень загрози та рівень чутливості були вихідними параметрами ймовірності реалізації конкретної загрози. П'ятий вид діяльності характеризував вплив інцидентів безпеки з точки зору втрати конфіденційності, цілісності та доступності. Потім значення ймовірності події та впливу були об'єднані для оцінки рівня ризику кожного активу для виявлених загроз. Адекватність запланованих та існуючих заходів безпеки організації також була включена в оцінку ризиків. На сьомому етапі заходи безпеки, які могли б зменшити або усунути виявлені ризики, були узгоджені з операціями організації. Запропоновані заходи контролю забезпечили утримання рівня ризику на керованому рівні. Нарешті, після завершення оцінки ризиків, результати були задокументовані в офіційному звіті. Рівні ризиків оцінювалися відповідно до визначених критеріїв, і були вжиті відповідні заходи. На рисунку 3.2 показано блок-схему етапів процесу оцінки ризиків.

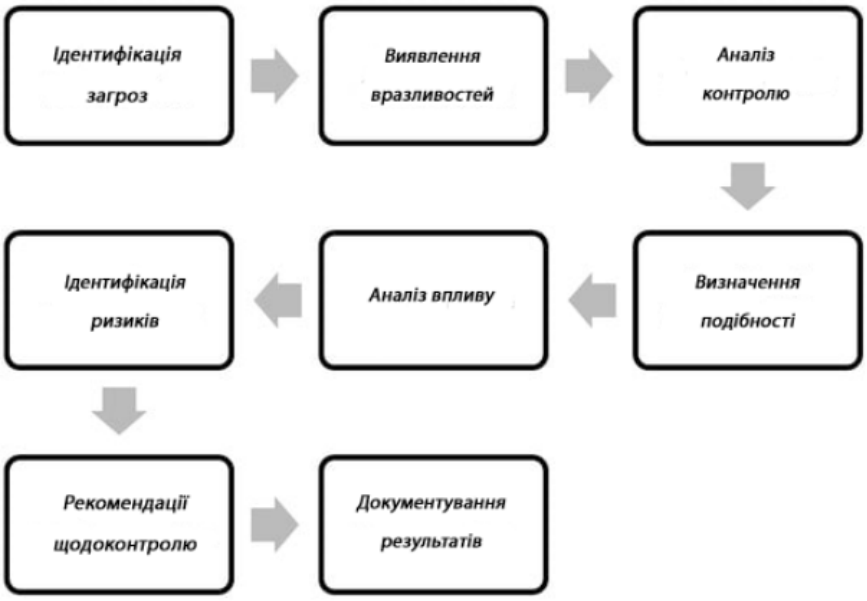

Рисунок 3.2 – Блок-схема кроків, які виконуються в процесі аналізу ризиків.

Що стосується ризиків, то для кожної вразливості та загрози необхідно було оцінити пов'язані з ними наслідки для кожного активу окремо. Ймовірність реалізації цих ризиків слід оцінювати для кожного активу. Серйозність ризику - це загальна оцінка як ймовірності реалізації ризику (ймовірність), так і наслідків, якщо це станеться (вплив). Потенційні вразливості та/або загрози визначаються як (майже певні, ймовірні, можливі, можливі, малоймовірні, рідкісні). Вплив інциденту безпеки визначається з точки зору втрати конфіденційності, цілісності та доступності. Вимірювання впливу і рівні ризику - на NIST SP 800-30; рівні ймовірності та частоти наведені в Таблиці 3.3, а рівні впливу - в Таблиці 3.4.

Табляця 3.3

Рівень вірогідності та частоти

Рівень вірогідності	Опис вірогідності
Майже ймовірно	що відбудеться с великим шансом

продовження табл. 3.3

Ймовірно	відбудеться в більшості випадків
Можливо	Може статися впевний момент часу
Малоймовірно	Можливо не відбудется
Рідко	трапляється лише за певних обставин

Табляця 3.4

Рівень впливу

Рівень впливу	Опис впливу
Максимальний (H5, H4, H3, H2, H1)	Втрата доступності, конфіденційності або цілісності має значний, критичний та/або негайний вплив на грошові потоки, операційну діяльність, функціональність, юридичні та договірні зобов'язання та/або репутацію компанії.
Середній (M5, M4, M3, M2, M1)	Втрата конфіденційності, доступності або цілісності може призвести до витрат і мати помірний або незначний вплив на юридичні та договірні зобов'язання та/або репутацію.
Низький (L5, L4, L3, L2, L1)	Втрата конфіденційності, доступності або цілісності не вплине на грошові потоки компанії, юридичні або договірні зобов'язання та/або репутацію.

Організація розробила шкалу ризиків і матрицю рівнів ризиків для вимірювання сприйнятого ризику. Остаточний показник ризику отримують шляхом перемноження оцінок ймовірності загрози та впливу загрози. Точний

рейтинг ризику може бути визначений на основі введених груп ймовірності загрози та впливу загрози.

Матриця рівня ризику (Таблиця 3.5) - це матриця 5 х 15 ймовірності загрози (майже певна, ймовірна, вірогідна, можлива, малоймовірна, малоймовірна, рідкісна) та впливу загрози (високий 1-5, середній 1-5, низький 1-5), яка показує, як визначається загальний рівень ризику. Визначення цих рівнів ризику або рейтингів може бути суб'єктивним. Основою для цього опису можуть слугувати ймовірність, присвоєна кожному рівню ймовірності загрози, і значення, присвоєне кожному рівню впливу. Кожному об'єкту приписуються всі можливі загрози.

Табляця 3.5

Матриця рівнів ризику

		Рідко	Малоймовірно	Можливо	Ймовірне	Майже певно
Вплив	Значення	0.20	0.40	0.60	0.80	1.00
H5	15	3	6	9	12	15
H4	14	2.8	5.6	8.4	11.2	14
H3	13	2.6	5.2	7.8	10.4	13
H2	12	2.4	4.8	7.2	9.6	12
H1	11	2.2	4.4	6.6	8.8	11
M5	10	2	4	6	8	10
M4	9	1.8	3.6	5.4	7.2	9
M3	8	1.6	3.2	4.8	6.4	8
M2	7	1.4	2.8	4.2	5.6	7
M1	6	1.2	2.4	3.6	4.8	6
L5	5	1	2	3	4	5

продовження табл. 3.5

L4	4	0.8	1.6	2.4	3.2	4
L3	3	0.6	1.2	1.8	2.4	3
L2	2	0.4	0.8	1.2	1.6	2
L1	1	0.2	0.4	0.6	0.8	1

Шкала оцінювання рівня впливу (з точки зору конфіденційності, цілісності та доступності) має 15 рівнів від L1 до H5: L1, L2, L3, L4, L5, M1, M2, M3, M4, M5, H1, H2, H3, H4, H5. Ці критерії базуються на ISO 27005. Шкала для оцінки рівня ймовірності встановлена за п'ятибальною шкалою: 0,20 - рідко, 0,40 - малоймовірно, 0,60 - можливо, 0,80 - ймовірно і 1,00 - майже певно. Межа ризику була встановлена на рівні 2,9.

Матриця рівнів ризиків наведена в Таблиці 3.5 Матриця рівнів ризику та рейтинги відображають рівень ризику, на який можуть наражатися інформаційні системи, активи та/або процеси організації за наявності відомих вразливостей та загроз. У Таблиці 3.6 наведено результати, а в Таблиці 3.7 - рівні результатів.

Табляця 3.6

Ймовірність-наслідки

Рейтинг ймовірності	Незначний	Серйозно	Сильний	Значний	Катастраф.
Практично впевнений	Середній	Високий	Критичний	Критичний	Критичний
Ймовірний	Середній	Значний	Високий	Критичний	Критичний
Можливий	Середній	Середній	Значний	Високий	Критичний
Малоймовірний	Низький	Низький	Середній	Значний	Критичний
Рідкісний	Низький	Низький	Середній	Середній	Високий

Табляця 3.7

Рівень результату

Рівень результату	Опис
Критичний	вимагає детального дослідження та планування
Високий	потребує негайної уваги
Суттєвий	потребує уваги керівництва
Середній	необхідно визначити відповідальність керівництва за управління
Низький	ризик незначний, необхідно виконувати регулярні процедури управління

3.9 План управління ризиками

Для кожного виявленого ризику має бути визначена план реакції на неї. Ймовірність і вплив ризику формують основу для рекомендацій щодо того, яких заходів слід вжити для зменшення ризику. Варіанти управління (контроль безпеки) повинні бути визначені на основі аналізу витрат і вигоди та відповідних критеріїв впливу. Обробка ризиків організації складається з чотирьох рівнів: прийняття, зменшення, передача та усунення. На першому рівні прийняття ризику здійснюється для низько пріоритетних ризиків, коли інші варіанти лікування коштують більше, ніж потенційний вплив. Для зменшення ідентифікованих ризиків, всі ризики повинні включати рекомендації щодо контролю та альтернативних рішень. На другому рівні зниження ризиків передбачає мінімізацію ймовірності або впливу загрози і вразливості ризику. Превентивні заходи проти ризиків завжди більш ефективні, ніж компенсація збитків, спричинених виявленими ризиками. Організація планує та розробляє майбутні заходи контролю для подолання виявлених ризиків. На третьому рівні

передача ризиків передбачає передачу негативних наслідків загроз і вразливостей. Передача ризиків третій стороні (постачальнику) не усуває загрозу або вразливість. Інша сторона все ще несе відповідальність за відповідні ризики. Компанія повинна перерахувати всі варіанти передачі ідентифікованих ризиків іншій організації (наприклад, страхування). На останньому рівні уникнення ризиків передбачає зміну аспектів загального бізнес-процесу або архітектури системи для усунення загрози, тобто уникнення ризику шляхом припинення відповідної бізнес-активності.

Для зменшення виявлених ризиків та мінімізації потенційного впливу на інформаційні системи організації були обрані відповідні цілі контролю. Для того, щоб не залишитися поза увагою, засоби контролю безпеки були обрані та розроблені відповідно до правил, наведених у ISO 27001:2013. Правила, обрані для відповідних загроз, повинні бути задокументовані.

Розроблено план обробки ризиків для управління та пом'якшення необхідних відновлювальних заходів. Плани обробки ризиків були розроблені для зменшення ризиків для критично важливих активів організації. Потенційні ризики, що виникають внаслідок виявлених вразливостей та загроз, були оцінені відповідно до рівня наслідків.

Висновки до розділу 3

У розділі проаналізовано, що при впровадженні стандарту ISO 27001 мета полягає в тому, щоб забезпечити аналіз ризиків інформаційної безпеки, усунення загроз і вразливостей, а також повне і послідовне документування та оновлення всіх даних.

Однією з найбільш важливих і трудомістких частин створення СУІБ в компанії є оцінка ризиків. Всі можливі ризики повинні бути ідентифіковані, оцінені та класифіковані. Існує багато інших ризиків для компанії, але бажаний

результат полягає в тому, щоб знайти найкраще рішення, яке забезпечить інформаційну безпеку та відповідатиме потребам компанії.

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто важливі аспекти аналізу ризиків в системі управління інформаційною безпекою (СУІБ) організації. Кожен метод аналізу ризиків має свої переваги та недоліки, і вибір методу залежить від потреб та ресурсів організації.

У першій частині кваліфікаційної роботи було проведено аналіз ризиків в системах управління інформаційною безпекою (СУІБ). Під час аналізу виявлено та оцінено потенційні загрози для інформаційних активів. Головною метою ефективного аналізу ризиків було з'ясувати, що може загрожувати конфіденційності, цілісності та доступності інформації.

У другій частині кваліфікаційної роботи було розглянуто різні методи аналізу ризиків, які використовуються для створення ефективної системи управління інформаційною безпекою (СУІБ) в організаціях. Проведений огляд та порівняльний аналіз цих методів дозволив виявити їх переваги, недоліки та сферу застосування.

У третій частині кваліфікаційної роботи скомбіновано метод аналізу ризиків в системах управління інформаційною безпекою. Визначено роль Системи управління інформаційною безпекою та стандарту ISO 27001 у впровадженні таких систем. Підкреслено переваги систем управління інформаційною безпекою і їх важливість для організацій. Розглянуто процес оцінки ризиків згідно зі стандартом ISO 27001 та принципи управління ризиками згідно зі стандартом ISO 31000. Представлено метод аналізу ризиків та результати аналізу і оцінки ризиків. Загальною висновком до цього розділу є підкреслення значення інтеграції систем управління інформаційною безпекою та ефективного аналізу ризиків для забезпечення безпеки та захисту інформації в організаціях.

Виходячи із поставленої мети кваліфікаційної роботи були виконані наступні завдання:

- Провести аналіз ризиків інформаційної безпеки
- Дослідити методи аналізу ризиків інформаційної безпеки
- Запропонувати метод аналізу ризиків в системах управління інформаційною безпекою

Всі задачі було виконано в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000:2018 "Information technology - Security techniques - Information security management systems - Overview and vocabulary", стор. 5-10.

2. NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations", стор. 3-5.

3. Безпека інформації. Терміни та визначення. Державний стандарт України ДСТУ ISO/IEC 27000:2015, стор. 4-7.

4. Інформаційна безпека. Системи управління інформаційною безпекою. Вимоги. Державний стандарт України ДСТУ ISO/IEC 27001:2015, стор. 7-10.

5. Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security (6th ed.). Boston, MA: Cengage Learning. стор. 278-300.

6. Rainer, R. K., Prince, B., & Cegielski, C. (2018). Introduction to Information Systems: Supporting and Transforming Business (7th ed.). Hoboken, NJ: Wiley. стор. 387-410.

7. National Institute of Standards and Technology (NIST). (2017). NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments. стор. 5-20.

8. ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA. стор. 67-85.

9. ENISA. (2018). ENISA Threat Landscape Report. стор. 10-25.

10. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York, NY: W. W. Norton & Company. Стор. 102-125.

11. Information Systems Audit and Control Association (ISACA). (2019). CISM Review Manual (15th ed.). Rolling Meadows, IL: ISACA. стор. 258-280.

12. Dhillon, G. (2008). Principles of Information Systems Security: Texts and Cases. Hoboken, NJ: John Wiley & Sons. стор.150-155

13. Sherwood, J., Clark, A., & Lynas, D. (2005). The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk. Boca Raton, FL: CRC Press. стор 220-225

14. Fennelly, L. J., & Grance, T. (2013). Guide to Computer Forensics and Investigations. Boston, MA: Cengage Learning. стор 260-265

15. Kresnawan A., Wahyudi A., Wahyuni D. (2017). Risk Analysis Method in Information Security Management System // Proceedings of the 2nd International Conference on Informatics and Computing (ICIC). стор 1-5

16. Dandurand A., Karygiannis T., Scarfone K. (2012) Risk Management Guide for Information Technology Systems // National Institute of Standards and Technology (NIST) Special Publication 800-30. стор 34-40

17. Alsharnouby M., Sandhu R., Sattar A. A (2013) Comparative Study of Risk Analysis Techniques in Information Security // Proceedings of the 6th International Conference on Security of Information and Networks (SIN). стор.254-261.

18. Woon L. Y., Ong H. C. (2016)Risk Analysis Method for Information Security Management System // Proceedings of the 2016 International Conference on Data and Software Engineering (ICoDSE). стор 1-5.

19. Khan M., Khan S., Zaki Y. (2018) A Review of Risk Analysis Methods for Information Security // International Journal of Computer Science and Security (IJCSS). стор. 13-21.

20. Шерстюк А. О., Гавриленко О. Ю., Бардась О. В. Метод аналізу ризиків в системах управління інформаційною безпекою // Вісник Національного університету «Львівська політехніка». Серія: Комп'ютерні науки та інформаційні технології. – 2019. стор 28-37.