МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ
ІНСТИТУТ ім. Ю. М. ПОТЕБНІ
Кафедра інформаційної економіки, підприємництва та фінансів
(повна назва кафедри)

Кваліфікаційна робота(проект)

магістра
(рівень вищої освіти)

на тему Удосконалення механізму моніторингу загроз інформаційної безпеки промислового підприємства

Виконав: студент 2 курсу, групи 8.0510-ie
спеціальності 051 Економіка
(код і назва спеціальності)
спеціалізації
_____
(код і назва спеціалізації)
освітньої програми Інформаційна економіка
(назва освітньої програми)
П. М. Рожко
(ініціали та прізвище)
Керівник доц., к.е.н., доц. Комазов П.В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Інженерний навчально-науковий інститут ім. Ю. М. Потебні
Кафедра інформаційної економіки, підприємництва та фінансів
Рівень вищої освіти магістр
Спеціальність 051 Економіка
(код та назва)
Спеціалізація
_____
(код та назва)
Освітня програма Інформаційна економіка

ЗАТВЕРДЖУЮ
Завідувач кафедри_____
«_____»_____20____року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)СТУДЕНТОВІ (СТУДЕНТЦІ)

Рожко Павло Миколайович
(прізвище, ім'я, по батькові)

1. Тема роботи (проекту) Удосконалення механізму моніторингу загроз інформаційної безпеки промислового підприємства

керівник роботи Комазов П. В., к.е.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від «____»_____20___року
№_____

2. Строк подання студентом роботи _____
3. Вихідні дані до роботи показники інформаційної безпеки ТОВ «Южмаш груп»

Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Методологічні аспекти моніторингу загроз інформаційної безпеки підприємства. 2. Моніторинг інформаційної безпеки промислового підприємства. 3. Практична реалізація системи моніторингу інформаційної безпеки.

Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Класифікація по джерелу загроз інформаційної безпеки. Процес ризик-менеджменту інформаційної безпеки. Деталізований процес оцінки ризику ІБ. Процес моніторингу ризику ІБ промислового підприємства.

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В.		
2	доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В.		
3	доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В.		

6. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Приміпка
1	Призначення наукових керівників. Затвердження тем дипломних робіт		
2	Напрацювання теоретичного матеріалу: дослідження сутності об'єкту та предмету дослідження, критичний аналіз існуючих методологічних засад, вибір та обгрунтування напрямку проведення дослідження		
3	Апробація результатів на Міжнародних та Всеукраїнських конференціях		
4	Розробка економіко-математичного забезпечення основних елементів концептуального підходу		
5	Збір та систематизація статистичного та нормативного матеріалу дослідження.		
6	Узагальнення отриманих результатів. Оформлення роботи		
7	Надання роботи та автореферату до рецензії. Нормоконтроль		
8	Прилюдний захист дипломної роботи на засіданні ЕК		

Студент _____ П. М. Рожко
(підпис) (ініціали та прізвище)

Керівник роботи (проєкту) _____ П. В. Комазов
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено

Нормоконтролер _____ _____
(підпис) (ініціали та прізвище)

АНОТАЦІЯ

Рожко. П. М. Удосконалення механізму моніторингу загроз інформаційної безпеки промислового підприємства.

Кваліфікаційна випускна робота для здобуття ступеня вищої освіти магістра за спеціальністю 051 – Економіка, науковий керівник П. В. Комазов. Інженерний навчально-науковий інститут ім. Ю. М. Потебні ЗНУ, кафедра інформаційної економіки, підприємництва та фінансів, 2021.

Магістерська робота присвячена розробці типових рішень моніторингу інформаційної безпеки промислових підприємств.

В дослідженні проаналізовано існуючі підходи до моніторингу загроз інформаційної безпеки підприємства. Розроблено концептуальну схему моніторингу стану інформаційної безпеки на підприємстві. Розроблено типове рішення моніторингу стану інформаційної безпеки промислового підприємства. Розроблено рекомендації щодо створення типових рішень організації систем управління станом інформаційної безпеки веб-ресурсу промислового підприємства.

Ключові слова: МОНІТОРИНГ, ЗАГРОЗА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА СИСТЕМА, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЮВАННЯ.

ABSTRACT

Rozhko P. M. Improvement of the mechanism of monitoring of threats of information security of the industrial enterprise.

Qualification final work for obtaining a master's degree in specialty 051 - Economics, supervisor P. V. Komazov. Engineering Educational and Scientific Institute named after Y M Potebny of ZNU, Department of Information Economics, Entrepreneurship and Finance, 2021.

The master's thesis is devoted to the development of standard solutions for monitoring the information security of industrial enterprises in the market of B2B services.

The study analyzes the existing approaches to monitoring threats to information security of the enterprise. A conceptual scheme for monitoring the state of information security at the enterprise has been developed. A standard solution for monitoring the state of information security of an industrial enterprise has been developed. Recommendations for the creation of standard solutions for the organization of information security management systems of industrial enterprises have been developed.

Keywords: MONITORING, THREAT, INFORMATION SECURITY, INFORMATION, INFORMATION SYSTEM, INFORMATION PROTECTION SYSTEM, SIMULATION.

АННОТАЦИЯ

Рожко. П. М. Усовершенствование механизма мониторинга угроз информационной безопасности промышленного предприятия.

Квалификационная выпускная работа по получению степени высшего образования магистра по специальности 051 – Экономика, научный руководитель П. В. Комазов. Инженерный учебно-научный институт им. Ю. М. Потебни ЗНУ, кафедра информационной экономики, предпринимательства и финансов, 2021.

Магистерская работа посвящена разработке типовых решений по мониторингу информационной безопасности промышленных предприятий. В исследовании проанализированы существующие подходы к мониторингу угроз информационной безопасности предприятия. Разработана концептуальная схема мониторинга состояния информационной безопасности на предприятии. Разработано типовое решение мониторинга состояния информационной безопасности промышленного предприятия. Разработаны рекомендации по созданию типовых решений организации систем управления состоянием информационной безопасности веб-ресурса промышленного предприятия.

Ключевые слова: МОНИТОРИНГ, УГРОЗА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИЯ, ИНФОРМАЦИОННАЯ СИСТЕМА, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, МОДЕЛИРОВАНИЕ.

ЗМІСТ

ВСТУП…… 7
РОЗДІЛ 1 МЕТОДОЛОГІЧНІ АСПЕКТИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА…….. 10
1.1. Методологія управління інформаційною безпекою підприємства…… 10
1.2. Сучасні підходи до класифікації загроз інформаційній безпеці…….. 13
1.3. Висновки до розділу 1…… 23
РОЗДІЛ 2 МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА…….. 24
2.1. Встановлення контексту забезпечення інформаційної безпеки…… 24
2.2. Оцінювання ризику інформаційної безпеки…….. 32
2.3. Висновки до розділу 2……. 60
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……. 61
3.1. Встановлення значення ризику інформаційної безпеки .. 61
3.2. Встановлення значень рівня ризиків інформаційної безпеки…….. 66
3.3. Висновки до розділу 3…… 91
ВИСНОВКИ…….. 92
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……. 93

ВСТУП

Інформаційне середовище є системоутворюючою ланкою в природному функціонуванні суспільних процесів. Вона забезпечує процеси споживання, зберігання і перетворення інформації. Інформаційна безпека відіграє ключову роль в ефективної та надійної роботи підприємства будь-якої сфери діяльності. Цей факт сприяє пильній увазі багатьох фахівців до проблематики інформаційної безпеки.

З урахуванням активного розвитку інформаційних технологій, появи інтернету речей (*IoT*) і наростаючого темпу зростання всесвітньої глобалізації для керівників підприємств відкривається новий ряд способів використання інформації для більш ефективної та раціональної оптимізації робочого або виробничого процесу. Ефективне використання інформації позитивно впливає не тільки на зовнішню комунікацію компанії, але і на внутрішню. Для оцінки об'єктивності прийняття тих чи інших рішень і підвищення показників продуктивності багато підприємств використовують у своїй роботі автоматизовані системи обробки інформації. Це дозволяє значно підвищити продуктивність процесів і заощадити тимчасові витрати, що, в кінцевому рахунку збільшує прибуток підприємства. Подібні системи мають велику кількість вразливостей і забезпечення безпеки в даному випадку стає питанням першорядної важливості. Варто зазначити, що з урахуванням збільшення кількості інформаційних потоків і різновидів їх використання, рівень загроз інформаційній безпеці значно зростає. Саме тому необхідно виявити весь перелік можливих порушень системи, які можуть становити небезпеку і виявити найбільш актуальні види загроз вже на етапі створення системи інформаційної безпеки.

Об’єкт дослідження: інформаційна безпека підприємства.

Предмет дослідження: методи моніторингу інформаційної безпеки підприємства.

Метою дослідження є розробка типових рішень моніторингу інформаційної безпеки промислових підприємств.

Для досягнення мети були поставлені та вирішені такі *завдання*:

1. Проаналізовано існуючі підходи до моніторингу загроз інформаційної безпеки підприємства.

2. Розроблено концептуальну схему моніторингу стану інформаційної безпеки на підприємстві.

3. Розроблено типове рішення моніторингу стану інформаційної безпеки промислового підприємства.

4. Розроблено рекомендації щодо створення типових рішень організації систем управління станом інформаційної безпеки веб-ресурсу промислового підприємства.

Методи дослідження. Для вивчення та узагальнення наукових розробок використані методи порівняння, аналізу і синтезу, індукції і дедукції, статистичні й експертні методи дослідження. Застосовані методи економіко-математичного моделювання (розробка моделей), абстрактно-логічний метод (теоретичні узагальнення та формулювання висновків), статистико-економічний (аналіз статистичних даних, вибіркове спостереження, групування), економічні методи дослідження.

Наукова новизна одержаних результатів полягає у наступному:

удосконалено:

− підходи до побудови системи моніторингу інформаційної безпеки підприємства яка дозволяє координувати та керувати системою інформаційного захисту на всіх етапах створення і функціонування системи управління інформаційною безпекою підприємства.

дістало подальшого розвитку:

− застосування системного підходу при побудові інформаційного захисту, який відтворений в концептуальній схемі системи моніторингу інформаційної безпеки на підприємстві.

Результати теоретичного аналізу проблеми інформаційного захисту висвітлено на Міжнародній науково-практичній конференції «Європейський вектор модернізації інженерної та економіко-управлінської освіти в умовах сталого розвитку промислового регіону» [16].

РОЗДІЛ 1
МЕТОДОЛОГІЧНІ АСПЕКТИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Методологія управління інформаційною безпекою підприємства

До основних стандартів, розроблених у західних країнах та широко застосовуваних у всьому світі, належать такі серії документів: *ITIL*, *ISO*, *COBIT* [2, 15, 27, 29, 33, 39].

Стандарт *ISO* відноситься до групи міжнародних документів, пов'язаних із універсальною стандартизацією аспектів людської діяльності. В тому числі ций стандарт регламентує питання підтримки та забезпечення інформаційної безпеки (*ISO* 27001, 2013 р.). *ISO* 27001 базується на моделі *Deming cycle* (взаємопов'язані елементи якої полягають у таких діях: планування, реалізація, аудит, виправлення) [39].

Загальні рекомендації стандарту такі [42]:

Перший етап.

Розробка політики управління *IT*-безпекою, що містить визначення «слабких місць» інформаційних систем, а також основних груп інформаційних ризиків (у тому числі ризиків фізичного знищення баз даних).

Другий етап.

Розробка програми вдосконалення та розвитку *IT*-систем на основі політики.

Третій етап.

Оптимізація / модернізація програмного забезпечення відповідно до політики та програми.

Четвертий етап.

Аудит (систематичний) інформаційних систем на предмет реалізації потенційних ризиків інформаційної безпеки.

П’ятий етап.

Постійне оновлення та актуалізація як документарної, і апаратної частини системи забезпечення інформаційної безпеки.

Основна перевага представленого стандарту ISO полягає в уніфікації принципів управління безпекою та загальною інфраструктурою інформаційних систем, однак, за рахунок цього знижуються адаптаційні можливості при впровадженні стандарту на різних підприємствах та/або в організаціях [29].

Документи серії *ITIL* (бібліотека інфраструктури інформаційних технологій) розвивають системний підхід стандарту *ISO* до питань інформаційної безпеки. Основними напрямками для досягнення більш безпечних форм управління інформаційними технологіями визнаються імплементація інформаційної безпеки у процеси розробки рівнів якості інформаційних послуг на підприємстві, а також формування оптимального рівня інформаційної безпеки відповідно до наявних ресурсами (людськими, фінансовими та ін.) [2].

За рахунок ширших можливостей узгодження загальноекономічних та інформаційних аспектів та пріоритетів діяльності організації, *ITIL* є набагато більш «рухомим» стандартом, порівняно з *ISO* 27001 [33]. Його додатковою перевагою є також можливість модульного впровадження, виходячи з існуючих умов (можливостей та загроз) зовнішньої середовища. У свою чергу основні регламентуючі умови для впровадження *ITIL* полягають у наступному:

Можливість комплексного впровадження принципів управління інформаційними системами відповідно до зазначених умов та вимог, а також інформування всіх учасників організаційної системи про заданих умовах та принципах.

Можливість постійного відстеження функціонування інформаційних систем щодо реалізації інцидентів (проблем) з інформаційною безпекою та іншими загрозами.

З урахуванням даних обмежень, впровадження *ITIL*, навіть з урахуванням модульної реалізації, є вкрай витратним заходом, що передбачає детальне навчання співробітників організації за принципами функціонування стандарту.

Стандарт *COBIT*, вперше розроблений у США, на відміну від двох попередніх систем документів, концентрується на чітко визначеному переліку інформаційних процесів (включаючи процес забезпечення та підтримки інформаційної безпеки). *COBIT* оперує поняттям «рівень зрілості процесу», кожен з яких передбачає якісну підтримку виконання кожного процесу на певному ступені (починаючи від «0» – відсутність процесу, до «5» – процес досяг можливості самооптимізації) [40].

У питаннях інформаційної безпеки *COBIT* передбачає виконання наступного плану дій [33]:

1. Визначення провідних / ключових завдань забезпечення інформаційної безпеки.

2. Позначення прийнятного рівня ризику інформаційної безпеки (відповідно до стратегії розвитку інформаційних систем).

3. Розробка плану мінімізації можливих ризиків (загроз) безпеки.

4. Підтримання та розвиток компетенцій управління інформаційною безпекою.

Важливою додатковою відмінністю *COBIT* від *ITIL* є можливість впровадження (і подальшого підтримання) процесу управління інформаційною безпекою на заданому рівні, без впровадження та необхідності одночасного розвитку будь-яких зв'язаних модулів, що значно знижує навантаження бюджету організацій. Разом з тим, цей стандарт вкрай спеціалізований з точки зору використання спеціальної термінології та вимагає щодо високого базового рівня розуміння інформаційних процесів (при цьому у *COBIT* відсутня широка деталізація дій з поясненнями для менеджерів порівняно з *ISO* та *ITIL*) [33].

Отже, підсумовуючи цю роботу, ми можемо констатувати необхідність подальшого всебічного вивчення існуючої методологічної основи управління інформаційної безпекою у межах освоєння накопиченого зарубіжними організаціями досвіду. Проміжна класифікація існуючих стандартів для подальшого розвитку вітчизняного досвіду (Як в аспекті теорії, так і практики) представлена в таблиці 1.1.

Таблиця 1.1

Трирівнева класифікація стандартів управління інформаційною безпекою [33, 39, 40]

Стандарт	Сильна сторона	Слабка сторона	Що стосується…
ISO	Універсальна модель в основі	Низька адаптованість	Великих та транснаціональних компаніях
ITIL	Можливість модульного впровадження	Дороге комплексне використання	Фінансово забезпечені компанії
COBIT	Найбільша гнучкість	Надмірність регуляторних аспектів	Молодих компаніях та стартапах

1.2. Сучасні підходи до класифікації загроз інформаційній безпеці

Перш, ніж класифікувати можливі види загроз інформаційній безпеці, необхідно детально розглянути існуючу етимологію даного словосполучення.

«Загроза інформаційної безпеки – це сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки» [6]. Стратегія національної безпеки дає нам загальне визначення поняття «загрози» і розглядає їх як «пряму або опосередковану можливість нанесення шкоди конституційним правам, свободам, гідної якості і рівню життя громадян, суверенітету і територіальної цілісності, сталого розвитку України». На відміну від правового акту, який би основні положення національної безпеки, тлумачний словник ім. С. І. Ожегова торкається питання

національного значення і визначає загрозу як можливу, ще не реалізовану небезпека [31]. В даному випадку під загрозою передбачається небезпека настання змін, а не сам процес.

Таким чином, в процесі дослідження проблем, пов'язаних з інформаційною безпекою необхідно враховувати не тільки фактичну, а й потенційну загрозу заподіяння шкоди. Під терміном «інформаційна безпека» загальноприйнято розуміти захищеність інформаційної системи від навмисного і випадкового втручання, яке може завдати шкоди користувачам інформації або її власникам [26]. Загроза інформаційної безпеки – це сукупність факторів і наслідків, які можуть створити потенційну або фактичну небезпеку станом захищеності особистості, суспільства і держави. Такими факторами може бути весь перелік основних принципів функціонування Інтернету. Серед них: принципи ієрархічності, демократичності, децентралізації, конвергенції і екстериторіальності [8]. У загальному сенсі під загрозами інформаційній безпеці прийнято розуміти сукупність факторів і умов, які створюють небезпеку порушення безпеки і цілісності інформації, в тому числі копіювання, поширення, зміна, блокування, несанкціонований доступ або інші невповноважені дії з захищеною інформацією.

Для реалізації загроз інформаційної безпеки необхідно створення каналу між носієм інформації і джерелом загрози, що створює сприятливе середовище для порушення безпеки інформаційної системи.

Існують три основні елементи для реалізації загроз інформаційної безпеки, це: джерело інформації, середа впливу і носій. Джерелом загроз інформаційній безпеці може виступати матеріальний об'єкт, суб'єкт або певне фізичне явище, що несе загрозу. Середовище впливає інформації являє собою той шлях поширення інформації, в якому певні програми, дані або сигнал можуть надавати впливу на доступність, цілісність та

конфіденційність захищеної інформації. Роль носія інформації може грати як матеріальний предмет або фізична особа, так і інформаційне поле.

Аналіз негативних впливів здійснення і виникнення загроз включає в себе обов'язкову ідентифікацію можливих джерел вразливостей, погроз, а також методів їх реалізації. Для здійснення ефективної і комплексної ідентифікації та подальшого усунення потенційних загроз інформаційній безпеці необхідно вибудувати чітку класифікацію.

Загальна класифікація загроз інформаційній безпеці здійснюється:

– за джерелом загроз інформаційній безпеці;

– за ступенем ймовірності здійснення;

– по об'єкту впливу;

– за способом реалізації;

– по положенню джерела;

– за характером джерела;

– за наслідками.

Розглянемо перераховані категорії більш детально. В першу чергу, необхідно визначити, хто або що може являти собою джерело загрози інформаційній безпеці. Мною вже було зазначено раніше, що джерелом загрози інформаційній безпеці можна розділити на три групи: антропогенні, технічні та природні, але для більш докладної класифікації необхідно проаналізувати кожну з них. Класифікація по джерелу загроз інформаційній безпеці представлена на рисунку 1.1.

До групи антропогенних загроз відносяться суб'єкти, які мають санкціонований або несанкціонований доступ до інформації. Антропогенні джерела, в свою чергу, також можна розділити на внутрішні і зовнішні.

І зовнішні, і внутрішні антропогенні джерела загроз інформаційній безпеці можуть бути навмисними або випадковими.

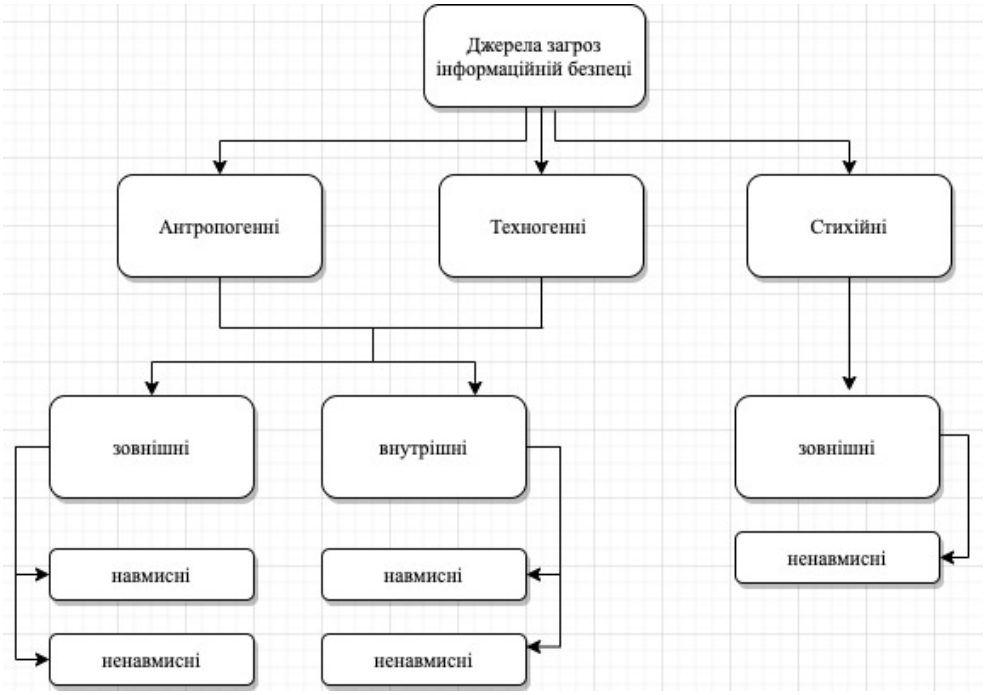

Рисунок 1.1 – Класифікація по джерелу загроз інформаційної безпеки

До ненавмисним внутрішнім джерелом антропогенного характеру загроз можна віднести персонал, некоректні дії якого можуть представляти загрозу інформаційній безпеці. Подібного роду загрози виникають, як правило, через помилки програмного забезпечення, відмов, збоїв або пошкоджень інформаційної системи.

Внутрішні антропогенні джерела складають групу штатних співробітників підприємства. Особливе значення в даній категорії загроз займають випадкові порушення співробітниками вимог експлуатації техніки або некоректне використання інформації. Таку групу представляє основний, технічний і допоміжний персонал. До них можуть також відноситься і висококваліфіковані фахівці, що працюють в сфері експлуатації технічних засобів і програмного забезпечення.

Навмисні джерела загроз відрізняються саме умисної дезорганізацією роботи. Спотворення, крадіжка, злом інформації здійснюється шляхом несанкціонованого доступу в конфіденційні інформаційні ресурси.

Особливу увагу слід приділити саме навмисним загрозам, як від внутрішніх, так і від зовнішніх джерел загроз інформаційної безпеки антропогенного характеру. Реалізація загрози і здійснення несанкціонованого доступу може протікати шляхом: елементів інформаційної інфраструктури, які можуть виявитися поза контролем через супутніх процесів, таких як: ремонт, супровід або утилізація; використання шкідливих програм, програмних або алгоритмічних закладок; несанкціонованого підключення до каналів зв'язку, які виходять за територіальні межі підприємства; використання автоматизованих робочих місць, які підключені до мереж загального користування. Також необхідно враховувати, що групу внутрішніх джерел можуть становити спеціально навчені агенти або люди з порушеннями психіки.

Варто відзначити, що загрози, розташовані за межами контрольованої підприємством зони або зовнішні загрози в системі інформаційної безпеки, не обов'язково несуть навмисний характер. Залежно від особливостей організації інформаційної та технічної системи підприємства певні дії зовнішніх суб'єктів можуть спричинити відхилення основних критеріїв інформаційної безпеки [1]. Це може здійснитися в процесі стандартної експлуатації системи з використанням доступу зовнішніх інтерфейсів. До зовнішніх антропогенним джерелам можна віднести: конкуруючі організації, партнерів, структури кримінального характеру, силові структури, провайдерів послуг зв'язку, потенційних зловмисників і користувачів інформаційної системи.

Техногенні джерела загроз інформаційній безпеці також можуть поділятися на внутрішні і зовнішні, і залежать виключно від технічної складової. Роль зовнішніх техногенних джерел загроз зазвичай виконують мережі комунікацій і засоби зв'язку: каналізація, водопостачання, опалення, лінії передач даних, телефонні лінії та інше.

Внутрішні техногенні джерела загроз інформаційній безпеці можуть проявлятися в неякісних програмних засобах обробки інформації, шкідливі програми і апаратних закладках.

Природні джерела загроз інформаційній безпеці відрізняються своєю непередбачуваністю і можуть мати виключно зовнішній характер. До них відносяться такі стихійні лиха, як: пожежі, урагани, землетруси і повені. Варто додати, що даний вид інформаційної загрози менше попередніх піддається прогнозу і протидії. Однак, багато підприємств забезпечують своїх співробітників чіткою інструкцією на випадок виникнення надзвичайної ситуації, яка допомагає скоротити збитки.

Всі джерела погроз мають різний рівень ймовірності, який можна розрахувати з урахуванням непрямих показників, таких як: можливість виникнення, готовність джерела і фатальність.

Класифікація загроз інформаційній безпеці по об'єкту впливу містить загрози порушення безпеки інформації, які можуть бути реалізовані шляхом впливу на сервери, взаємодія каналів зв'язку, використання автоматизованих робочих місць і певних засобах обробки інформації, таких як принтери, монітори і проектори.

Реалізація загрози інформаційної безпеки спрямована на порушення процесу експлуатації інформаційної системи, а також може спрямована на основні характеристики інформації: доступність, актуальність, цілісність і конфіденційність. Сам процес створення іншої загрози, як правило складається з чотирьох етапів: збір інформації, проникнення в середу, реалізація несанкціонованого доступу і ліквідація слідів доступу. Класифікація за способом реалізації загрози інформаційної безпеки складається з наступних видів:

– навмисне вплив на інформаційну систему підприємства з використанням вразливостей апаратного і програмного забезпечення або вірусних програм;

– витік інформації техногенного характеру;

– соціальна інженерія, тобто використання методів впливу безпосередньо на людину з метою несанкціонованого доступу до інформаційних ресурсів.

Відповідно до положення джерела можна виділити два види загроз:

– джерело загрози розташований в межах контрольованої підприємством зони;

– джерело загрози розташований за межами контрольованої підприємством зони.

За характером можна також виділити два види загроз:

– пасивні загрози, які не впливають на роботу інформаційної системи, але можуть порушити певні правила кордонів доступу до мережевих ресурсів або іншої інформації;

– активні загрози, які роблять безпосередній вплив на інформаційну систему, порушуючи кордону доступу до мережевих ресурсів і інформації.

Також загрози інформаційній безпеці можна класифікувати за такими основними критеріями:

1. Спосіб здійснення загрози. Виділяють навмисні, випадкові дії, а також надзвичайні ситуації техногенного або природного характеру.

2. Націленість загрози на найважливіші властивості інформації такі як: конфіденційність, цілісність, доступність. Саме проти цих складових в першу чергу спрямовані інформаційні атаки.

3. Компоненти інформаційних технологій і систем. На що безпосередньо націлені загрози: мережі, дані, програмно-апаратні комплекси, інша підтримує інфраструктура, а також апаратна частина інформаційної системи.

4. Локалізація джерела загрози. Вона може бути, як всередині інформаційної системи, так і поза системою або технології.

Була розглянута основна і найбільш поширена класифікація загроз інформаційній безпеці. На даному етапі слід звернути увагу на більш вузьку класифікацію, а саме на загрози інформаційної безпеки систем уділеної обробки даних. Для подальшого дослідження необхідно проаналізувати основи класифікації загроз інформаційній безпеці систем дистанційної обробки даних, оскільки обраний об'єкт дослідження задіє цей процес у своїй роботі. У процесі віддаленої обробки даних різного характеру задіяні інформаційно-вимірювальні системи, які, в свою чергу, складаються з трьох основних структурних складових, а саме: програмна, комунікаційна та апаратна. Отже, серед загроз, спрямованих на порушення безпеки інформації, можна також виділити:

– загрози, які пов'язані безпосередньо з апаратною частиною інформаційної системи;

– загрози, які пов'язані з комунікаційною системою;

– загрози, характерні для ПО.

Наочну схему класифікації перерахованих вище загроз можна розглянути більш докладно на рисунку 1.2.

Розглянемо більш детально клас загроз, який характерний для програмного забезпечення інформаційної системи підприємства.

Загрози даного кластера спрямовані на інформацію, що зберігається в пам'яті. Процес запису даних за або перед межами виділеного буфера програмою, затираючи тим самим дані називається переповнення буфера. Це явище є причиною порушення конфіденційності, доступності та цілісності інформації. Подібну ситуацію може спровокувати неправильна робота з даними.

Також, до погроз, спрямованих на інформацію, що зберігається в пам'яті, можна віднести шкідливе посилання на об'єкт, за допомогою якої зловмисник отримує несанкціонований доступ до інформації, що зберігається на певній ділянці пам'яті.

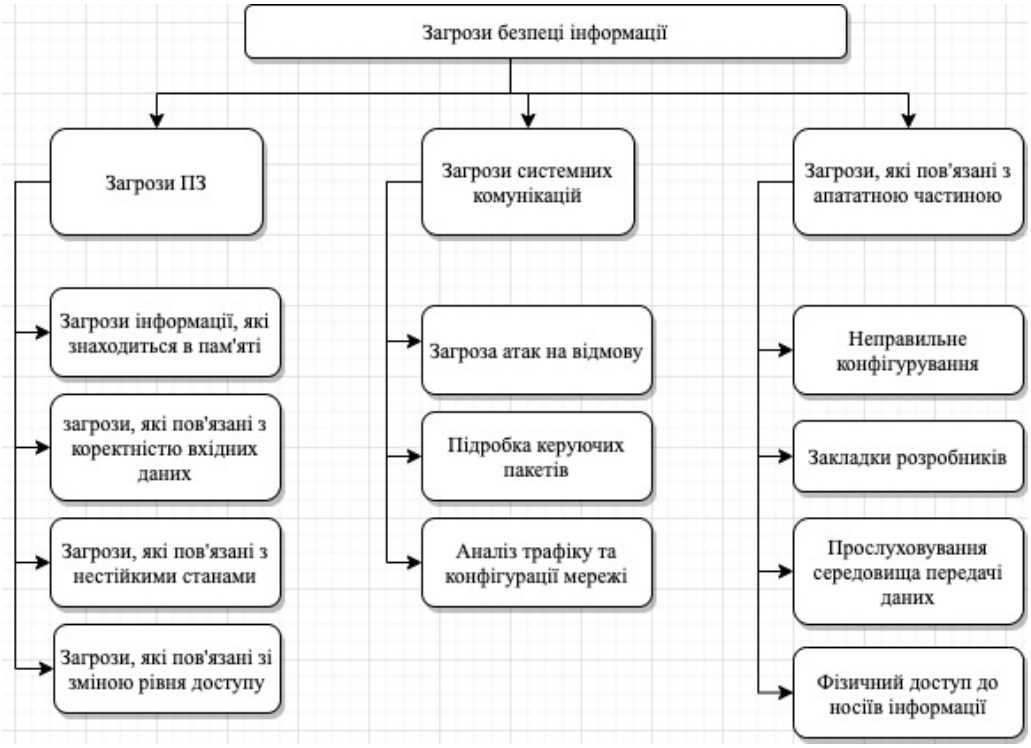

Рисунок 1.2 – Класифікація загроз інформаційній безпеці в інформаційних системах

У цю ж групу можна віднести загрози, які пов'язані з некоректністю вхідних даних і зміною рівня доступу.

Загроза застосування в запити також є видом загроз, спрямованим на інформацію, що зберігається в пам'яті. Цей метод заснований на впровадженні в запит довільних команд, що може спровокувати порушення цілісності та конфіденційності інформації [28].

Незахищений доступ до областей інформаційної системи дозволяє користувачеві відкрити доступ до областям системи, що грає принципово значиму роль в працездатності системи.

Розглянемо загрози, які характерні для системи комунікацій. До цієї групи загроз можна віднести різні види інформаційних атак в мережі Інтернет. Серед цих атак можна виявити наступні:

1. Проста атака на відмову. Принцип дії даної атаки полягає в перевищенні відправляються запитів системі, що надалі, призводить до

нездатності системи обробити запитувана кількість інформації і, в кінцевому рахунку, система обмежує доступність інформації.

2. Розподілена атака на відмову. На відміну від простої атаки на відмову, розподілена атака задіє велику кількість робочих станцій.

3. Підробка пакетів керуючих мережевих пристроїв.

4. Перехоплення мережевого трафіку.

5. Сканування. Отримання доступу до мережевих портів інформаційної системи з метою виявлення вразливостей програмного забезпечення. Остання група загроз відноситься до апаратної частини. До цієї групи можна віднести наступні види загроз:

1. Неправильна конфігурація апаратних засобів. Некоректна настройка апаратної частини може стати причиною фізичного пошкодження або відмови роботи апаратури.

2. Отримання фізичного доступу до носія інформації.

3. Використання закладок. Несанкціоноване використання зловмисниками закладок може привести до порушення конфіденційності, цілісності та доступності інформації. Цей вид загрози характерний для апаратних пристроїв без використання процесу аутентифікації [11].

4. Апаратне прослуховування даних. Мається на увазі перехоплення повідомлень, шляхом використання бездротової мережі або фізичне підключення зловмисника до засобу передачі даних. Цей вид загрози характерний для розподільних систем з низьким рівнем криптостійкості.

Таким чином, можна стверджувати, що класифікація загроз інформаційній безпеці може бути проведена по безлічі різних показників. Найбільш поширеним показником у вітчизняній і зарубіжній науково-публіцистичній літературі є показник природи виникнення загрози, саме цей показник був проаналізований максимально детально.

Слід зазначити, що найбільш поширені ненавмисні помилки і саме вони являють собою найбільшу небезпеку і найбільшу можливість

заподіяння шкоди. Найчастіше, ці помилки і є загрозами, але також вони можуть бути причинами виникнення загроз, створюючи вразливі місця в інформаційній системі. До таких помилок можна віднести ненавмисні дії, некоректно введені дані системних адміністраторів, операторів, штатних користувачів або інших осіб, що займаються обслуговуванням інформаційної системи. Користувачі системи можуть бути джерелами таких загроз, як: ненавмисне або навмисне спотворення або знищення даних, технічне відсутність можливості роботи з інформаційною системою, відсутність відповідної підготовки користувача, що, в свою чергу може спровокувати некоректне використання інформації.

Найбільш ефективним способом усунення помилок ненавмисного характеру є строгий регламент будь-яких дій користувачів, а також максимальна стандартизація та автоматизація процесів.

Класифікація та ідентифікація загроз інформаційній безпеці підприємства є одними з найважливіших процесів для ефективної і безпечної роботи.

1.3. Висновки до розділу 1

Було проаналізовані відомі методології з аналізу ризиків інформаційній безпеці, такі як ISO, ITIL, COBIT. Проведено порівняльний аналіз даних методологій, виявлено їх недоліки та переваги. На основі проведеного аналізу, можна зробити висновок, що оптимальним варіантом для вибору методики управління загрозами інформаційної безпеки в контексті забезпечення безпеки інформації підприємства та місцям її зберігання, обробки та передачі є адаптація та удосконалення відомих методик логічним об’єднанням їх переваг і мінімізацією недоліків.

РОЗДІЛ 2
МОНІТОРІНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПИЄМСТВА

2.1. Встановлення контексту забезпечення інформаційної безпеки

На основі стандарту ДСТУ ISO / IEC 27005-2010 «Інформаційна технологія. Методи і засоби забезпечення безпеки: Менеджмент ризику інформаційної безпеки» (ISO / IEC 27005: 2008 *Information technology – Security techniques – Information security risk management* (IDT)) розглянемо процес управління ризиком інформаційної безпеки веб-ресурсу промислового підприємства (надання *B2B* послуг).

Наведемо типові поди оцінки ризику організації на прикладі веб-ресурсу промислового підприємства.

Процес управління ризиком інформаційної безпеки

Процес менеджменту ризику ІБ складається з:

– встановлення контексту;

– оцінки ризику;

– обробки ризику;

– прийняття ризику;

– комунікацій ризику;

– моніторингу та переоцінки ризику ІБ (рисунок 2.1).

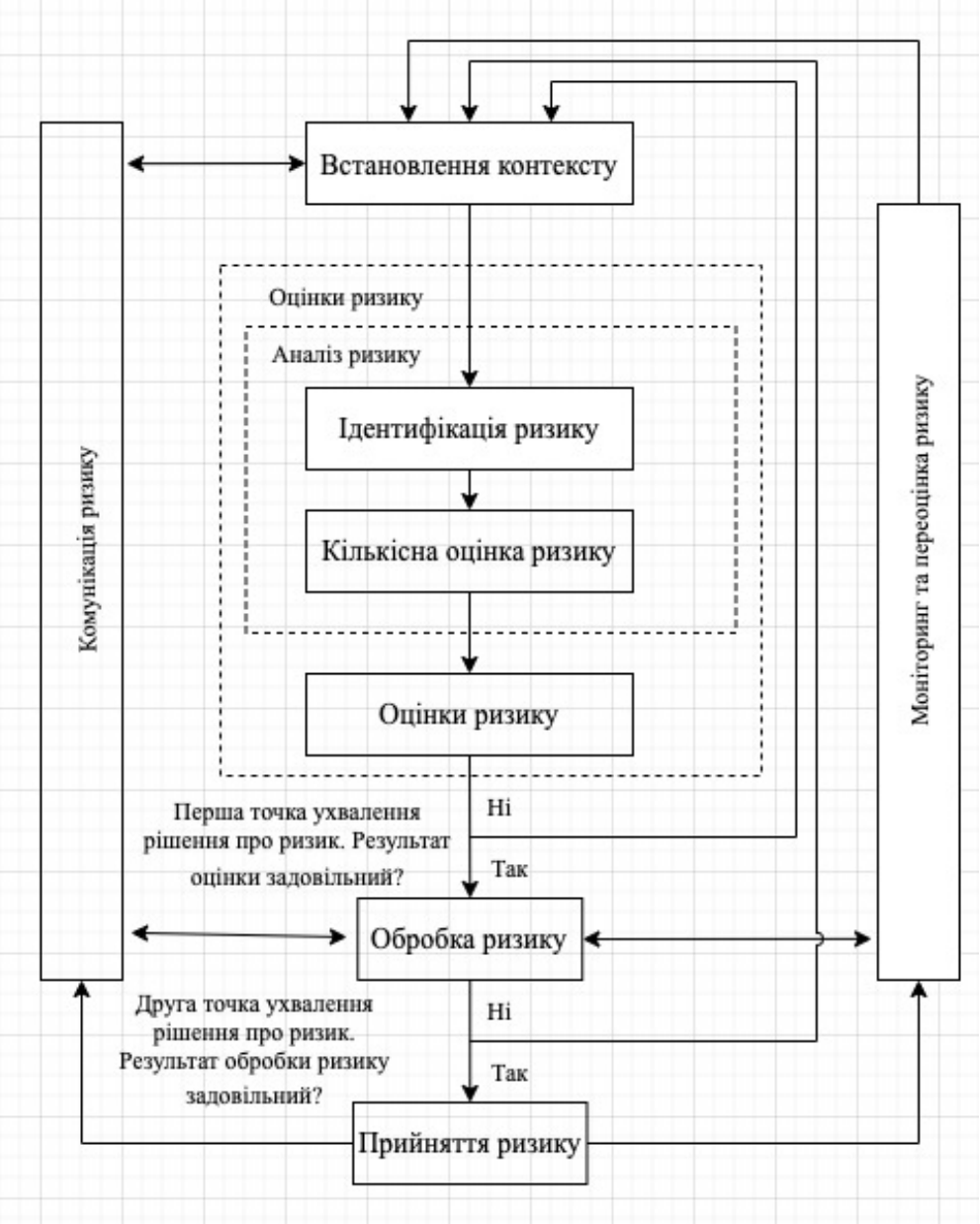

Рисунок 2.1. – Процес ризик-менеджменту інформаційної безпеки

Процедури оцінки ризику і обробки ризику в процесі менеджменту ризику ІБ можуть виконуватися ітеративно, такий підхід до проведення оцінки ризику може збільшити деталізацію і глибину оцінки при кожній наступній ітерації. Якщо для ефективного визначення дій вдається отримати достатню інформацію на черговому кроці ітерації, необхідну для зниження ризику до необхідного рівня, то вважається, що завдання етапу виконана, потім йде етап обробки ризику. У разі недостатності інформації

для прийняття рішення, переглядається контекст і здійснюється чергова ітерація оцінки ризику (критеріїв оцінки, впливу або прийняття ризиків), можливо для деякої окремої частини повної предметної області, яка обмежена першою точкою прийняття рішення.

Ефективність обробки ризику безпосередньо залежить від результатів одержуваних при оцінці ризику. Первісна обробка ризику може не забезпечити необхідний рівень залишкового ризику. В цьому випадку можуть знадобитися, додаткові ітерації оцінки ризику зі зміною відповідних параметрів контексту (критеріїв оцінки, впливу і прийняття ризику), за кожною з яких піде відповідна кроці ітерації процедура обробки ризику, що запускається на другій точці прийняття рішення (рисунок 2.2).

Встановлення контексту, оцінка, розробка плану обробки, прийняття ризику в системі моніторингу інформаційної безпеки (СМІБ) представляють собою розділ фази «планування». У фазі «здійснення» СМІБ за планом обробки ризику реалізуються процедури і заходи для зниження ризику до необхідного рівня. Керівництво в фазі «перевірка» СМІБ встановлює необхідність оцінки і обробки ризику повторно через що з'явилися інцидентів і обставин, що змінилися. Проведення необхідних робіт, щодо підтримки та вдосконалення процесу моніторингу ризику ІБ відбувається в фазі «дія». У таблиці 2.1 показані чотири фази процесу СМІБ у взаємозв'язку з процедурами моніторингу ризику.

Таблиця 2.1

Співвідношення процесу ризик-менеджменту інформаційної безпеки і компонентів процесу системи менеджменту інформаційної безпеки

Процес СМІБ	**Процес менеджменту ризику ІБ**
Планування	Встановлення контексту
	Оцінка ризику
	Планування обробки ризику
	Прийняття ризику
Здійснення	Реалізація плану обробки ризику
Перевірка	Проведення безперервного моніторингу та переоцінки ризиків
Дія	Підтримка та вдосконалення процесу менеджменту ризику ІБ

В процесі менеджменту ризику інформаційної безпеки виділимо і деталізуємо процес оцінки ризику ІБ і зобразимо його у вигляді схеми на рисунку 2.3.

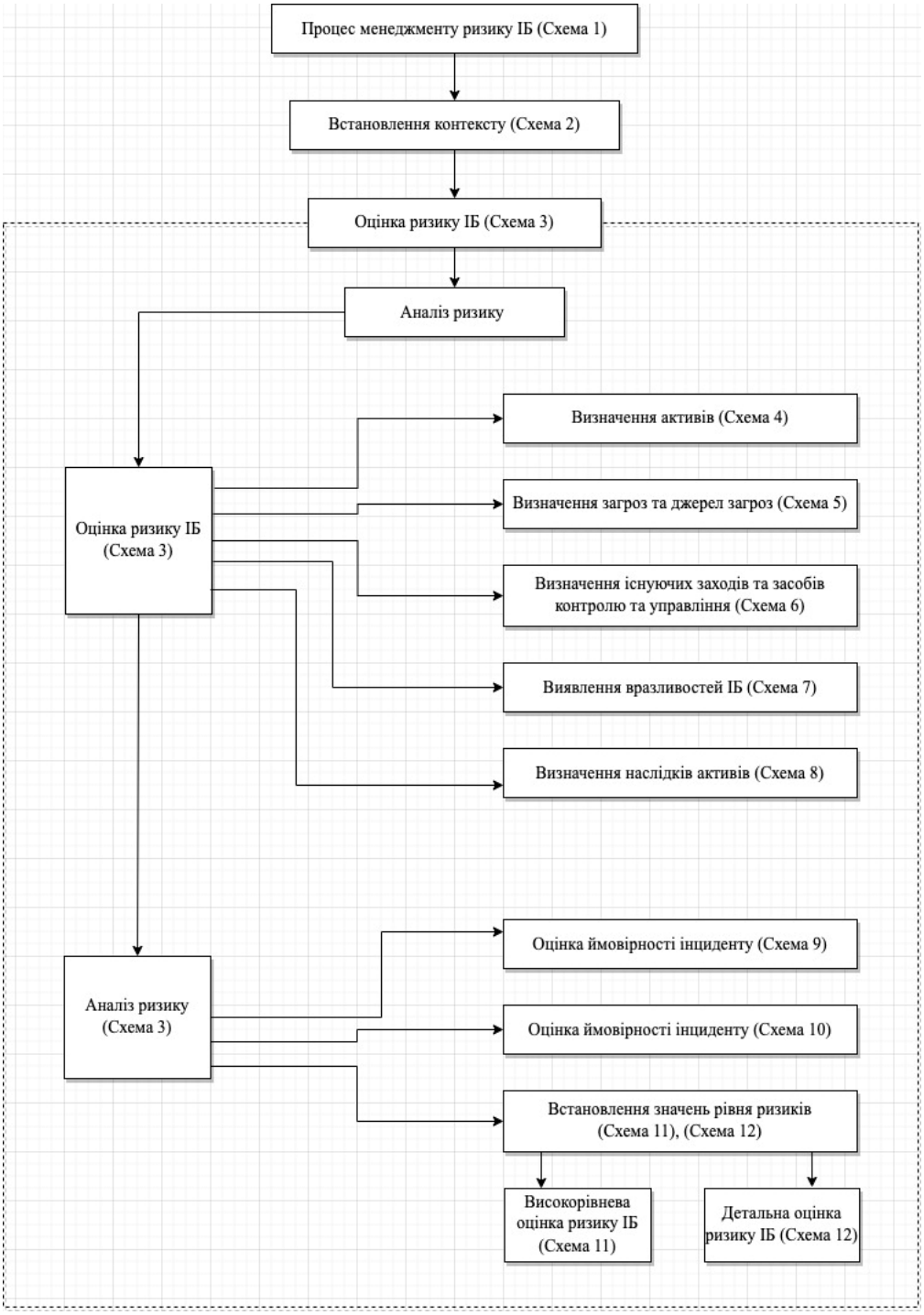

Рисунок 2.2. – Деталізований процес оцінювання ризику ІБ

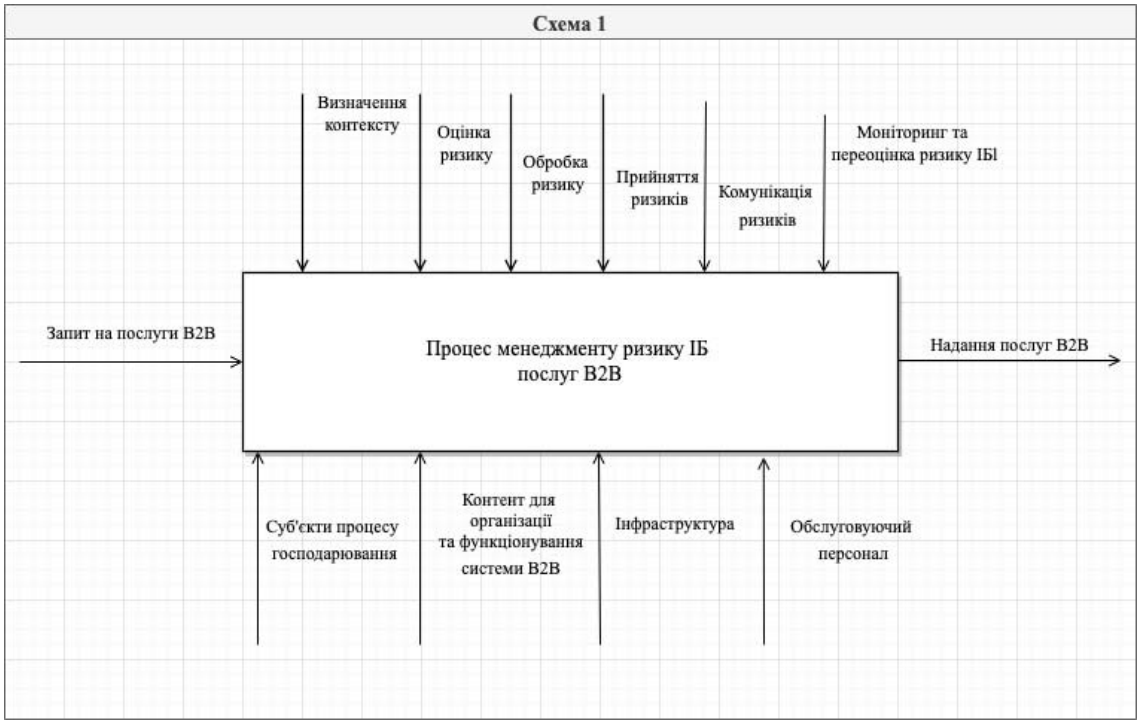

Рисунок 2.3 – Процес моніторингу ризику ІБ промислового підприємства

Встановлення контексту (схема 2, рис. 2.4).

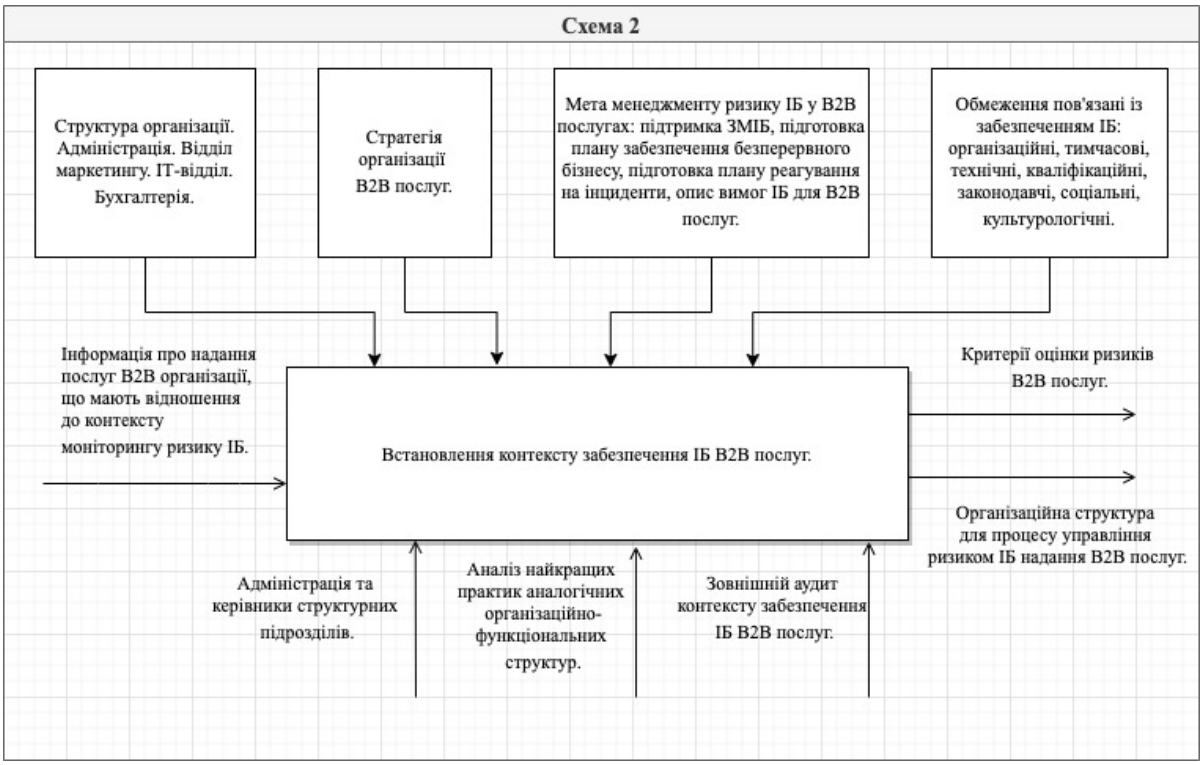

Рисунок 2.4 – Встановлення контексту забезпечення ІБ B2B послуг

Вхідні дані. Вся інформація про надання послуг організації, що має відношення до контексту менеджменту ризику ІБ.

Аналіз організації.

Основна мета організації. Надання *B2B* послуг.

Структура організації:

– адміністрація.

–відділ маркетингу.

– ІТ-відділ.

– бухгалтерія.

Стратегія організації. Надання якісних *B2B* послуг з використанням сучасних способів подання електронного контенту.

Дія. Завдання даного етапу полягає у встановленні контексту менеджменту ризику ІБ, в цю процедуру входить визначення основних критеріїв, необхідних для менеджменту ризику ІБ, а також встановлення області застосування і меж і створення відповідної організаційної структури, що забезпечує менеджмент ризику ІБ.

Функціональні обмеження. Цілодобова робота сервісу, для безперервно забезпечення доступу до *B2B* послуг.

Обмеження, що стосуються персоналу. Наявність фахівця з ІБ.

Обмеження культурної властивості. Освіта, навчання, професійний досвід, роботу, на яку поширюється життєвий досвід, думки, філософію, переконання, почуття, соціальний статус і т.д.

Нормативні вимоги, що ставляться до діяльності промислового підприємства на ринку *B2B* послуг. До їх числа можуть бути віднесені закони, постанови, спеціальні інструкції, що належать до сфери діяльності організації або внутрішнім / зовнішнім нормам. Це стосується також договорів і угод та будь-яких зобов'язань юридичної властивості.

Технічні обмеження.

Відносяться до інфраструктури технічні обмеження, як правило, виникають від функціонуючих в організації апаратних і програмних засобів і від площадок або приміщень, де здійснюються процеси:

– файлові архіви (вимоги, щодо організації, менеджмент носіїв, менеджмент правил доступу і т.д.);

– загальна архітектура (вимоги, щодо топології (централізована архітектура, розподілена архітектура, архітектура клієнт-сервер, фізична архітектура і т.д.));

– прикладні програми для організації B2B-сервісів – (вимоги, щодо проектування специфічного програмного забезпечення задовольняє особливі потреби B2B ринку, ринкові стандарти і т.д.);

– апаратні засоби (вимоги, що ставляться до стандартів, якості, відповідності нормам і т.д.);

– мережі зв'язку (вимоги, що ставляться до стандартів організації мереж, розширюваності, масштабованості, надійності і т.д.);

Обмеження за часом. Якщо на реалізацію заходів та засобів контролю і управління безпекою йде дуже багато часу, то ризики, для яких розроблялася система заходів і засобів контролю та управління, можуть змінитися. При прийнятті рішень і виборі пріоритетів час є визначальним фактором.

Організаційні обмеження. Вимоги організації накладають певні обмеження:

– експлуатація (вимоги, що стосуються надання послуг, тривалості виробничого циклу, моніторингу, спостереження, погіршення роботи, планів дій в надзвичайних ситуаціях та ін.);

– підтримка (вимоги до процедури пошуку несправностей, пов'язаних з інцидентом, здійсненню превентивних дій, швидкого виправлення та ін);

– менеджмент кадрових ресурсів (вимоги, які стосуються навчання операторів і користувачів, до рівня кваліфікації, необхідної для таких посад,

це можу бути посади системного адміністратора або адміністратора даних і ін.);

– адміністративний менеджмент (вимоги до персоналу, що стосуються обов'язків і ін.);

– менеджмент розробки (вимоги, що ставляться до інструментальних засобів розробки, вимоги до системи автоматизованої розробки програм, планів приймального контролю та ін.);

– менеджмент зовнішніх відносин (вимоги, що ставляться до формування відносин з третіми сторонами, договорів і т.д.).

Керівництво по реалізації. Мета моніторингу ризику ІБ веб-ресурсів промислового підприємства на ринку B2B послуг:

– підтримка СМІБ;

– підготовка плану забезпечення безперервності бізнесу щодо здійснення послуги;

– підготовка плану реагування на інциденти;

– опис вимог ІБ для *B2B* послуги.

Вихідні дані. Специфікація основних критеріїв, кордони, сфера дії, організаційна структура для процесу менеджменту ризику ІБ.

Критерії оцінки ризиків інформаційної безпеки.

Критерії для оцінки ризиків інформаційної безпеки *B2B* послуг вибираються з урахуванням:

– стратегічної цінності обробки бізнес-інформації (інтелектуальна праця);

– критичності порушених інформаційних активів (персональні дані клієнтів);

– законодавчо-нормативних вимог і договірних зобов'язань (надання *B2B* послуг відповідного рівня обсягу і якості);

– оперативного значення і значення для бізнесу доступності, конфіденційності та цілісності;

– очікування і реакції причетних сторін, а також негативних наслідків для нематеріальних активів і репутації підприємства.

2.2. Оцінювання ризику інформаційної безпеки

Оцінка ризику інформаційної безпеки (Схема 3, рис. 2.5).

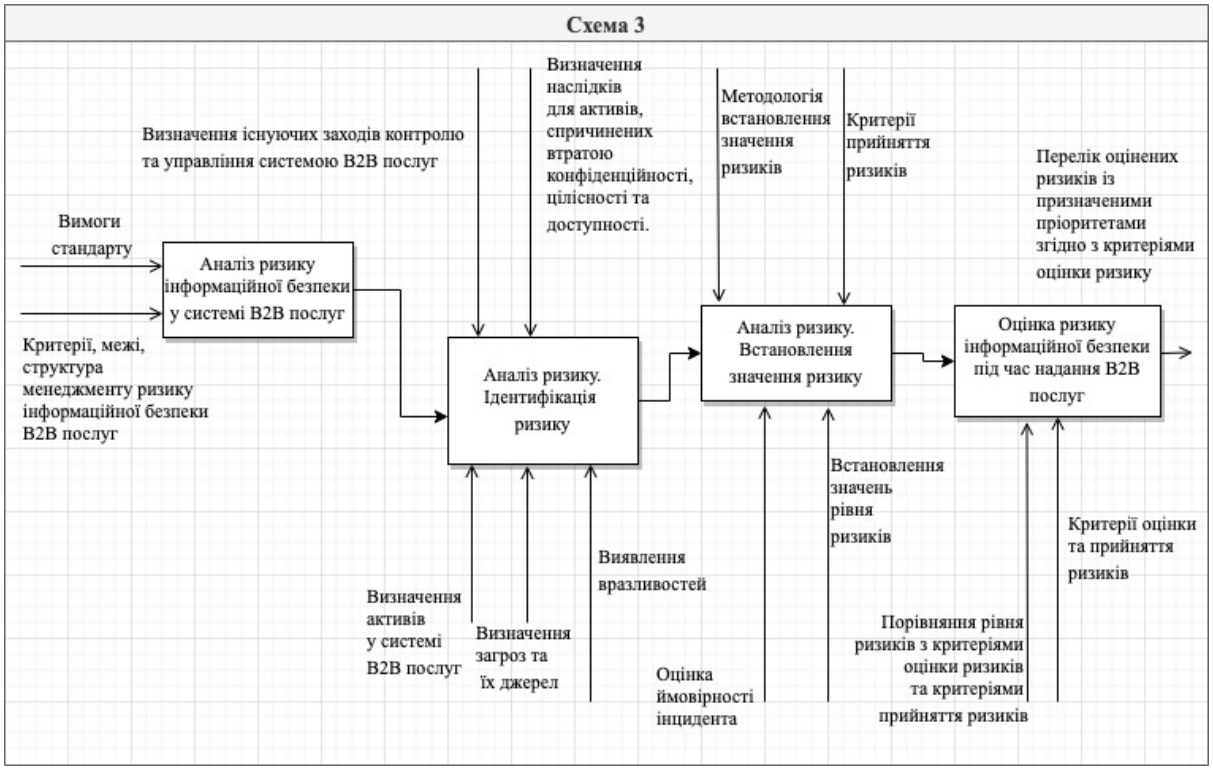

Рисунок 2.5 – Оцінка ризику інформаційної безпеки в процесі надання B2B послуг

Загальний опис оцінки ризику інформаційної безпеки

Вхідні дані. Встановлені основні критерії, сфера дії і кордони, структура процесу ризик-менеджменту інформаційної безпеки, прийняті для організації, що надає *B2B* послуги.

Дія. Необхідно ідентифікувати ризики, кількісно або якісно їх охарактеризувати, призначити для них пріоритети відповідно до критеріїв оцінки ризику і цілей промислового підприємства.

Керівництво по реалізації. Ризик являє собою комбінацію наслідків, що випливають з небажаної події та ймовірності виникнення події.

Оцінка ризику кількісно або якісно характеризує ризики і дає керівникам можливість призначати для ризиків пріоритети відповідно до усвідомленої керівництвом серйозністю або іншими встановленими критеріями.

Процес оцінки ризику складається з:

– аналізу ризику, що включає ідентифікацію ризику і встановлення значення ризику;

– оцінки ризику.

Вихідні дані. Перелік оцінених ризиків відповідно до призначеними пріоритетами узгоджується з критеріями оцінки ризику.

Аналіз ризику: ідентифікація ризику.

Мета ідентифікації ризику – у визначенні того, що може статися при нанесенні можливого збитку, і в отриманні уявлень про те, як, де і чому могла мати місце така шкода. Зазначені нижче етапи, повинні об'єднувати вхідні дані для діяльності по кількісній оцінці ризику.

Визначення активів (схема 4, рис. 2.6)

Вхідні дані. Сфера дії та межі етапу проведення оцінки ризику, перелік, що включає місце розташування, власників, функцію і т.д.

Дія. Визначаємо активи, що входять до встановленої сфери дії.

Керівництво по реалізації. Активом є що-небудь, що має цінність для організації і, тому, потребує захисту. При визначенні активів необхідно враховувати, що інформаційна система складається не тільки з програмних і апаратних засобів.

Вихідні дані. Перелік активів, які підлягають менеджменту ризику, а також перелік бізнес-процесів, пов'язаних з активами та їх значущість.

Визначення і встановлення цінності активів і оцінка впливу (Схема 4, рис. 2.6)

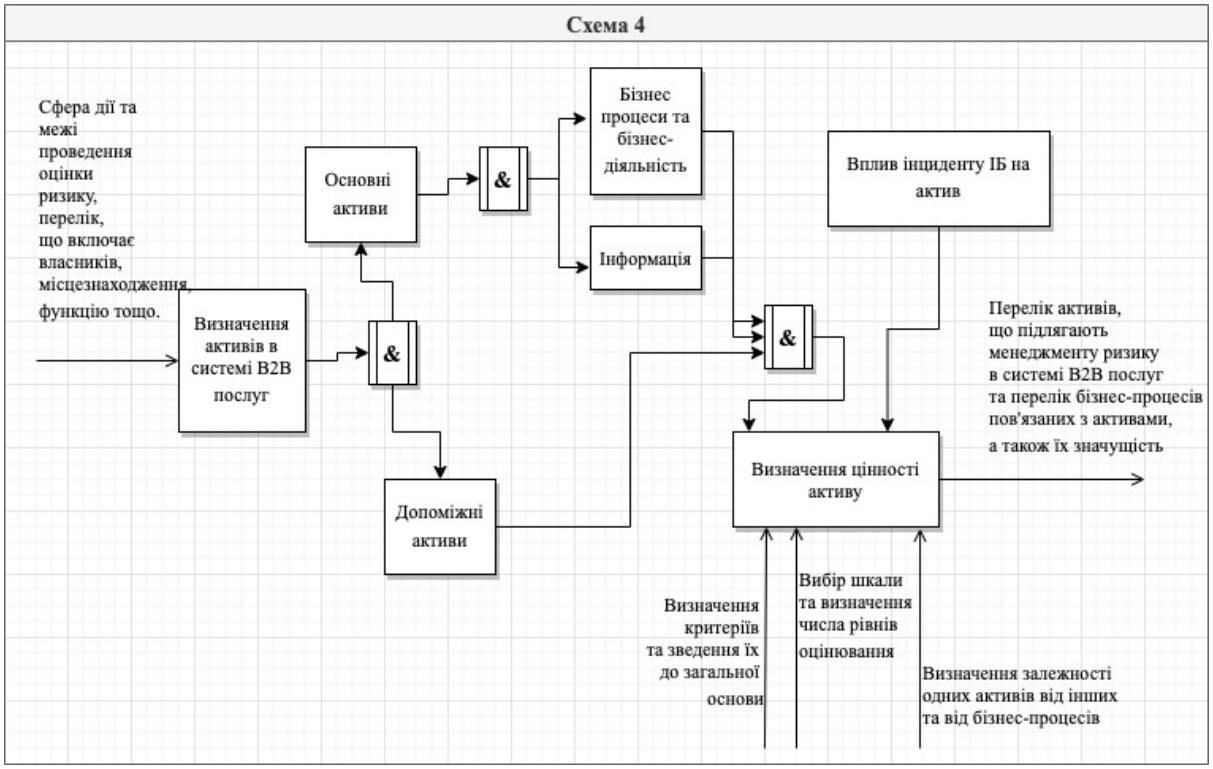

Рисунок 2.6 – Визначення активів в системі B2B послуг

Щоб встановити пріоритет активів, організація повинна, в першу чергу, визначити всі належні їй активи на відповідному рівні деталізації. Розрізняють два види активів:

– основні активи, що містять бізнес-процеси, бізнес-діяльність і інформацію;

– допоміжні (підтримуючі) активи, від них залежать основні складові частини області застосування всіх типів, що містять програмне забезпечення, апаратні засоби, мережу, місце функціонування організації, персонал, структуру організації.

Основними активами як правило є базові процеси і інформація про діяльність підприємства, що надає *B2B* послуги в її сфері дії. Також можуть розглядатися й інші основні активи, такі, як процеси життєдіяльності організацію, які будуть мати відношення до формування політики ІБ або плану безперервності бізнесу. Залежно від мети, не завжди потрібно вичерпний аналіз всіх елементів, що становлять процес менеджменту

ризику. У таких випадках область вивчення може бути обмежена найбільш значущими елементами.

Основні активи бувають двох типів:

1. Бізнес-процеси (або під-процеси) і бізнес-діяльність, наприклад:

– процеси, втрата і / або погіршення яких унеможливлює реалізацію цілей і завдань організації;

– процеси, що містять засекречені процеси і / або процеси, створені з використанням запатентованої технології;

– процеси, модифікація яких може значно вплинути на реалізацію основних цілей і завдань організації;

– процеси, необхідні організації для виконання договірних, нормативних або законодавчих вимог.

2. Інформація. Основна інформація, здебільшого, включає в себе:

– інформацію, яка необхідна для реалізації призначення або бізнесу організації;

– інформацію особистого характеру, яка відповідно до національних законів про недоторканність приватного життя визначена особливим чином;

– стратегічну інформацію, яка необхідна для досягнення цілей, визначених напрямком стратегії організації;

– цінну інформацію, обробка і передача, збір і зберігання якої вимагають тривалого часу чи пов'язані з великими витратами на її придбання.

Апаратні засоби:

Сервери, персональні електронні пристрої з доступом в мережу Інтернет.

Програмні засоби:

Операційна система.

Антивірусні засоби.

Програмне середовище для організації *B2B* послуг. Браузери і плагіни до них для доступу до середовища *B2B* послуг.

Мережа:

Телекомунікаційні пристрої, що використовуються для з'єднання декількох фізично віддалених комп'ютерів або елементів інформаційної системи.

Пристрої, є не кінцевими, а проміжними пристроями зв'язку. Ретранслятори, мости, маршрутизатори, комутатори, концентратори.

Мережеве програмне забезпечення управління та моніторингу активного мережевого обладнання. Генерація журналів реєстрації.

Персонал:

Администрация підприємства, що надає *B2B* послуги.

Менеджери *B2B* послуги.

Керівник відділу кадрів, керівник фінансового відділу, керівник який здійснює менеджмент ризику.

Персонал з експлуатації та супроводу інформаційної системи.

Разработчики программных элементов *B2B* системи та сайту промислового підприємства.

Місце функціонування організації:

Офіс та серверна.

Зовнішній хостинг сайту.

Віддалені точки доступу до системи *B2B*.

Організація:

Організація, що надає послуги.

Структура організації:

Адміністрація.

Відділ маркетингу.

ІТ-відділ.

Бухгалтерия.

Встановлення цінності активів.

Встановлення цінності активів полягає в узгодженні використовуваної шкали цінностей і критеріїв для присвоєння кожному активу визначеного положення на шкалі, заснованого на встановленні цінності. Терміни, які зазвичай використовуються для якісного встановлення цінності активів: критична, дуже висока, висока, середня, низька, дуже низька, нехтує мала.

1. Критерії

Цінність деяких активів, може, встановлюватися суб'єктивно і приймати рішення, можливо, будуть різні люди. Ймовірні критерії, які використовуються для визначення цінності активу, включають його вихідну вартість, вартість його заміни або відтворення, або цінність, яка може бути абстрактною така як цінність репутації організації.

Також підставою задля встановлення цінності активів є витрати, які можуть бути понесені через втрату конфіденційності, цілісності, облікових та доступності в результаті інциденту. Неспростовності, справжність і надійність також повинні розглядатися певним для цього чином.

2. Зведення до загальної основі

Критерії, для встановлення цінностей активів, зведені до загальної основі, можуть використовуватися при оцінці можливих наслідків, що випливають з втрати конфіденційності цілісності, доступності, облікових, надійності, неспростовності або справжності активів, включають:

– переривання сервісу (неможливість забезпечення доступу до системи *B2B* послуг;

– втрата довіри клієнта (втрата репутації промислового підприємства);

– порушення внутрішньої функціонування (порушення всередині самого підприємства (що можуть виникнути з огляду на хворобу фахівця обслуговуючого критичні процеси, пошук фахівця відповідної кваліфікації і необхідний час на адаптацію до умов і використовуваних засобів *B2B* послуг які спричиняють додаткові внутрішні витрати));

– порушення функціонування третьої сторони (цей збої в роботі організації, що надає хостинг для розміщення сайту підприємства), що спричинить за собою різні види збитків, як матеріальних у втраті клієнтів);

– порушенням законів / норм (нездатність виконання правових зобов'язань).

– порушення договору (нездатність клієнта виконувати договірні зобов'язання пов'язані з оплатою за *B2B* послуги, що тягне фінансові втрати);

– небезпека для персоналу / безпеку користувачів (небезпека крадіжки і неправомірного використання авторських наукових праць, контенту,);

– вторгнення в приватне життя користувачів (крадіжка і поширення персональних даних користувачів системи);

– фінансові втрати, пов'язані з надзвичайними обставинами або ремонтом (злом системи *B2B* послуг, DoS- атаки, вихід з ладу електронних носіїв, сховищ інформації, комунікаційного обладнання, відсутність кваліфікованого персоналу на момент виникненню надзвичайної ситуації);

– втрата товарів / фондів / активів - крадіжка і незаконне використання конкурентами електронних ресурсів;

– втрата клієнтів в результаті неефективної роботи маркетингових служб щодо своєчасного і широкому поширенню рекламної інформації, проведення інформаційних акцій та конкурсів;

– судові справи і штрафи (розміщення в системі *B2B* послуг контенту, який суперечить законодавству України і порушення авторських прав при використанні електронних ресурсів;

– втрата конкурентної переваги (необхідно використовувати сучасні методики ведення *B2B* бізнесу і регулярно оновлювати електронні ресурси);

– втрата технологічного / технічного лідерства (необхідно стежити за оновленням IT- інфраструктури, відповідності її продуктивності та обсягів

пам'яті вимогам для обслуговування великої кількості сеансів одночасної роботи з сучасними ресурсами в реальному часі);

– втрата ефективності / надійності (необхідно стежити за збільшенням кваліфікації персоналу системи *B2B* послуг, регулярно відстежувати необхідність оновлення апаратних засобів, необхідно регулярно оновлювати антивірусні програмні засоби, відслідковувати DoS-атаки і використовувати ефективні засоби протидії їм);

– втрата технічної репутації (необхідно стежити за тим, щоб не було регулярних збоїв обладнання, відмову в доступі до системи *B2B* послуг та сайту підприємства);

– матеріальні збитки (крадіжка обладнання, обслуговуючого систему *B2B* послуг).

3. Шкала

Визначимо шкалу, яку будемо використовуватися в організації. Як правило, використовується будь-яке число рівнів от 3 (наприклад, низький, середній і високий) до 10 відповідно до обраного організацією підходом, для процесу оцінки ризику.

Освітня організація в силу свого роду діяльності може встановити свої межі цінності активів, такі як «високий», «середній», «низький». Ці межі оцінюватися відповідно до обраних критеріїв (для можливих фінансових втрат межі повинні бути вказані в грошовому вираженні, при розгляді загрози особистої безпеки, визначити грошову цінність може бути важко і неприйнятно). Рішення, що вважати незначними або серйозними наслідками, повністю залежить від організації.

Для системи *B2B* послуг виберемо шкалу цінності активу від 0 до 4.

4. Залежності

Чим більш значимі і численні бізнеси-процеси підтримуються активом, тим найбільша цінність цього активу. Повинна бути також визначена

залежність одних активів від інших, оскільки це може впливати на цінність активів.

Інформація про залежності допоможе у визначенні загроз і особливо в виявленні вразливостей. Крім того, це допоможе забезпечити правильне присвоєння значення цінності активів (завдяки залежним взаємозв'язкам), показуючи, яким чином, відповідний рівень захисту.

Цінність активів, від яких залежать інші активи, може змінюватися таким чином:

– якщо цінність залежних активів (наприклад, даних) нижче або дорівнює цінності розглянутого активу (наприклад, програмного забезпечення), його цінність залишається такою ж;

– якщо цінність залежних активів (наприклад, даних) вище цінності розглянутого активу (наприклад, програмного забезпечення), його цінність повинна бути збільшена відповідно до ступеня залежності або цінністю інших активів.

5. Результат

Остаточним результатом цього кроку буде перелік активів і їх цінності по відношенню до модифікації (збереження цілісності, автентичності, неспростовності і облікових) розкриття (збереження конфіденційності), руйнування і недоступності (збереження надійності та доступності) і відновної вартості.

Визначення загроз і джерел загроз (Схема 5, рис. 2.7).

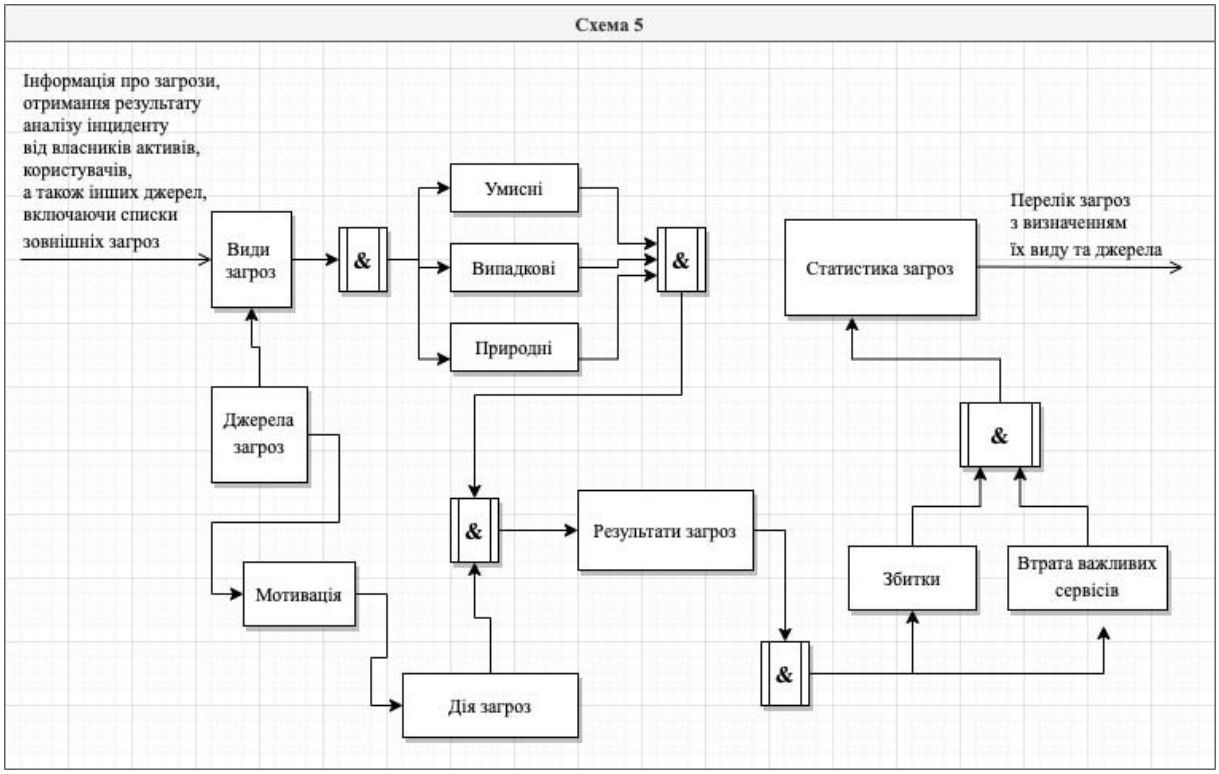

Рисунок 2.7 – Визначення загроз та їх джерел

Вхідні дані. Інформація про загрози, яка отримана в результаті аналізу інциденту від власників активів, користувачів системи і з інших джерел, в тому числі і списки зовнішніх загроз.

Дія. Загрози і їх джерела повинні бути визначені.

Керівництво по реалізації. Загроза може завдати шкоди активам організації, таким як інформація, процеси і системи.

Загрози можуть бути навмисними, випадковими або пов'язаними з зовнішнім середовищем (природними) і можуть в результаті представляти збиток або втрату важливих сервісів.

Необхідно встановити випадкові, навмисні, природні джерела загроз. Загрози можуть виходити як з самої організації, так і з джерела поза її меж. Загрози повинні визначатися і в загальному і по виду (це можуть бути фізичні збитки, неавторизовані дії, технічні збої), а потім, де це можливо, окремі загрози визначаються всередині родового класу. Деякі загрози можуть впливати більш ніж на один актив. У цих випадках вони можуть

бути причиною різних впливів в залежності від того, які активи виявляються схильні до дії.

Вхідні дані для визначення і кількісної оцінки ймовірності виникнення загроз можуть бути отримані від власників активів або керівництва організації, користувачів, персоналу відділу кадрів, фахівців в області ІБ, фахівців юридичного відділу, експертів в галузі фізичної безпеки, та інших підрозділів, а також від метеорологічних служб , юридичних організацій, національних урядових установ, страхових компаній. В ході аналізу загроз потрібно враховувати аспекти середовища і культури.

Списки загроз і їх статистику можна отримати від уряду, промислових підприємств, страхових компаній, юридичних організацій, і т.д.

Вихідні дані етапу визначення загроз і джерел загроз. Перелік загроз з визначенням їх виду і джерела.

В процесі оцінки загроз в системі *B2B* послуг отримано перелік загроз систематизований за видами загроз і наведений в таблиці 2.2.

Для кожної загрози вказується її походження: «П» (природна) «У» (умисна), «В» (випадкова), загроза.

– «П» позначає всі інциденти, які базуються на діях персоналу.

– «У» позначає все умисні дії, спрямовані на інформаційні активи.

– «В» позначає всі дії персоналу, які можуть випадково нанести шкоду інформаційних активів.

Загрози перераховуються не в пріоритетному порядку.

Таблиця 2.2

Перелік загроз системі *B2B* послуг

Вид	**Загрози**	**Походження**
Фізичні збитки	Пожежа	В, У, П
	Збитки, завдані водою	В, У, П
	Руйнування обладнання чи носіїв	В, У, П
	Пил, корозія, замерзання	В, У, П
Природні явища	Кліматичне явище	П

	Метеорологічне явище	П
Втрата важливих сервісів	Аварія системи кондиціювання повітря чи водопостачання	В, У
	Порушення енергопостачання	В, У, П
	Відмова телекомунікаційного обладнання	В, У
Перешкоди внаслідок випромінювання	Електромагнітне випромінювання	В, У, П
	Теплове випромінювання	В, У, П
	Електромагнітні імпульси	В, У, П
Компрометація інформації	Перехоплення компрометуючих сигналів перешкод	У
	Крадіжка носіїв чи документів	У
	Крадіжка обладнання	У
	Розкриття	В, У
	Дані з ненадійних джерел	В, У
	Злочинне використання апаратних засобів	У
	Злочинне використання програмного забезпечення	В, У
	Визначення місцезнаходження	У
Технічні несправності	Відмова обладнання	В
	Несправна робота обладнання	В
	Насичення інформаційної системи	В, У
	Порушення функціонування програмного забезпечення	В
	Порушення супроводу інформаційної системи	В, У
Несанкціоновані дії	Несанкціоноване використання обладнання	У
	Шахрайське копіювання програмного забезпечення	У
	Використання контрафактного або скопійованого програмного забезпечення	В, У
	Спотворення даних	У
	Незаконна обробка даних	У
Компрометація функцій	Помилка при використанні	В
	Зловживання правами	В, У
	Фальсифікація прав	У
	Відмова у здійсненні дій	У
	Порушення працездатності персоналу	В, У, П

Джерела загроз, що походять від діяльності людини.

Таблиця 2.3

Джерела загрози системі *B2B* послуг

Джерело загрози	Мотивація	Дія загрози
Хакер, зломщик	Виклик Зарозумілість Бунтарство Статус Гроші	Хакерство Соціальна інженерія Проникнення в систему, злом Несанкціонований доступ до системи
Особа, яка вчиняє комп'ютерний злочин	Руйнування інформації Незаконне розкриття інформації Грошова вигода Несанкціонована зміна даних	Комп'ютерний злочин (комп'ютерне переслідування та ін. дії) Шахрайська діяльність (відтворення, видача себе за іншого, перехоплення та ін. дії) Інформаційний підкуп Отримання доступу обманним шляхом Проникнення в систему
Терорист	Шантаж Руйнування Використання в особистих інтересах Помста Політична вигода	Вибух/Тероризм Інформаційна війна Системна атака (розподілена відмова в обслуговуванні, DoS-атаки та ін. дії) Проникнення в систему Псування системи
Промисловий шпигунство (відомості секретного характеру компанії)	Конкурентна перевага Економічний шпигунство	Отримання інформаційної переваги Економічна експлуатація Розкрадання інформації Замах на недоторканність особистого життя Соціальна інженерія Проникнення в систему Несанкціонований доступ до системи (доступ до секретної інформації, що є власністю фірми та/або пов'язаної з технологією)
Інсайдери (погано навчені, незадоволені, зловмисні, безтурботні, нечесні чи звільнені службовці)	Цікавість Зарозумілість Розвідка Грошова вигода Помста Ненавмисні помилки та упущення (наприклад, помилка введення даних, помилка у складанні програми)	Напад на службовця Шантаж Перегляд інформації, що є власністю фірми Неправильне використання комп'ютера Шахрайство та розкрадання Інформаційний підкуп Шкідливе програмне забезпечення (наприклад, вірус, логічна бомба, Троянський кінь) Продаж інформації особистого характеру «Жучки» у системі Проникнення в систему Шкідництво у системі Несанкціонований доступ до системи

Визначення існуючих заходів і засобів контролю та управління (Схема 6, рис. 2.8).

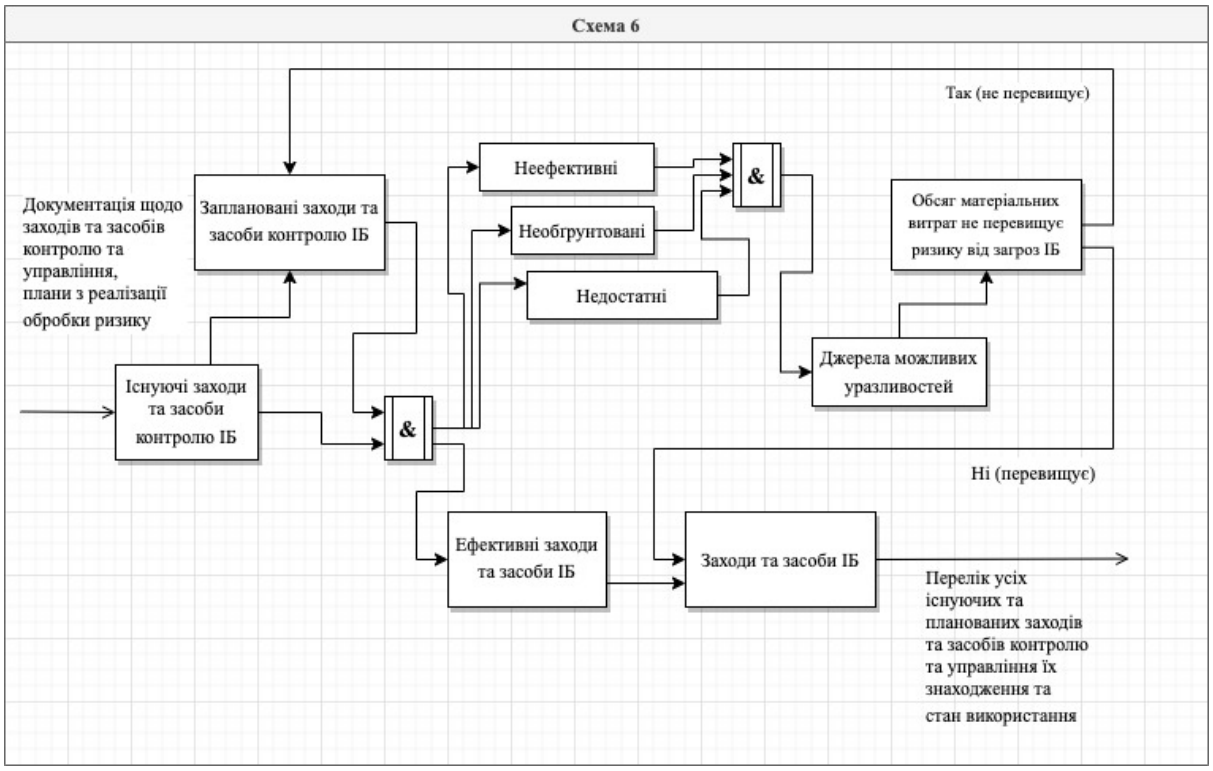

Рисунок 2.8 – Визначення існуючих заходів і засобів контролю та управління

Вхідні дані. Документація по заходам і засобам контролю і управління та плани по реалізації обробки ризику.

Дія. Визначаються існуючі та заплановані заходи і засоби контролю і управління.

Керівництво по реалізації. Щоб уникнути зайвої роботи або витрат, наприклад, при дублюванні заходів і засобів контролю та управління, необхідно визначити існуючі заходи і засоби контролю і управління. Крім цього, при визначенні існуючих заходів і засобів контролю та управління необхідно провести перевірку, щоб переконатися в правильності функціонування заходів і засобів контролю та управління – процедура звернення до існуючих звітів по аудиту системи моніторингу ІБ повинна скорочувати час, що витрачається на вирішення цього завдання. Неналежне

функціонування засобів і заходів управління і контролю може стати причиною вразливості.

Один із способів кількісної оцінки дії засобів і заходів управління та контролю – виявити, те як знижується ймовірність виникнення загрози, утруднюється використання уразливості і можливості впливу інциденту. Перевірки, проведені керівництвом, і звіти по аудиту також забезпечують інформацію про ефективність існуючих заходів і засобів контролю та управління.

Існуючі або плановані заходи і засоби контролю і управління можуть бути віднесені до розряду неефективних, недостатніх або необґрунтованих. Якщо їх віднесли до необґрунтованих або недостатнім, засіб і міру контролю і управління необхідно піддати перевірці, щоб визначити, чи підлягають вони заміні більш придатними, видалення, або можливо варто залишити їх через вартість.

Вихідні дані. Перелік всіх існуючих і планованих заходів і засобів контролю та управління, їх знаходження і стан використання.

Заходи і засоби контролю і управління забезпечення ІБ системи *B2B* послуг:

– документування процесів менеджменту ІБ з метою доступності інформації про всі існуючі або плановані заходи і засоби контролю і управління, а також про стан їх реалізації.

– регулярний аналіз документів, що містять інформацію про засоби контролю і управління в тому числі планів обробки ризиків.

– перевірки, що проводяться спільно з співробітниками, що відповідають за ІБ (представником адміністрації, співробітником забезпечує ІБ в цілому, співробітником, відповідальним за безпеку програмної системи, охороною офісу будівлі, представниками адміністрації та представниками користувачів системи);

– регулярний обхід будівлі і огляд фізичних засобів контролю, порівняння існуючих засобів контролю з документованим списком засобів, перевірка існуючих засобів контролю на їх правильну і ефективну роботу;

– аналіз результатів внутрішніх аудитів.

Виявлення вразливостей інформаційної безпеки (Схема 7, рис. 2.9).

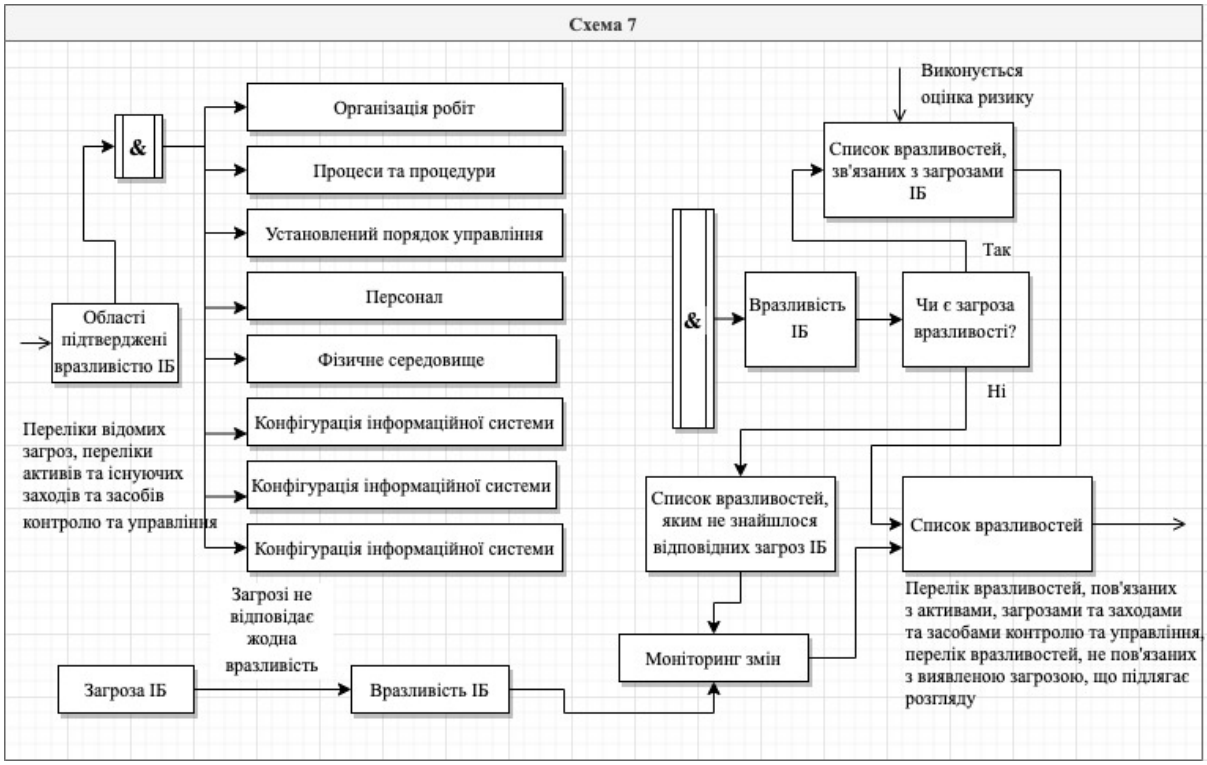

Рисунок 2.9 – Виявлення вразливостей інформаційної безпеки

Вхідні дані. Переліки відомих загроз, переліки активів і існуючих заходів і засобів контролю та управління.

Дія. Необхідно виявити уразливості, які можуть бути використані загрозами для нанесення шкоди активам або організації.

Керівництво по реалізації. Уразливості можуть бути виявлені в наступних областях:

– організація робіт;

– сталий порядок управління;

– процеси і процедури;

– персонал;

– конфігурація інформаційної системи;

– фізичне середовище;

– апаратні засоби, програмне забезпечення та апаратура зв'язку;

– залежність від зовнішніх сторін.

Наявність уразливості не завдає шкоди саме по собі, так як необхідна наявність загрози, яка зможе скористатися вразливістю. Для уразливості, якої не відповідає певна загроза, може не знадобитися впровадження засобів контролю та управління, але вона повинна усвідомлювати, враховуватися і піддаватися моніторингу на предмет змін. З іншого боку, загроза, якої не відповідає певна вразливість, може не призводити до ризику. Невірно реалізоване, неправильно використовується, неправильно функціонує засіб управління і контролю саме може стати причиною вразливості. Ефективність або неефективність заходів і засобів управління і контролю може залежати від середовища, в якій вони функціонують.

Уразливості можуть бути пов'язані з властивостями активу, так як спосіб і цілі використання активу в процесі надання *B2B* послуги можуть відрізнятися від планованих при придбанні або створенні активу. Потрібно враховувати уразливості, що виникають з різних джерел, і які є зовнішніми і внутрішні по відношенню до активу.

Вихідні дані. Перелік вразливостей, пов'язаних з активами, загрозами і заходами і засобами контролю і управління; перелік вразливостей, які пов'язані з виявленою загрозою, що підлягає розгляду.

Уразливості і методи оцінки вразливості для системи B2B послуг представлено в табл. 2.4.

Таблиця 2.4

Уразливості ІБ і відповідні їм загрози для системи B2B послуг

Вид	Вразливості ІБ	Загрози ІБ
Апаратні засоби	Недостатнє технічне обслуговування/неправильне встановлення носіїв даних	Порушення ремонтопридатності інформаційних систем
	Відсутність програм періодичної заміни	Погіршення стану носіїв даних
	Чутливість до вологості, пилу, забруднення	Утворення пилу, корозія, замерзання
	Чутливість до електромагнітного випромінювання	Електромагнітне випромінювання
	Відсутність ефективного контролю змін конфігурації	Помилка використання
	Чутливість до коливань напруги	Втрата електроживлення
	Чутливість до коливань температури	Метеорологічні явища
	Незахищене зберігання	Розкрадання носіїв даних чи документів
	Недбале (безвідповідальне) розміщення	Розкрадання носіїв даних чи документів
	Неконтрольоване копіювання	Розкрадання носіїв даних чи документів
Програмні засоби	Відсутнє чи недостатнє тестування програмних засобів	Зловживання правами
	Широко відомі дефекти програмних засобів	Зловживання правами
	Відсутність «завершення сеансу» при виході з робочого місця	Зловживання правами
	Списання чи повторне використання носіїв даних без належного видалення інформації	Зловживання правами
	Відсутність «слідів» аудиту	Зловживання правами
	Неправильний розподіл прав доступу	Зловживання правами
	Широко розподілене програмне забезпечення	Псування даних
	Застосування прикладних програм для невідповідних, з погляду часу, даних	Псування даних
	Складний інтерфейс користувача	Помилка використання
	Відсутність документації	Помилка використання
	Неправильні установки	Помилка використання
	Неправильні дані	Помилка використання
	Відсутність механізмів ідентифікації та аутентифікації, таких як аутентифікація користувачів	Фальсифікація прав
	Незахищені таблиці паролів	Фальсифікація прав
	Поганий менеджмент паролів	Фальсифікація прав
	Активізація непотрібних сервісів	Нелегальна обробка даних

Продовження табл. 2.4

	Недопрацьоване або нове програмне забезпечення	Збій програмних засобів
	Нечіткі чи неповні специфікації для розробників	Збій програмних засобів
	Відсутність ефективного контролю змін	Збій програмних засобів
	Неконтрольоване завантаження та використання програмних засобів	Таємні дії із програмними засобами
	Відсутність резервних копій	Таємні дії із програмними засобами
	Відсутність фізичного захисту будівлі, дверей та вікон	Розкрадання носіїв даних чи документів
	Відмова у забезпеченні звітів з менеджменту	Неавторизоване використання обладнання
Мережа	Відсутність підтвердження надсилання або отримання повідомлення	Відмова у здійсненні дій
	Незахищені лінії зв'язку	Перехоплення інформації
	Незахищений чутливий трафік	Перехоплення інформації
	Погане розведення кабелів	Відмова телекомунікаційного обладнання
	Єдина точка відмови	Відмова телекомунікаційного обладнання
	Відсутність ідентифікації та автентифікації відправника та одержувача	Фальсифікація прав
	Ненадійна мережева архітектура	Дистанційний шпигунство
	Передача паролів у незашифрованому вигляді	Дистанційний шпигунство
	Неадекватний мережевий менеджмент (стійкість маршрутизації)	Насичення інформаційної системи
	Незахищені з'єднання мережі загального користування	Неавторизоване використання обладнання
Персонал	Відсутність персоналу	Порушення працездатності персоналу
	Неадекватні процедури набору персоналу	Руйнування обладнання або носіїв даних
	Недостатнє усвідомлення безпеки	Помилка використання
	Неналежне використання програмних та апаратних засобів	Помилка використання
	Відсутність поінформованості про безпеку	Помилка використання

Продовження табл. 2.4

	Відсутність механізмів моніторингу	Нелегальна обробка даних
	Бездоглядна робота зовнішнього персоналу чи персоналу організації, що займається прибиранням	Розкрадання носіїв даних чи документів
	Відсутність політик щодо правильного використання телекомунікаційного середовища та обміну повідомленнями	Неавторизоване використання обладнання
Місце функціонування організації	Неадекватне або недбале використання фізичного управління доступом до будівель та приміщень	Погіршення стану носіїв даних
	Розміщення в місцевості, схильній до повеней	Затоплення
	Нестабільна електрична мережа	Відсутність електроживлення
	Відсутність фізичного захисту будівлі, дверей та вікон	Викрадення апаратури
Організація	Організація	Організація
	Відсутність формальної процедури для реєстрації та зняття з реєстрації користувачів	Відсутність формальної процедури для реєстрації та зняття з реєстрації користувачів
	Зловживання правами	Зловживання правами
	Відсутність формального процесу для перегляду (нагляду) прав доступу	Відсутність формального процесу для перегляду (нагляду) прав доступу
	Зловживання правами	Зловживання правами
	Відсутність або недостатні умови (що стосуються безпеки) у договорах з клієнтами та/або третіми сторонами	Відсутність або недостатні умови (що стосуються безпеки) у договорах з клієнтами та/або третіми сторонами
	Зловживання правами	Зловживання правами
	Відсутність процедури щодо моніторингу засобів обробки інформації	Відсутність процедури щодо моніторингу засобів обробки інформації
	Зловживання правами	Зловживання правами
	Відсутність регулярних аудитів (нагляду)	Відсутність регулярних аудитів (нагляду)
	Зловживання правами	Зловживання правами
	Відсутність процедур ідентифікації та оцінки ризику	Відсутність процедур ідентифікації та оцінки ризику
	Зловживання правами	Зловживання правами

Продовження табл. 2.4

	Відсутність повідомлень про помилки, зафіксовані в журналі реєстрації адміністратора та оператора	Відсутність повідомлень про помилки, зафіксовані в журналі реєстрації адміністратора та оператора
	Зловживання правами	Зловживання правами
	Неадекватна відповідальність за технічне обслуговування	Неадекватна відповідальність за технічне обслуговування
	Порушення обслуговування інформаційної системи	Порушення обслуговування інформаційної системи
	Відсутня чи незадовільна угода про рівень сервісу	Відсутня чи незадовільна угода про рівень сервісу
	Порушення обслуговування інформаційної системи	Порушення обслуговування інформаційної системи
	Відсутність процедури контролю змін	Відсутність процедури контролю змін
	Порушення обслуговування інформаційної системи	Порушення обслуговування інформаційної системи
	Відсутність формальної процедури контролю документації щодо системи менеджменту ІБ	Відсутність формальної процедури контролю документації щодо системи менеджменту ІБ
	Псування даних	Псування даних
	Відсутність формальної процедури нагляду за записами системи управління ІБ	Відсутність формальної процедури нагляду за записами системи управління ІБ
	Псування даних	Псування даних
	Відсутність формального процесу санкціонування загальнодоступної інформації	Відсутність формального процесу санкціонування загальнодоступної інформації
	Дані з ненадійних джерел	Дані з ненадійних джерел
	Відсутність належного розподілу обов'язків щодо забезпечення інформаційної безпеки	Відсутність належного розподілу обов'язків щодо забезпечення інформаційної безпеки
	Відмова у провадженні діяльності	Відмова у провадженні діяльності
	Відсутність планів забезпечення безперервності бізнесу	Відсутність планів забезпечення безперервності бізнесу

Визначення наслідків для активів (Схема 8, рис. 2.10).

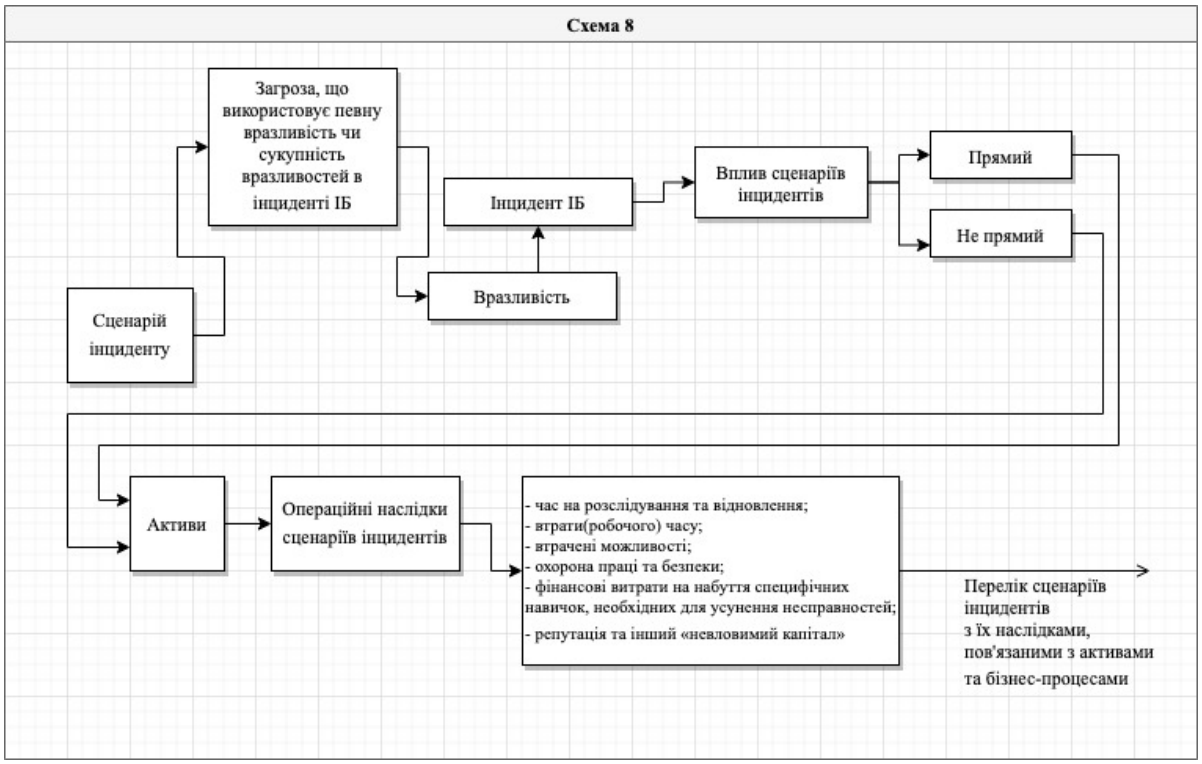

Рисунок 2.10 – Визначення наслідків

Вхідні дані. Перелік активів, бізнес-процесів, загроз і вразливостей, де це доречно, пов'язаних з активами, і їхню соціальну значимість.

Дія. Повинні бути визначені наслідки для активів, викликані втратою конфіденційності, цілісності та доступності.

Керівництво по реалізації. Наслідком може бути зниження ефективності, несприятливі операційні умови, втрата бізнесу, збиток, нанесений репутації і т.д.

Ця діяльність визначає збитки або наслідки для організації, які можуть бути обумовлені сценарієм інциденту. Сценарій інциденту – це опис загрози, використовує певну вразливість або сукупність вразливостей в інциденті інформаційної безпеки. Вплив сценаріїв інцидентів обумовлюється критеріями впливу, обумовленими в ході діяльності по встановленню контексту. Вплив може зачіпати один або кілька активів, а також частина активу. Тому активів може призначатися цінність,

обумовлена як їх фінансової вартістю, так і наслідками для бізнесу в разі їх псування або компрометації. Наслідки можуть бути тимчасовими або постійними, як це буває в разі руйнування активів.

Організації повинні визначати операційні наслідки сценаріїв інцидентів на основі (але не обмежуючись):

– часу на розслідування і відновлення;

– втрат (робочого) часу;

– втрачену можливість;

– охорони праці та безпеки;

– фінансові витрат на придбання специфічних навичок, необхідних для усунення несправності;

– репутації і іншого «невловимого капіталу».

Оцінка впливу. Інцидент ІБ може впливати більш ніж на один актив або тільки на частину активу. Вплив пов'язаний зі ступенем успішності інциденту. Як наслідок, існує суттєва відмінність між цінністю активу і впливом, що є результатом інциденту. Вплив розглядається як наявний або негайний (операційний) ефект, або майбутній (бізнес-) ефект, який включає фінансові та ринкові наслідки.

Безпосереднє (операційне) вплив буває прямим або непрямим.

Прямий вплив:

– фінансова відновна вартість втраченого активу (частини активу);

– вартість призупинених через інцидент операцій, поки послуга, що надається активом (активами), очікує відновлення;

– вартість придбання, конфігурації і установки нового активу або повна резервна копія;

– вплив призводить до порушення ІБ.

Непряме вплив:

– вартість перерваних операцій;

– витрати втрачених можливостей (фінансові ресурси, необхідних заміни або відновлення активу, могли бути використані будь-де);

– можливе зловживання інформацією, отриманою в результаті порушення безпеки;

– порушення етичних норм поведінки;

– порушення встановлених законом або нормативних зобов'язань.

Перша оцінка (без заходів і засобів контролю та управління будь-якого роду) оцінюватиме вплив як дуже близьке до цінності пов'язаного з цим активу або комбінації активів. При кожній наступній ітерації для цього (цих) активу (активів) вплив буде відрізнятися (зазвичай буде набагато нижче) внаслідок наявності і ефективності реалізованих заходів і засобів контролю та управління.

Вихідні дані. Перелік сценаріїв інцидентів з їх наслідками, пов'язаними з активами і бізнес-процесами (табл. 2.5)

Таблиця 2.5

Перелік сценаріїв інцидентів з їх наслідками, пов'язаними з активами і бізнес-процесами.

Список сценаріїв інцидентів	**Загроза, яка використовує цю вразливість**	**Уразливість**	**Активи та бізнес-процеси**	**Операційні наслідки сценаріїв**
З обладнанням	Порушення вимовної працездатності інформаційних систем	Недостатнє технічне обслуговування/неправильне встановлення носіїв інформації	Сервери, персональні електронні пристрої з доступом до мережі Інтернет.	- час для дослідження і відновлення; - втрата (робочого) часу; - втрачені можливості; - репутація та інший «нематеріальний капітал».
	Погіршення стану носіїв даних	Без програм періодичної заміни		
	Пилоутворення, корозія, замерзання	Чутливість до вологості, пилу, забруднення		
	Електромагнітне випромінювання	Чутливість до електромагнітного випромінювання		
	Помилка у використанні	Відсутність ефективного контролю над змінами конфігурації		
	Втрата електропостачання	Чутливість до коливань напруги		
	Метеорологічні явища	Чутливість до коливань температури		

Продовження табл. 2.5

	Крадіжка носіїв даних або документів	Незахищене сховище		
		Необережне (безвідповідальне) житло		
		Неконтрольоване копіювання		
Програмне забезпечення	Зловживання правами	Відсутнє або недостатнє тестування програмного забезпечення	Операційна система. Антивірусні інструменти. Програмне середовище для організації B2B послуг. Браузери та плагіни до них для доступу до середовища B2B послуг.	- час для дослідження і відновлення; - втрата (робочого) часу; - втрачені можливості; - охорона праці та безпека праці; - фінансові витрати на придбання специфічних навичок, необхідних для усунення несправностей; - репутація та інший «нематеріальний капітал».
		Відомі дефекти програмного забезпечення		
		Немає «закінчення сесії» при виході з робочого місця		
		Зняття з експлуатації або повторне використання носіїв даних без належного видалення інформації		
		Відсутність «слідів» аудиту		
		Неправильний розподіл прав доступу		
	Забруднення даних	Широко поширене програмне забезпечення		
		Застосування заявок на недостосівні дані, що не під час		
	Помилка у використанні	Складний інтерфейс користувача		
		Відсутність документації		
		Неправильні параметри установки		
		Неправильні дані		
	Фальсифікація прав	Відсутність механізмів ідентифікації та аутентифікації, таких як аутентифікація користувачів		
		Незабезпечені таблиці паролів		
		Погане керування паролями		
	Незаконна обробка даних	Активація непотрібних послуг		
	Збій програмного забезпечення	Незакінчене або нове програмне забезпечення		
		Незрозумілі або неповні специфікації для розробників		
		Відсутність ефективного контролю змін		
	Таємні дії з програмними інструментами	Безконтрольне завантаження та використання програмних засобів		
		Немає резервних копій		
	Крадіжка носіїв даних або документів	Відсутність фізичного захисту будівлі, дверей і вікон		
	Несанкціоноване використання обладнання	Відмова від надання управлінських звітів		

Продовження табл. 2.5

З мережею	Відмова від дій	Немає підтвердження надсилання або отримання повідомлення	Телекомунікаційні пристрої, що використовуються для підключення декількох фізично віддалених комп'ютерів або елементів інформаційної системи. Пристрої, які не є кінцевими, а проміжними пристроями зв'язку. Ретранслятори, мости, маршрутизатори, комутатори, маточини. Мережеве програмне забезпечення для управління та моніторингу активного мережевого обладнання. Генерація колод.	- час для дослідження і відновлення; - втрата (робочого) часу; - втрачені можливості; - охорона праці та безпека праці; - фінансові витрати на придбання специфічних навичок, необхідних для усунення несправностей; - репутація та інший "нематеріальний капітал".
	Перехоплення інформації	Незахищені лінії зв'язку		
		Незахищений конфіденційний трафік		
	Вихід з ладу телекомунікаційного обладнання	Бідні кабелі		
		Єдина точка невдачі		
	Фальсифікація прав	Відсутність ідентифікації та аутентифікації відправника та одержувача		
	Дистанційне шпигунство	Ненадійна мережева архітектура		
		Перенесення паролів у незашифрованому вигляді		
	Насиченість інформаційної системи	Недостатнє управління мережею (стабільність маршрутизації)		
	Несанкціоноване використання обладнання	Незахищені підключення до мережі загального користування		
З персоналом	Порушення роботи персоналу	Відсутність персоналу	Адміністрація організації, що здійснює B2B послуги. Начальник відділу кадрів, начальник фінансового відділу, керівник управління ризиками. Персонал для роботи та обслуговування інформаційної системи. Розробники програмних елементів середовища B2B послуг та сайту організації.	- втрата (робочого) часу; - втрачені можливості; - охорона праці та безпека праці; - фінансові витрати на придбання специфічних навичок, необхідних для усунення несправностей;
	Знищення обладнання або носіїв даних	Неадекватні процедури підбору персоналу		
	Помилка у використанні	Недостатня обізнаність про безпеку		
		Неправильне використання програмного та апаратного забезпечення		
		Недостатня обізнаність про безпеку		
	Незаконна обробка даних	Відсутність механізмів моніторингу		

Продовження табл. 2.5

	Крадіжка носіїв даних або документів	Безперешкодна робота зовнішнього персоналу або персоналу організації, що займається прибиранням		
	Несанкціоноване використання обладнання	Відсутність політики щодо належного використання телекомунікаційного середовища та обміну повідомленнями		
З місцем функціонування організації	Погіршення стану носіїв даних	Неадекватне або недбале використання фізичного контролю доступу до будівель і приміщень	Офіс і сервер. Зовнішній хостинг веб-сайтів. Віддалені точки доступу до системи B2B послуг.	- час для дослідження і відновлення; - втрата (робочого) часу; - охорона праці та безпека праці;
	Повені	Проживання в районі, схильному до затоплення		
	Немає джерела живлення	Нестабільна електрична мережа		
	Крадіжка обладнання	Відсутність фізичного захисту будівлі, дверей і вікон		
З організацією	Зловживання правами	Немає формальної процедури реєстрації та зняття з реєстрації користувачів	Організація, що надає B2B послуги. Структура організації: Адміністрація. Міністерство. Відділ маркетингу. IT-відділ. Бухгалтерський облік.	- час для дослідження і відновлення; - втрата (робочого) часу; - втрачені можливості; - охорона праці та безпека праці; - фінансові витрати на придбання специфічних навичок, необхідних для усунення несправностей; - репутація та інший "нематеріальний капітал".
		Немає формального процесу перегляду (нагляду) прав доступу		
		Відсутність або недостатні умови (щодо забезпечення) в договорах з клієнтами та/або третіми особами		
		Відсутність процедури моніторингу інструментів обробки інформації		
		Відсутність регулярних аудитів (нагляду)		
		Відсутність процедур ідентифікації та оцінки ризиків		
		У журналі адміністраторів і операторів не записано повідомлень про помилки		
	Порушення обслуговування інформаційних систем	Недостатня відповідальність за технічне обслуговування		
		Відсутня або незадовільні угоди про рівень обслуговування		
		Відсутність процедури контролю змін		
	Забруднення даних	Відсутність формальної процедури моніторингу документації, пов'язаної з системою управління інформаційною безпекою		

Продовження табл. 2.5

		Відсутність формальної процедури нагляду за записами системи управління інформаційною безпекою		
	Дані з ненадійних джерел	Немає формального процесу авторизації загальнодоступної інформації		
	Відмова від здійснення діяльності	Відсутність належного розподілу обов'язків із забезпечення інформаційної безпеки		
	Несправність обладнання	Відсутність планів безперервності бізнесу		
	Помилка у використанні	Немає політики електронної пошти		
		Відсутність процедур впровадження програмного забезпечення в операційні системи		
		Немає записів у журналі адміністраторів і операторів		
		Відсутність процедур обробки секретної інформації		
		Відсутність обов'язків з інформаційної безпеки в посадових інструкціях		
	Незаконна обробка даних	Відсутність або недостатні умови (що стосуються інформаційної безпеки) в договорах з працівниками		
	Крадіжка обладнання	Відсутність визначеного дисциплінарного процесу у разі інциденту з безпекою		
		Немає офіційної політики ноутбука		
		Відсутність контролю над активами за межами організації		
	Крадіжка носіїв або документів	Відсутня або незадовільні політики «чистий стіл і порожній екран» політика		
		Відсутність авторизації інструментів обробки інформації		
		Відсутність встановлених механізмів моніторингу порушень безпеки		
	Несанкціоноване використання обладнання	Відсутність регулярних перевірок, що проводяться керівництвом		
		Відсутність процедур для повідомлення про слабкі місця безпеки		
	Використання підробленого або скопійованого програмного забезпечення	Відсутність процедур забезпечення дотримання прав інтелектуальної власності		

2.3. Висновки до розділу 2

Наведено типові поди оцінки ризику організації на прикладі веб-ресурсу промислового підприємства. Встановлено, що процес менеджменту ризику ІБ складається з таких етапів: встановлення контексту; оцінки ризику; обробки ризику; прийняття ризику; комунікацій ризику; моніторингу та переоцінки ризику ІБ.

В процесі менеджменту ризику інформаційної безпеки виділено і деталізовано процес оцінки ризику інформаційної безпеки.

Встановлені основні критерії, сфера дії і кордони, структура процесу ризик-менеджменту інформаційної безпеки, прийняті для організації, що надає *B2B* послуги.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Встановлення значення ризику інформаційної безпеки

Методологія встановлення значення ризику може бути кількісної, якісної, комбінованої, залежно від обставин. Встановлення якісного значення часто використовується спочатку для отримання загальних відомостей про рівень ризику і виявлення основних значень ризиків. Пізніше може виникнути необхідність в здійсненні більш специфічного встановлення кількісного аналізу основних значень ризиків, оскільки зазвичай виконання якісного аналізу в порівнянні з кількісним є менш складним і витратним.

Для встановлення якісного значення використовується шкала кваліфікації атрибутів, за допомогою якої описуються величини можливих наслідків (наприклад, низький, середній і високий) і ймовірності виникнення цих наслідків. Перевага встановлення якісного значення полягає в доступності для розуміння всім відповідним персоналом, а недоліком – залежність від суб'єктивного вибору шкали.

Для встановлення кількісної оцінки використовується шкала з числовими значеннями (а не описові шкали, які використовуються при встановленні якісного значення) як наслідків, так і ймовірності, із застосуванням даних з різних джерел. Якість аналізу залежить від точності і повноти числових значень і від обґрунтованості використовуваних моделей. У більшості випадків для встановлення кількісного значення використовуються фактичні дані за минулий період.

Оцінка наслідків (Схема 9, рис. 3.1).

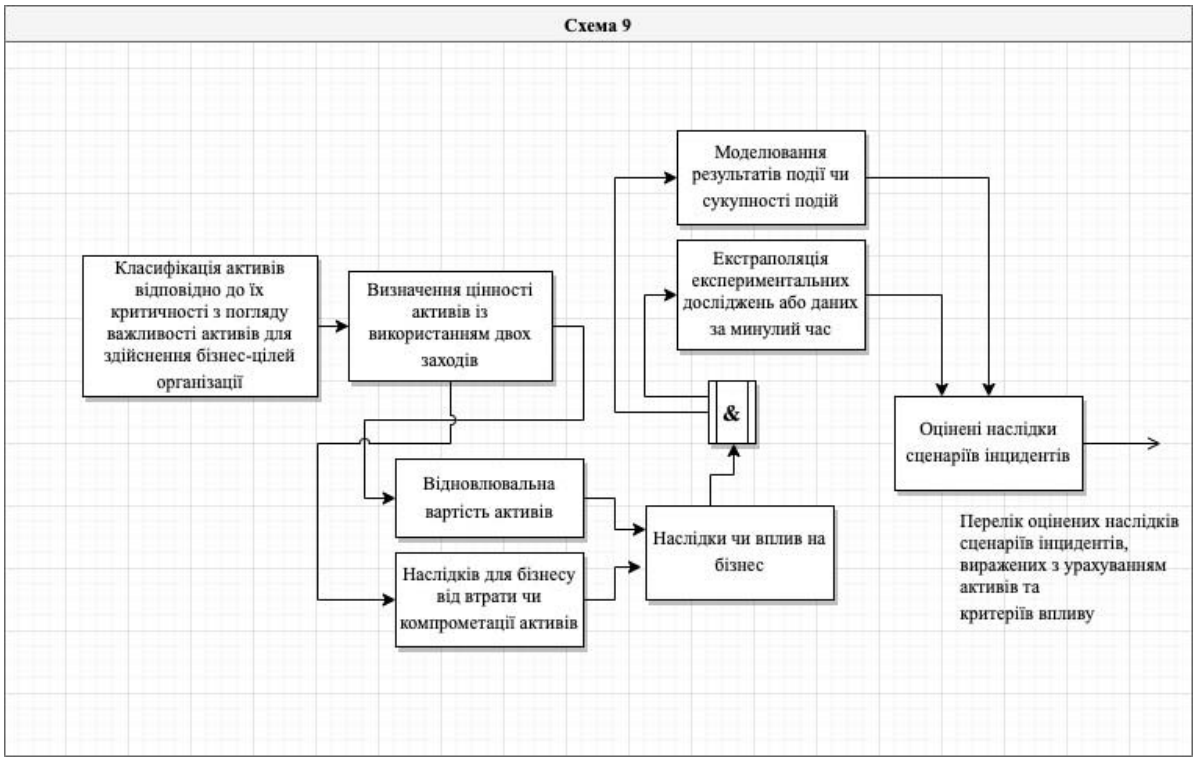

Рисунок 3.1 – Оцінка наслідків

Вхідні дані. Перелік певних значущих сценаріїв інцидентів, включаючи виявлення загроз, вразливостей і порушених активів, а також наслідків для активів і бізнес-процесів.

Дія. Повинно бути оцінено вплив на бізнес організації, яке може бути результатом передбачуваних або фактичних інцидентів ІБ з урахуванням наслідків порушення ІБ, таких, як втрата конфіденційності, цілісності або доступності активів.

Керівництво по реалізації. Після визначення всіх перевірених активів, привласнена їм цінність повинна враховуватися при оцінці наслідків.

Значення впливу на бізнес може бути виражено в якісній або кількісній формах.

Визначення цінності активів починається з класифікації активів відповідно до їх критичністю з точки зору важливості активів для

здійснення бізнес-цілей організації. Потім цінність активів визначається з використанням двох заходів:

– відновної вартості активу (вартості його очищення з метою відновлення і заміни інформації (якщо це можливо));

– наслідків для бізнесу від втрати або компрометації активу, наприклад можливі несприятливі наслідки для бізнесу та / або законодавчі або регулюють наслідки розкриття, модифікації, недоступності і / або руйнування інформації, а також інших інформаційних активів.

Це визначення цінності може бути встановлено на основі аналізу впливу на бізнес. Цінність, яка визначається наслідками для бізнесу, зазвичай значно вище просто відновної вартості і залежить від значущості активу для організації при виконанні її бізнес-цілей.

Визначення цінності активів є ключовим фактором оцінки впливу сценарію інциденту, оскільки інцидент може торкатися більш одного активу (наприклад, залежні активи), або тільки частина активу. Різні загрози і вразливості можуть мати різний вплив на активи, наприклад втрата конфіденційності, цілісності та доступності. Тому оцінка наслідків пов'язана з визначенням цінності активів або стає пов'язаної, виходячи з аналізу впливу на бізнес.

Наслідки або вплив на бізнес можуть визначатися шляхом моделювання результатів події або сукупності подій, екстраполяції експериментальних досліджень або даних за минулий час.

Наслідки можуть бути виражені за допомогою грошових, технічних персональних критеріїв впливу або інших критеріїв, які є значущими для організації. В окремих випадках для визначення наслідків, що розрізняються за часом, місцем, групам або ситуацій, потрібно більше одного цифрового значення.

Наслідки, що розрізняються за часом або фінансів, повинні вимірюватися з використанням того ж підходу, який застосовується щодо

ймовірності загрози і вразливості. Повинна підтримуватися послідовність кількісного або якісного підходу.

Вихідні дані. Перелік оцінених наслідків сценарію інцидентів, виражених з урахуванням активів і критеріїв впливу.

Таблиця 3.1

Кількісна оцінка наслідків сценарію інцидентів за шкалою від 0 до 4

Перелік сценаріїв інцидентів	**Оцінка наслідків сценарію інцидентів**
Інцидент з апаратними засобами	4
Інцидент із програмними засобами	4
Інцидент із мережею	3
Інцидент із персоналом	2
Інцидент із місцем функціонування організації	1
Інцидент із організацією	3

Оцінка ймовірності інциденту (Схема 10, рис. 3.2)

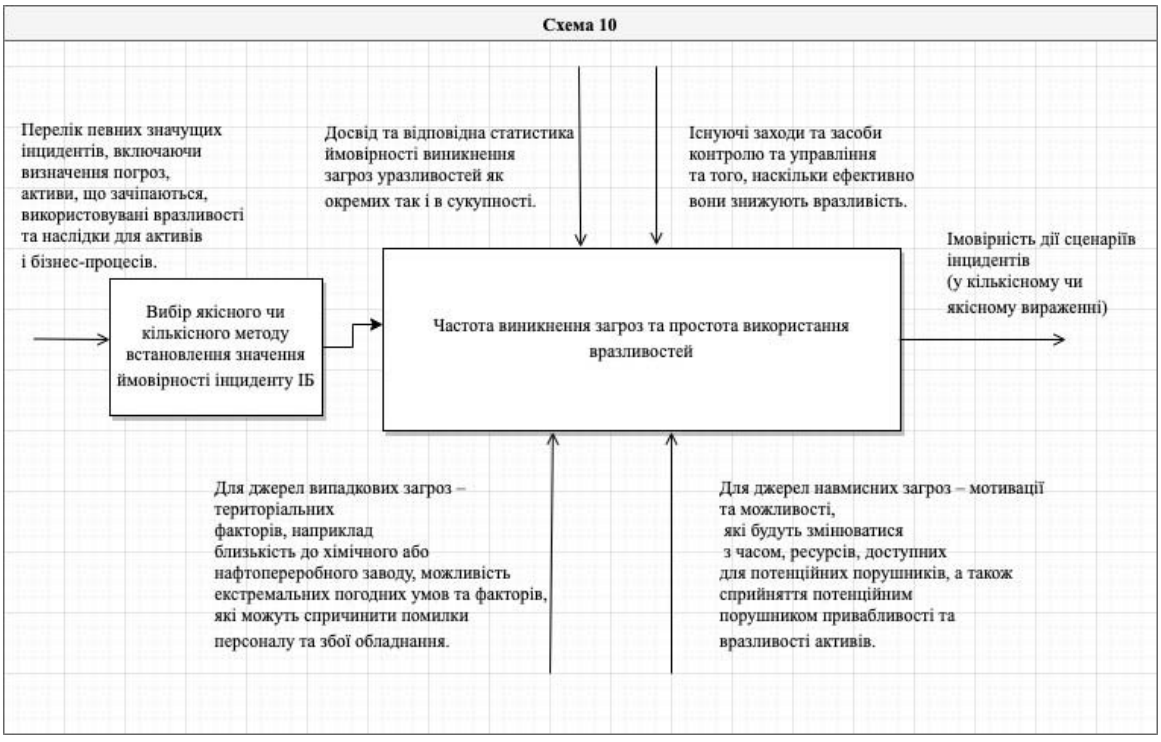

Рисунок 3.2 – Оцінка ймовірності інциденту

Вхідні дані. Перелік певних значущих сценаріїв інцидентів, включаючи визначення загроз, які поставлені активи, які використовуються уразливості і наслідки для активів і бізнес-процесів. Крім того, переліки всіх існуючих і планованих заходів і засобів контролю та управління, рівень їх ефективності, реалізації та використання.

Дія. Повинна бути оцінена ймовірність дії сценаріїв інцидентів.

Керівництво по реалізації. Після визначення сценаріїв інцидентів необхідно оцінити ймовірність дії кожного сценарію і його вплив з використанням якісного або кількісного методу встановлення значення. Необхідно брати до уваги частоту виникнення загроз і простоту використання уразливості, з урахуванням:

– для джерел умисних загроз (мотивації і можливості, які будуть змінюватися з плином часу, ресурсів, доступних для потенційних порушників, а також сприйняття потенційним порушником привабливості і уразливості активів);

– досвіду і відповідної статистики ймовірності виникнення загроз;

– для джерел випадкових загроз (територіальних чинників, наприклад близькість до хімічного або нафтопереробному заводу, можливість екстремальних погодних умов і факторів, які можуть викликати помилки персоналу і збої обладнання);

– існуючих заходів і засобів контролю та управління і того, наскільки ефективно вони знижують уразливості;

– вразливостей як окремих, так і в сукупності.

Залежно від необхідної точності активи можуть бути згруповані або розбиті на елементи, може виникати необхідність співвіднесення сценаріїв з елементами. Так, в залежності від місця розташування характер загроз щодо одних і тих же видів активів може змінюватися або відрізнятися ефективність існуючих заходів і засобів контролю та управління.

Вихідні дані. Імовірність дії сценаріїв інцидентів (в кількісному або якісному вираженні).

Таблиця 3.2

Оцінка ймовірності дій сценаріїв інцидентів за шкалою від 0 до 4

Перелік сценаріїв інцидентів	**Оцінка наслідків сценарію інцидентів**	**Імовірність дії сценаріїв інцидентів**
Інцидент з апаратними засобами	4	1
Інцидент із програмними засобами	4	2
Інцидент із мережею	3	3
Інцидент із персоналом	2	4
Інцидент із місцем функціонування організації	1	0
Інцидент із організацією	3	3

3.2. Встановлення значень рівня ризиків інформаційної безпеки

Встановлення значень рівня ризиків.

Вхідні дані. Перелік сценаріїв інцидентів з їх наслідками, що стосуються активів і бізнес-процесів, і їх вірогідність (в кількісному або якісному вираженні).

Дія. Повинні бути встановлені значення рівня ризиків для всіх значущих сценаріїв інцидентів.

Керівництво по реалізації. При встановленні значень ризиків присвоюються значення ймовірності виникнення ризику і його наслідків. Ці значення можуть бути виражені якісно або кількісно. Встановлення значень ризиків ґрунтується на оцінених наслідки і їх ймовірності. Крім того, воно може також враховувати вартість і ефективність, проблеми причетних сторін та інші змінні, використовувані при оцінці ризику. Задана ризику є комбінацією значень ймовірності сценарію інциденту і його наслідків.

Вихідні дані. Перелік ризиків з рівнями привласнених значень.

Високорівнева оцінка ризику інформаційної безпеки (Схема 11, рис. 3.3)

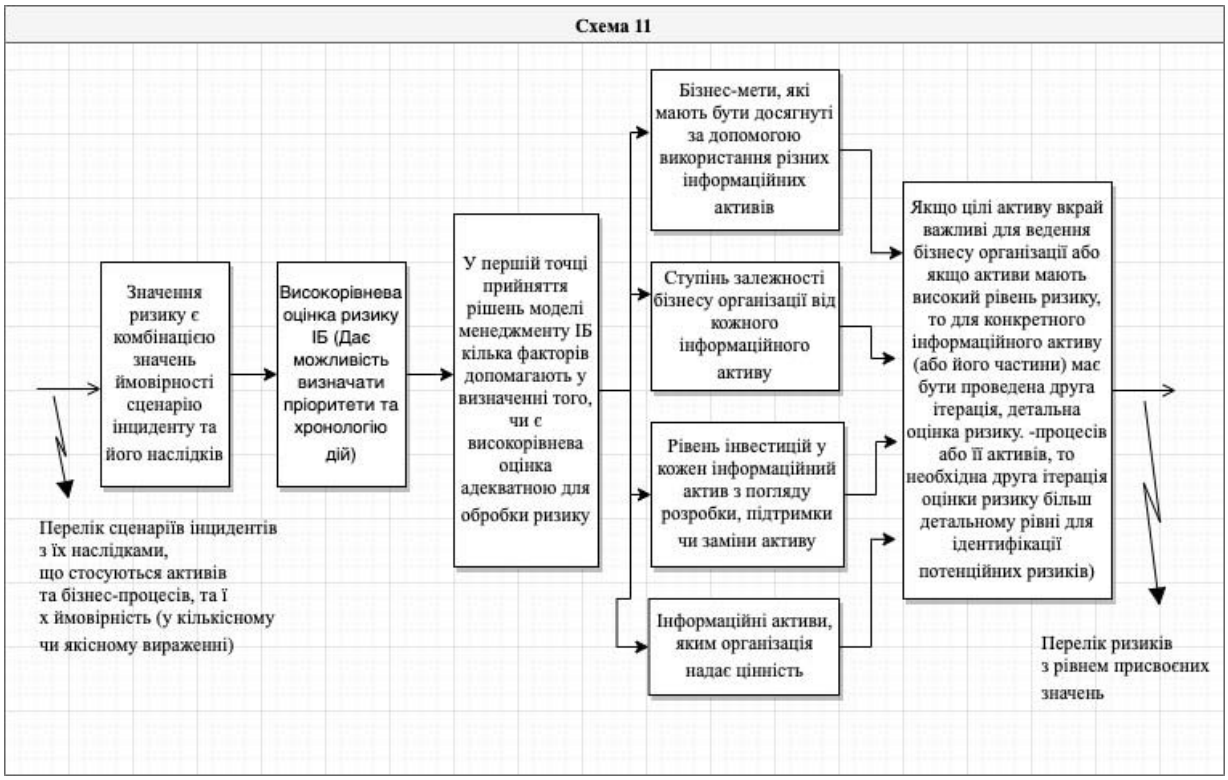

Рисунок 3.3 – Високорівнева оцінка ризику інформаційної безпеки

Високорівнева оцінка дає можливість визначати пріоритети і хронологію дій. З різних причин, наприклад, бюджетних, одночасна реалізація всіх заходів і засобів контролю та управління не завжди можлива, і за допомогою процесу обробки ризику можуть розглядатися тільки найбільш критичні ризики. Також може бути передчасним починати детальний менеджмент ризику, якщо реалізація передбачається тільки через рік або два. Для досягнення цієї мети високорівнева оцінка може початися з високорівневою оцінки наслідків, а не з систематичного аналізу загроз, вразливостей, активів і наслідків.

Причиною почати з високорівневою оцінки є синхронізація з іншими планами, пов'язаними з управлінням змінами (або забезпеченням безперервності бізнесу). Наприклад, не має сенсу забезпечувати повний

захист системи або додатку, якщо в найближчому майбутньому планується залучити для роботи з ними зовнішні ресурси, хоча, можливо, варто виконати оцінку ризику, щоб визначити доцільність укладення договору про залучення зовнішніх ресурсів.

При використанні високорівневою оцінки ризику розглядається цінність для бізнесу інформаційних активів і ризики з точки зору бізнесу організації. У першій точці прийняття рішення кілька факторів допомагають у визначенні того, чи є високорівнева оцінка адекватної для обробки ризику.

Цими факторами можуть бути:

– ступінь залежності бізнесу організації від кожного інформаційного активу (тобто, чи є функції, які організація вважає критичними для свого виживання або ефективного ведення бізнесу, що залежать від кожного активу або від конфіденційності, цілісності, доступності, неспростовності, облікових, автентичності та надійності інформації, що зберігається і оброблюваної в даному активі);

– бізнес-цілі, які повинні бути досягнуті за допомогою використання різних інформаційних активів;

– інформаційні активи, якими організація безпосередньо привласнює цінність;

– рівень інвестицій в кожен інформаційний актив з точки зору розробки, підтримки або заміни активу.

Якщо цілі активу вкрай важливі для ведення бізнесу організації або якщо активи мають високий рівень ризику, то для конкретного інформаційного активу (або його частини) повинна бути проведена друга ітерація, детальна оцінка ризику.

Тут застосовується таке загальне правило: якщо відсутність ІБ може привести до значних несприятливих наслідків для організації, її бізнес-

процесів або її активів, то необхідна друга ітерація оцінки ризику на більш детальному рівні для ідентифікації потенційних ризиків.

Детальна оцінка ризику інформаційної безпеки (Схема 12, рис. 3.4)

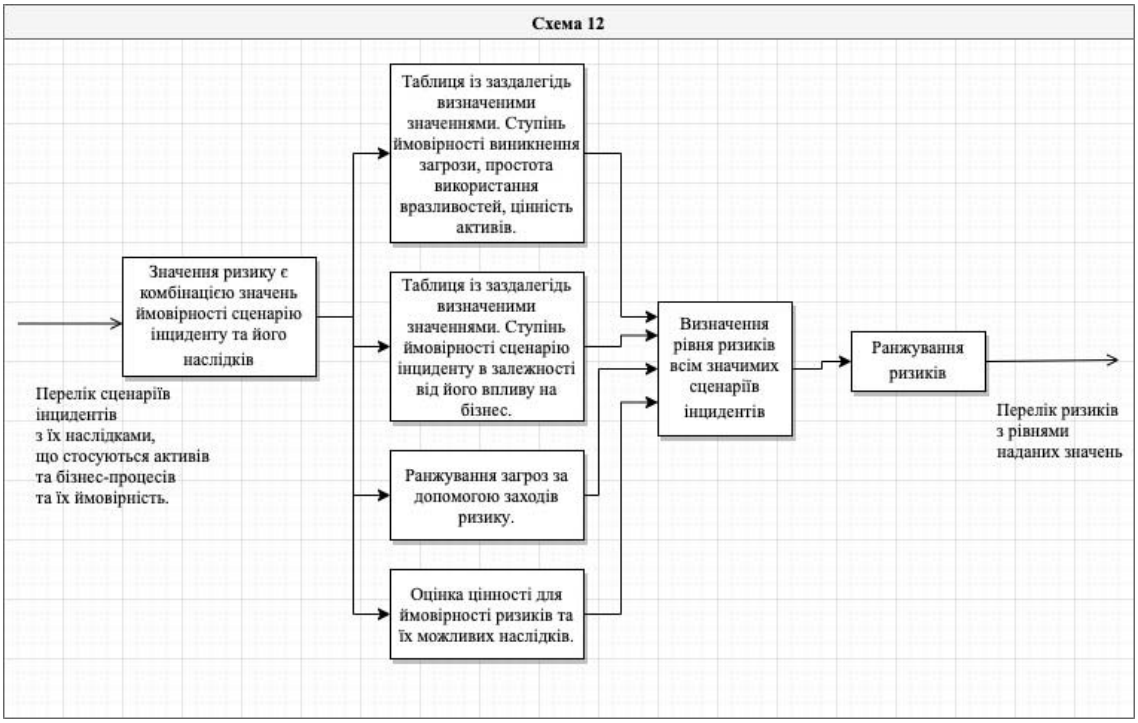

Рисунок 3.4 – Оцінка ризику інформаційної безпеки

Детальний процес оцінки ризику ІБ включає ретельне визначення і встановлення цінності активів, оцінку загроз цим активам та оцінку вразливостей. Результати цієї діяльності використовуються для оцінки ризиків, а потім для визначення способу обробки ризику.

Детальна послідовність дій зазвичай вимагає тривалого часу, значних зусиль і компетентності і тому може бути найбільш придатною для інформаційних систем з високим рівнем ризику.

Остаточним етапом детальної оцінки ризику ІБ є оцінка загальних ризиків, що знаходиться у фокусі цього додатка.

Наслідки можуть оцінюватися кількома методами, включаючи кількісні, наприклад грошові, і якісні заходи (з використанням таких

визначень, як «помірні» або «серйозні») або їх комбінації. Для оцінки ймовірності виникнення загрози повинні бути встановлені тимчасові рамки, в яких актив буде володіти цінністю або мати потребу в захисті.

На ймовірність виникнення конкретної загрози впливають такі чинники:

– простота перетворення активу, що використовує уразливість за винагороду, – може бути застосовано при розгляді умисної загрози з боку персоналу;

– привабливість активу або можливий вплив – може бути застосовано при розгляді умисної загрози з боку персоналу;

– чутливість уразливості до використання – можна застосувати до технічних і нетехнічних вразливостей;

– технічні можливості чинного фактора загрози – може бути застосовано при розгляді умисної загрози з боку персоналу.

У багатьох методах використовуються таблиці і об'єднуються суб'єктивні і емпіричні заходи. Важливо, щоб організація використовувала метод, який є для неї найбільш зручним, в якому організація впевнена і який буде забезпечувати повторюваність результатів.

1) Таблиця із заздалегідь визначеними значеннями

У методах оцінки ризику даного виду фактичні або передбачувані фізичні активи оцінюються з точки зору вартості заміни або відновлення (тобто кількісні заходи). Ця вартість потім переводиться в ту ж якісну шкалу, яка використовується для інформації. Фактичні або передбачувані програмні активи оцінюються таким же чином, як і фізичні активи, – визначається вартість придбання або відновлення, а потім переводиться в ту ж якісну шкалу, яка використовується для інформації. Крім того, якщо вважається, що будь-яка прикладна програма має власні притаманні їй вимоги щодо конфіденційності або цілісності (наприклад, якщо вихідний

текст програми сам по собі є комерційно критичним), вона оцінюється таким же чином, як і інформація.

Цінність інформації визначається з опитувань окремих представників бізнес-менеджменту (власників інформації), які можуть авторитетно судити про дані з метою визначення цінності і критичності фактично використовуваних даних або даних, які повинні зберігатися, оброблятися або оцінюватися. Опитування полегшують оцінку значущості та критичності інформації з точки зору сценаріїв найгірших варіантів, виникнення яких можна припускати виходячи з несприятливих наслідків для бізнесу, обумовлених несанкціонованим розкриттям, несанкціонованою модифікацією, недоступністю протягом різних періодів часу і руйнуванням.

Цінність визначається використанням принципів визначення цінності інформації, які охоплюють наступні проблеми:

– особиста безпека;

– юридичні та нормативні зобов'язання;

– особиста інформація;

– дотримання законів;

– фінансові втрати / порушення діяльності;

– комерційні та економічні інтереси;

– громадський порядок;

– втрата «невловимого капіталу»;

– політика і операції бізнесу;

– договір або угоду з клієнтом.

Принципи полегшують визначення значень цінності по числовий шкалою від 0 до 4, здійснюючи таким чином привласнення кількісних значень, якщо це можливо і обґрунтовано, і якісних значень там, де кількісні значення неможливі, наприклад в разі створення небезпеки для людського життя.

Наступним важливим етапом діяльності є заповнення ряду опитувальних листів для кожного виду загрози, кожної групи активів, з якою пов'язаний даний вид загрози, щоб уможливити оцінку рівнів загроз (ймовірності виникнення) і рівнів вразливостей (простоти використання погроз для створення несприятливих наслідків). Кожна відповідь на питання дає бали. Ці бали складаються з використанням бази знань і порівнюються з діапазонами. Це ідентифікує рівні загроз, наприклад, за шкалою від високого до низького і, аналогічно, рівні вразливостей (таблиця 3.3), з проведенням відмінностей між видами наслідків. Інформація для заповнення опитувальних листів повинна збиратися з опитувань технічного персоналу, представників відділу кадрів, з даних обстежень фактичного розташування і перевірки документації.

Цінність активів, рівні загроз і вразливостей, які стосуються кожному виду наслідків, наводяться в табличній формі (матриці), щоб для кожної комбінації ідентифікувати відповідну міру ризику на основі шкали від 0 до 8. Значення заносяться в матрицю структурованим чином.

Таблиця 3.3

Цінність активів, ймовірності виникнення загроз, рівні уразливості

Ступінь ймовірності виникнення загрози		**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)		Н	С	В	Н	С	В	Н	С	В
Цінність активів	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для кожного активу розглядаються доречні уразливості і відповідні їм загрози. Якщо існує вразливість без відповідної загрози або загроза без відповідної уразливості, то в даний час ризик відсутній (але слід вживати

заходів у разі зміни цієї ситуації). Відповідний рядок в таблиці 3.4-3.11 встановлюється за значенням цінності активу, а відповідна колонка встановлюється за ступенем ймовірності виникнення загрози і простоті використання. Наприклад, якщо актив має цінність 3, загроза є «високою», а уразливість «низькою», то міра ризику буде дорівнює 5. Припустимо, що актив має цінність 2 і, наприклад, для модифікації рівень загрози є «низьким», а простота використання «високою», тоді міра ризику буде дорівнювати 4.

Розмір таблиці з точки зору числа категорій ймовірності загроз, категорій простоти використання і числа категорій визначення цінності активів може бути адаптований до потреб організації.

Для додаткових заходів ризику будуть потрібні додаткові колонки і рядки.

Цінність даного підходу полягає в ранжируванні ризиків, які потребують розгляду.

Ступінь ймовірності виникнення загрози. Процес.

Таблиця 3.4

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	**Процес#**	0	0	1	2	1	2	3	2	3	4
	Процес реєстрації.#	1	1	2	3	2	3	4	3	4	5
	Процес формування контенту#	2	2	3	4	3	4	5	4	5	6
	Процес отримання матеріалів.#	3	3	4	5	4	5	6	5	6	7
	Процес надання консультаційних послуг.# Процес звітності.# Процеси маркетингу та обслуговування сайту та системи B2B послуг.#	4	4	5	6	5	6	7	6	7	8

Таблиця 3.5

Ступінь ймовірності виникнення загрози. Інформація

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	**Інформація#** Інформація про персональні дані користувачів та персоналу системи B2B послуг.# Інформація про фінансовий стан організації, яка надає B2B послуг.# Інформаційні ресурси бази даних.#	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблиця 3.6

Ступінь ймовірності виникнення загрози. Апаратні засоби

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	**Апаратні засоби** Сервери, персональні електронні пристрої з доступом до мережі Інтернет.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблиця 3.7

Ступінь ймовірності виникнення загрози. Програмні засоби

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	***Програмні засоби*** Операційна система. Антивірусні засоби. Програмне середовище для організації B2B послуг. Браузери та плагіни до них для доступу до середовища B2B послуг.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблиця 3.8

Ступінь ймовірності виникнення загрози.

Простота використання

Ступінь ймовірності виникнення загрози			Низька			Середня			Висока		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	***Мережа***	0	0	1	2	1	2	3	2	3	4
	Телекомунікаційні пристрої, які використовуються для з'єднання кількох фізично віддалених комп'ютерів чи елементів інформаційної системи.	1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8
	Пристрої, які є кінцевими, а проміжними пристроями зв'язку. Ретранслятори, мости, маршрутизатори, комутатори, концентратори.										
	Мережеве програмне забезпечення управління та моніторингу активного мережного обладнання. Генерація журналів реєстрації.										

Таблиця 3.9

Ступінь ймовірності виникнення загрози. Персонал

Ступінь ймовірності виникнення загрози			Низька			Середня			Висока		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	***Персонал***	0	0	1	2	1	2	3	2	3	4
	Адміністрація.	1	1	2	3	2	3	4	3	4	5
	Менеджери.	2	2	3	4	3	4	5	4	5	6
	Керівник відділу кадрів, керівник фінансового відділу, керівник здійснює менеджмент ризику.	3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8
	Персонал з експлуатації та супроводу інформаційної системи.										
	Розробники програмних елементів середовища та сайту організації.										
	Персонал з експлуатації та супроводу інформаційної системи.										
	Розробники програмних елементів.										

Таблиця 3.10

Ступінь ймовірності виникнення загрози. Місце функціонування організації

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	***Місце функціонування організації*** Офіс та серверна. Зовнішній хостинг сайту. Видалені точки доступу до системи B2B послуг.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблиця 3.11

Ступінь ймовірності виникнення загрози			**Низька**			**Середня**			**Висока**		
Простота використання (Рівень вразливості)			Н	С	В	Н	С	В	Н	С	В
Цінність активу	***Організація*** Організація, що надає освітні послуги. Структура організації: Адміністрація. Відділ маркетингу. IT-відділ. Бухгалтерія.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Ступеня ймовірності сценарію інциденту, відображеного на кількісно оцінене вплив бізнесу

Імовірність сценарію інциденту дана за допомогою загрози, що використовує уразливість з певною ймовірністю. Таблиця 3.12 відображає цю ймовірність впливу на бізнес, пов'язану зі сценарієм інциденту.

Одержуваний в результаті ризик вимірюється за шкалою від 0 до 8, може бути оцінений щодо критеріїв прийняття ризику. Дана шкала ризиків може також відображатися на простий спільний рейтинг ризиків, наприклад таким чином:

– низький ризик: 0-2;

– середній ризик: 3-5;

– високий ризик: 6-8.

Таблиця 3.12

Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес

	Ступінь ймовірності сценарію інциденту	**Дуже низька (дуже малоймовірна)**	**Низька (малоймовірна)**	**Середня (можлива)**	**Висока (імовірна)**	**Дуже висока (часта)**
Вплив на бізнес	Дуже низька	0	1	2	3	4
	Низьке	1	2	3	4	5
	Середнє	2	3	4	5	6
	Висока	3	4	5	6	7
	Дуже висока	4	5	6	7	8

Таблиця 3.13

Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес в системі B2B

Перелік сценаріїв інцидентів	**Перелік сценаріїв інцидентів**	**Перелік сценаріїв інцидентів**	**Перелік сценаріїв інцидентів**	**Перелік сценаріїв інцидентів**
Ступінь ймовірності сценарію інциденту	Ступінь ймовірності сценарію інциденту	Ступінь ймовірності сценарію інциденту	Ступінь ймовірності сценарію інциденту	Ступінь ймовірності сценарію інциденту
Вплив	Вплив	Вплив	Вплив	Вплив
на бізнес	на бізнес	на бізнес	на бізнес	на бізнес
Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес	Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес	Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес	Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес	Ступінь ймовірності сценарію інциденту в залежності від його впливу на бізнес
Простий загальний рейтинг ризиків	Простий загальний рейтинг ризиків	Простий загальний рейтинг ризиків	Простий загальний рейтинг ризиків	Простий загальний рейтинг ризиків
Інцидент з апаратними засобами	Інцидент з апаратними засобами	Інцидент з апаратними засобами	Інцидент з апаратними засобами	Інцидент з апаратними засобами

1) Ранжування загроз за допомогою заходів ризику

Для зв'язку факторів наслідків (цінність активів) з ймовірністю виникнення загрози (беручи до уваги аспекти уразливості) використовують таблицю 3.14. В якій перераховуються загрози (стовпець *a*), над якими виконуються наступні кроки:

– перший крок полягає в оцінці наслідків (цінності активів) за заздалегідь визначеною шкалою (визначимо значення шкали від 1 до 5), для кожного знаходиться під загрозою активу (стовпець «*b*»).

– другий крок полягає в оцінці ступеня ймовірності виникнення загрози за заздалегідь визначеною шкалою, наприклад від 1 до 5, для кожної загрози (стовпець «*c*»).

– третій крок полягає в обчисленні міри ризику (стовпець d) шляхом множення (*b*c*).

– четвертий крок ранжуємо (стовпець e) загрози в порядку відповідної міри ризику. Відзначимо, що «1» відповідає найменшим наслідків і найнижчою ступеня ймовірності виникнення.

Ця процедура, дозволяє зіставити і ранжувати в порядку призначених пріоритетів різні загрози з різними наслідками і ймовірністю виникнення. (В деяких випадках необхідно результати, отримані за емпіричними шкалами, представляти в грошовому вираженні.)

Таблиця 3.14

Ранжування загроз за допомогою заходів ризику

Ідентифікатор загрози (*a*)	**Наслідки (цінність активу) (*b*)**	**Ступінь ймовірності виникнення загрози (*c*)**	**Міра ризику (*d*)**	**Ранжування загроз (*e*)**
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1
Загроза D	1	3	3	5
Загроза E	4	1	4	4
Загроза F	2	4	8	3

Раніше виділені загрози ІБ (таблиця 3.15)

Таблиця 3.15

Загрози ІБ

Групи загроз	Загроза
З апаратними засобами	Порушення ремонтопридатності інформаційних систем
	Погіршення стану носіїв даних
	Утворення пилу, корозія, замерзання
	Електромагнітне випромінювання
	Помилка використання
	Втрата електроживлення
	Метеорологічні явища
	Розкрадання носіїв даних чи документів
З програмними засобами	Зловживання правами
	Псування даних
	Помилка використання
	Фальсифікація прав
	Нелегальна обробка даних
	Збій програмних засобів
	Таємні дії із програмними засобами
	Розкрадання носіїв даних чи документів
	Неавторизоване використання обладнання
З мережею	Відмова у здійсненні дій
	Перехоплення інформації
	Відмова телекомунікаційного обладнання
	Фальсифікація прав
	Дистанційний шпигунство
	Насичення інформаційної системи
	Неавторизоване використання обладнання
З персоналом	Порушення працездатності персоналу
	Руйнування обладнання або носіїв даних
	Помилка використання
	Нелегальна обробка даних
	Розкрадання носіїв даних чи документів
	Неавторизоване використання обладнання
З місцем функціонування організації	Погіршення стану носіїв даних
	Затоплення
	Відсутність електроживлення
	Викрадення апаратури
З організацією	Зловживання правами
	Порушення обслуговування інформаційної системи
	Псування даних
	Дані з ненадійних джерел
	Відмова у провадженні діяльності
	Відмова обладнання
	Помилка використання
	Нелегальна обробка даних
	Викрадення обладнання
	Розкрадання носіїв інформації чи документів
	Неавторизоване використання обладнання
	Використання контрафактних або копійованих програмних засобів

Таблиця 3.16

Вага груп загроз на ІБ

Перелік груп загроз	Ступінь ймовірності загрози	Вплив на бізнес (цінність активу)
З апаратними засобами	2 - Низька	5 - Дуже високий
З програмними засобами	3 - Середня	4 - Високий
З мережею	4 - Висока	4 - Високий
З персоналом	5 - Дуже висока	3 - Середній
З місцем функціонування організації	1 - Дуже низька	1 - Дуже низький
З організацією	3 - Середня	2 - Низький

Таблиця 3.17

Ідентифікатор загрози (*a*)	Наслідки (цінність активу) (*b*)	Ступінь ймовірності виникнення загрози (*c*)	міра ризику (*d*)	Ранжування загроз у порядку зменшення ступеня ризику від 1 (максимальний ризик) до 6 (мінімальний ризик) (e)
Загроза апаратним засобам	5	2	10	4
Загроза програмним засобам	4	3	12	3
Загроза мережі	4	4	16	1
Загроза персоналу	3	5	15	2
Загроза місцю функціонування організації	1	1	1	6
Загроза організації	2	3	6	5

2) Оцінка цінності для ймовірності ризиків і їх можливих наслідків

У цьому прикладі особлива увага приділяється наслідків інцидентів ІБ (сценаріями інцидентів) та визначенню того, яким системам слід віддавати перевагу. Це виконується шляхом оцінки двох значень - для кожного активу і ризику, комбінація яких буде визначати бали для кожного активу. Коли підсумовуються всі бали активів системи, визначається міра ризику для цієї системи.

Спочатку кожному активу присвоюється цінність. Це значення пов'язано з можливими несприятливими наслідками, які можуть виникати, якщо актив знаходиться під загрозою. Ця цінність присвоюється активу для кожного випадку виникнення відповідної активу загрози. Потім оцінюється значення ймовірності. Воно оцінюється виходячи з комбінації ступеня ймовірності виникнення загрози і простоти використання уразливості (див. таблицю 3.18, яка має ймовірність здійснення сценарію інцидентів).

Таблиця 3.18

Оцінка цінності для ступеня ймовірності та можливих наслідків ризиків

Рівні загрози	Низька			Середня			Висока		
Рівні вразливості	Н	С	В	Н	С	В	Н	С	В
Значення ступеня ймовірності	0	1	2	1	2	3	2	3	4

Потім, знаходячи перетин ліній значення цінності активу і значення ступеня ймовірності в таблиці 3.19, присвоюються бали активу / загрозі. Бали активу / загрози підраховуються, щоб отримати підсумкові бали для активу. Ця цифра може використовуватися для проведення відмінностей між активами, які складають частину системи.

Таблиця 3.19

Цінності активу і значення ступеня ймовірності

Значення ступеня ймовірності	**Цінність активу**				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Остаточний крок полягає в підрахунку всіх підсумкових балів активів системи, щоб отримати бали системи. Ця цифра може використовуватися

для проведення відмінностей між системами і визначення того, захисту якої системи слід віддавати перевагу.

Припустимо, що система С має три активи: *A1*, *A2* і *A3*. Також припустимо, що існують дві загрози *Z1* і *Z2*, застосовані до системи С. Нехай цінність активу *A1* буде 3, припустимо також, що цінність активу *A2* дорівнює 2, а цінність активу *A3* дорівнює 4.

Якщо для *A1* і *Z1* ступінь ймовірності загрози низька, а простота використання уразливості середня, то значення ступеня ймовірності дорівнює 1 (таблиця 3.18).

Бали для активу / загрози *A1* / *Z1* можуть бути виведені з таблиці 3.19 на перетині ліній цінності активу 3 і значення ступеня ймовірності 1, тобто рівні 4. Аналогічним чином, нехай для *A1* / *Z2* ступінь ймовірності загрози буде середньої, а простота використання уразливості буде високою, що дасть для *A1* / *Z2* значення 6.

Тепер можуть бути обчислені підсумкові бали активу *A1Z*, тобто рівні 10. Підсумкові бали активу обчислюються для кожного активу і застосовної загрози. Підсумкові бали системи обчислюються шляхом підсумовування *A1Z* + *A2Z* + *A3Z*, що дає *CZ*.

Різні системи можуть порівнюватися для встановлення пріоритетів, а також різних активів в межах однієї системи.

Активи системи *C*	**Цінність активів**
A1	3
A2	2
A3	4

Загрози системи С відповідні активу *A1*
Z1
Z2

Оцінка цінності для ступеня ймовірності та можливих наслідків ризиків для *A1* / *Z1*

Рівні загрози	Низька			Середня			Висока		
Рівні вразливості	Н	С	В	Н	С	В	Н	С	В
Значення ступеня ймовірності	0	1	2	1	2	3	2	3	4

Цінності активу і значення ступеня ймовірності для *A1* / *Z1*

Значення ступеня ймовірності	Цінність активу А1				
0	0	1	2	3	4
1	1	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Таким чином, *A1Z1* = 4

Для *A2 / Z2*

Рівні загрози	Низька			Середня			Висока		
Рівні вразливості	Н	С	В	Н	С	В	Н	С	В
Значення ступеня ймовірності	0	1	2	1	2	3	2	3	4

Для *A2/Z2*

Значення ступеня ймовірності	Цінність активу *A2*				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	**6**	7
4	4	5	6	7	8

Таким чином, *A2/Z2* = 6.

Підсумкові бали активу *A1* визначаються наступною сумою *A1Z = A1Z1 + A1Z2 = 10*

Міра ризику для всієї системи (підсистеми) – CZ буде обчислюватися так *CZ = A1Z + A2Z + A3Z.*

Наведені розрахунки застосовні як до інформаційних систем, так і до бізнес-процесів.

Отже розглянемо оцінку цінності для ймовірності ризиків і їх можливих наслідків, стосовно до системи B2B ТОВ «Южмаш груп».

З таблиці переліку сценарію інцидентів виберемо два поля активи і відповідні їм загрози (таблиця 3.20):

Таблиця 3.20

Сценарії інцидентів ТОВ «Южмаш груп»

Активи та бізнес процеси	**Загрози, що відповідають активу**
Апаратні засоби: (Актив *A1*) Сервери Персональні електронні пристрої з доступом до Інтернету.	Порушення ремонтопридатності інформаційних систем (Загроза *Z1-1*)
	Погіршення стану носіїв даних (Загроза *Z1-2*)
	Утворення пилу, корозія, замерзання (Загроза *Z1-3*)
	Електромагнітне випромінювання (Загроза *Z1-4*)
	Помилка використання (Загроза *Z1-5*)
	Втрата електроживлення (Загроза *Z1-6*)
	Метеорологічні явища (Загроза *Z1-7*)
	Викрадення носіїв даних або документів (Загроза *Z1-8*)
Програмні засоби: (Актив *A2*) Операційна система. Антивірусні засоби. Програмне середовище для організації B2B послуг. Браузери та плагіни до них для доступу до B2B послуг.	Зловживання правами (Загроза *Z2-1*)
	Псування даних (Загроза *Z2-2*)
	Помилка використання (Загроза *Z2-3*)
	Фальсифікація прав (Загроза *Z2-4*)
	Нелегальна обробка даних (Загроза *Z2-5*)
	Збій програмних засобів (Загроза *Z2-6*)
	Таємні дії з програмними засобами (Загроза *Z2-7*)
	Викрадення носіїв даних або документів (Загроза *Z2-8*)
	Неавторизоване використання обладнання (Загроза *Z2-9*)

Продовження табл. 3.20

Мережа: (Актив *А3*) Телекомунікаційні пристрої, які використовуються для з'єднання кількох фізично віддалених комп'ютерів чи елементів інформаційної системи. Ретранслятори, мости, маршрутизатори, комутатори, концентратори. Мережеве програмне забезпечення управління та моніторингу активного мережного обладнання. Генерація журналів реєстрації.	Відмова у здійсненні дій (Загроза *Z3-1*)
	Перехоплення інформації (Загроза *Z3-2*)
	Відмова телекомунікаційного обладнання (Загроза *Z3-3*)
	Фальсифікація прав (Загроза *Z3-4*)
	Дистанційний шпигунство (Загроза *Z3-5*)
	Насичення інформаційної системи (Загроза *Z3-6*)
	Неавторизоване використання обладнання (Загроза *Z3-7*)
Персонал: (Актив *А4*) Адміністрація організації,. Менеджери. Керівник відділу кадрів, керівник фінансового відділу, керівник здійснює менеджмент ризику. Персонал з експлуатації та супроводу інформаційної системи. Розробники програмних елементів середовища B2B послуг та сайту організації.	Порушення працездатності персоналу (Загроза *Z4-1*)
	Руйнування обладнання або носіїв даних (Загроза *Z4-2*)
	Помилка використання (Загроза *Z4-3*)
	Нелегальна обробка даних (Загроза *Z4-4*)
	Викрадення носіїв даних або документів (Загроза *Z4-5*)
	Неавторизоване використання обладнання (Загроза *Z4-6*)
Місце функціонування організації: (Актив *А5*) Офіс та серверна. Зовнішній хостинг сайту. Видалені точки доступу до системи B2B послуг.	Погіршення стану носіїв даних (Загроза *Z5*-1)
	Затоплення (Загроза *Z5*-2)
	Відсутність електроживлення (Загроза *Z5*-3)
	Викрадення апаратури (Загроза *Z5*-4)
Організація: (Актив *А6*) Організація. Структура організації: Адміністрація. Відділ маркетингу. IT-відділ. Бухгалтерія.	Зловживання правами (Загроза *Z6-1*)
	Порушення обслуговування інформаційної системи (Загроза *Z6-2*)
	Псування даних (Загроза *Z6-3*)
	Дані з ненадійних джерел (Загроза *Z6-4*)
	Відмова у провадженні діяльності (Загроза *Z6*-5)
	Відмова обладнання (Загроза *Z6-6*)
	Помилка використання (Загроза *Z6-7*)
	Нелегальне оброблення даних (Загроза *Z6-8*)
	Викрадення обладнання (Загроза *Z6-9*)
	Викрадення носіїв інформації або документів (Загроза *Z6-10*)
	Неавторизоване використання обладнання (Загроза *Z6-11*)
	Використання контрафактних чи копійованих програмних засобів (Загроза *Z6-12*)

Розрахуємо міру ризику для кожної групи активу і для всієї системи в цілому (таблиця 3.21).

Таблиця 3.21

Цінність активу ТОВ «Южмаш груп»

Актив	**Цінність активу**
Апаратні засоби	4
Програмні засоби	3
Мережа	3
Персонал	2
Місце функціонування організації	0
Організація	1

1) Апаратні засоби: (Актив групи *A1*)

(Актив A1)/(Загроза Z1-1)=8

(Актив A1)/(Загроза Z1-2)=7

(Актив A1)/(Загроза Z1-3)=4

(Актив A1)/(Загроза Z1-4)=4

(Актив A1)/(Загроза Z1-5)=5

(Актив A1)/(Загроза Z1-6)=6

(Актив A1)/(Загроза Z1-7)=4

(Актив A1)/(Загроза Z1-8)=7

(Актив A1)/(Загрози Z1)=(Актив A1)/(Загроза Z1-1)+(Актив A1)/(Загроза Z1-2)+(Актив A1)/(Загроза Z1-3)+(Актив A1)/(Загроза Z1-4)+(Актив A1)/(Загроза Z1-5)+(Актив A1)/(Загроза Z1-6)+(Актив A1)/(Загроза Z1-7)+(Актив A1)/(Загроза Z1-8)=8+7+4+4+5+6+4+7=30

2) Програмні засоби:

(Актив A2)/(Загроза Z2-1)=3

(Актив A2)/(Загроза Z2-2)=4

(Актив A2)/(Загроза Z2-3)=3

(Актив A2)/(Загроза Z2-4)=3

(Актив А2)/(Загроза Z2-5)=4

(Актив А2)/(Загроза Z2-6)=5

(Актив А2)/(Загроза Z2-7)=3

(Актив А2)/(Загроза Z2-8)=6

(Актив А2)/(Загроза Z2-9)=3

(Актив А2)/(Загрози Z2)= (Актив А2)/(Загроза Z2-1)+(Актив А2)/(Загроза Z2-2)+(Актив А2)/(Загроза Z2-3)+(Актив А2)/(Загроза Z2-4)+(Актив А2)/(Загроза Z2-5)+(Актив А2)/(Загроза Z2-6)+(Актив А2)/(Загроза Z2 -7)+(Актив А2)/(Загроза Z2-8)+(Актив А2)/(Загроза Z2-9)=3+5+4+3+4+5+4+6+3=37

3) Мережа:

(Актив А3)/(Загроза Z3-1)=7

(Актив А3)/(Загроза Z3-2)=6

(Актив А3)/(Загроза Z3-3)=7

(Актив А3)/(Загроза Z3-4)=3

(Актив А3)/(Загроза Z3-5)=4

(Актив А3)/(Загроза Z3-6)=5

(Актив А3)/(Загроза Z3-7)=6

(Актив А3)/(Загрози Z3)= *(Актив А3)/(Загроза Z3-1)+(Актив А3)/(Загроза Z3 -2)+(Актив А3)/(Загроза Z3 -3)+(Актив А3)/(Загроза Z3 -4)+(Актив А3)/(Загроза Z3-5)+(Актив А3)/(Загроза Z3-6)+(Актив А3)/(Загроза Z3-7)=7+6+7+3+4+5+6=**38***

4) Персонал:

(Актив А4)/(Загроза Z4-1)=5

(Актив А4)/(Загроза Z4-2)=4

(Актив А4)/(Загроза Z4-3)=6

(Актив А4)/(Загроза Z4-4)=5

(Актив А4)/(Загроза Z4-5)=6

(Актив А4)/(Загроза Z4-6)=5

(Актив А4)/(Загрози Z4)= (Актив А4)/(Загроза Z4-1)+(Актив А4)/(Загроза Z4-2)+(Актив А4)/(Загроза Z4-3)+(Актив А4)/(Загроза Z4-4)+(Актив А4)/(Загроза Z4-5)+(Актив А4)/(Загроза Z4-6)=5+4+6+5+6+5=31

5) Місце функціонування організації:

(Актив А5)/(Загроза Z5-1)=3

(Актив А5)/(Загроза Z5-2)=0

(Актив А5)/(Загроза Z5-3)=4

(Актив А5)/(Загроза Z5-4)=2

(Актив А5)/(Загрози У5)=(Актив А5)/(Загроза Z5-1)+(Актив А5)/(Загроза Z5-2)+(Актив А5)/(Загроза Z5-3)=4+(Актив А5)/(Загроза Z5-4)=3+0+4+2=9

6) Організація:

(Актив А6)/(Загроза Z6-1)=2

(Актив А6)/(Загроза Z6-2)=4

(Актив А6)/(Загроза Z6-3)=2

(Актив А6)/(Загроза Z6-4)=2

(Актив А6)/(Загроза Z6-5)=3

(Актив А6)/(Загроза Z6-6)=2

(Актив А6)/(Загроза Z6-7)=3

(Актив А6)/(Загроза Z6-8)=1

(Актив А6)/(Загроза Z6-9)=1

(Актив А6)/(Загроза Z6-10)=5

(Актив А6)/(Загроза Z6-11)=2

(Актив А6)/(Загроза Z6-12)=1

(Актив А5)/(Загрози Z5)=(Актив А6)/(Загроза Z6-1)+(Актив А6)/(Загроза Z6-2)+(Актив А6)/(Загроза Z6-3)+(Актив А6)/(Загроза Z6-4)+(Актив А6)/(Загроза Z6-5)+(Актив А6)/(Загроза Z6-6)+(Актив А6)/(Загроза Z6-7)+(Актив А6)/(Загроза Z6-8)+(Актив А6)/(Загроза Z6-9)+(Актив А6)/(Загроза Z6-10)+(Актив А6)/(Загроза Z6-11)+(Актив А6)/(Загроза Z6 -12)=2+4+2+2+3+2+3+1+1+5+2+1=28

Таблиця 3.22

Результати розрахунків

	Активи	Оцінка цінності для ймовірності ризиків та їх можливих наслідків	Ранжування загроз у порядку зменшення ступеня ризику від 1 (максимальний ризик) до 5 (мінімальний ризик)
1	Апаратні засоби	30	4
2	Програмні засоби	37	2
3	Мережа	38	1
4	Персонал	31	3
5	Місце функціонування організації	9	6
6	Організація	28	5

Оцінка ризику

Вхідні дані. Перелік ризиків з рівнями привласнених значень і критеріями оцінки ризику.

Дія. Повинні порівнюватися рівні ризиків з критеріями оцінки ризиків та критеріями прийняття ризиків.

Керівництво по реалізації. Характер рішень, пов'язаних з оцінкою ризиків, і критерії оцінки ризиків, які будуть використані для прийняття цих

рішень, повинні визначатися при встановленні контексту. Ці рішення і контекст повинні більш детально аналізуватися на етапі отримання більшого обсягу інформації про конкретні ідентифікованих ризиків. Для оцінки ризиків організація повинна порівнювати встановлені значення ризиків (з використанням обраних методів, розглянутих в додатку) з критеріями оцінки ризику, обраними на етапі встановлення контексту.

Критерії оцінки ризику, що використовуються для прийняття рішень, повинні узгоджуватися з певним зовнішнім і внутрішнім контекстом менеджменту ризику ІБ і враховувати цілі організації, думки причетних сторін і т.д. Рішення, пов'язані з оцінкою ризику, зазвичай ґрунтуються на прийнятному рівні ризику. Однак також повинні враховуватися наслідки, ймовірність, ступінь впевненості при ідентифікації і аналізу ризику. Сукупність безлічі ризиків низького і середнього рівня в результаті може мати результатом загальний ризик більш високого рівня.

При цьому необхідно враховувати наступне:

– значимість бізнес-процесу або діяльності, підтримуваних конкретним активом або сукупністю активів, якщо процес визначений як має низьку значимість, пов'язаним з ним ризиків слід приділяти менше уваги, ніж ризиків, що впливає на більш важливі процеси або діяльність;

– властивості ІБ (якщо один критерій не актуальний для організації (наприклад, втрата конфіденційності), то всі ризики, що впливають на цей критерій, можуть бути теж не актуальними).

Оцінка ризику ґрунтується на розумінні ризику, отриманому при аналізі ризику, і використовується при прийнятті рішень про майбутні дії. Рішення повинні включати в себе наступне:

– пріоритети при обробці ризику з урахуванням встановлених значень рівнів ризиків;

– необхідність в якоїсь діяльності.

На стадії оцінки ризику на додаток до ризиків з встановленими значеннями повинні прийматися в розрахунок договірні, юридичні та нормативні вимоги.

Вихідні дані. Перелік ризиків з призначеними пріоритетами відповідно до критеріїв оцінки ризиків, що стосуються сценаріїв інцидентів, які призводять до цих ризиків.

3.3. Висновки до розділу 3

Встановлено, що визначення цінності активів є ключовим фактором оцінки впливу сценарію інциденту. Різні загрози і вразливості можуть мати різний вплив на активи.

Доведено, що після визначення сценаріїв інцидентів необхідно оцінити ймовірність дії кожного сценарію і його вплив з використанням якісного або кількісного методу встановлення значення. Необхідно брати до уваги частоту виникнення загроз і простоту використання уразливості.

Визначено, що високорівнева оцінка дає можливість визначати пріоритети і хронологію дій.

Проведено ранжування загроз у порядку зменшення ступеня ризику для ТОВ «Южмаш груп»

ВИСНОВКИ

Проаналізовано відомі методології з аналізу ризиків інформаційній безпеці, такі як ISO, ITIL, COBIT.

Проведено порівняльний аналіз методологій аналізу ризиків інформаційній безпеці, виявлено їх недоліки та переваги.

Встановлено, що оптимальним варіантом для вибору методики управління загрозами інформаційної безпеки в контексті забезпечення безпеки інформації підприємства та місцям її зберігання, обробки та передачі є адаптація та удосконалення відомих методик логічним об'єднанням їх переваг та мінімізацією недоліків.

Розроблено типове рішення управління послугами та оцінки ризику ІБ у рамках системи менеджменту інформаційної безпеки на прикладі системи B2B послуг промислового підприємства.

Наведено типові поди оцінки ризику організації на прикладі веб-ресурсу промислового підприємства.

Встановлено, що процес менеджменту ризику ІБ складається з таких етапів: встановлення контексту; оцінки ризику; обробки ризику; прийняття ризику; комунікацій ризику; моніторингу та переоцінки ризику ІБ.

В процесі менеджменту ризику інформаційної безпеки виділено і деталізовано процес оцінки ризику інформаційної безпеки.

Встановлені основні критерії, сфера дії і кордони, структура процесу ризик-менеджменту інформаційної безпеки, прийняті для організації, що надає *B2B* послуги.

Розроблено рекомендації щодо створення типових рішень організації систем управління інформаційними послугами та інформаційною безпекою для організацій різного профілю, що містять типову методику розрахунку ризиків інформаційної безпеки організації

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артемов А. В. Информационная безопасность. Курс лекций. Орел: Литагент «МАБИВ», 2014. 51 с. URL: https://royallib.com/book/artemov_a/informatsionnaya_bezopasnost_kurs_lektsiy.html (дата звернення: 10.11.2021).

2. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О. Г., Гнатюк С. О., Казмірчук С. В. та ін.]. Київ : Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. 190 с.

3. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. *Вісник Національного університету «Львівська політехніка»*. 2008. №610. С. 20-33.

4. Бодрук О. Структури воєнної безпеки : національний та міжнародний аспекти : монографія. Київ : НІПМБ, 2001. 300 с.

5. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ. *Форум права*. 2009. №1. С.50-55.

6. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» URL: https://docs.cntd.ru/document/1200058320 (дата звернення: 10.11.2021).

7. Гуцу С. Ф. Правові основи інформаційної діяльності. URL: http://studrada.com.ua (дата звернення: 17.10.2021).

8. Дашян М. С. Право информационных магистралей – Law of Information Highways: вопросы правового регулирования в сфере Интернет. Москва : Волтерс Клувер, URL: http://www.telecomlaw.ru/monograph/Dashyan.pdf (дата звернення: 17.10.2021).

9. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. №14/2009. URL: www.president.gov.ua (дата звернення: 17.10.2021).

10. Введение в COBIT URL: http://www.iso27000.ru/chitalnyi-zai/standarty-informacionnoi-bezopasnosti/vvedenie-v-cobit (дата звернення: 17.10.2021).

11. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности. URL: http://www.scrf.gov.ru/security/information/document155/ (дата звернення: 17.10.2021).

12. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр.: 25.00.01. Львів, 2011. 24 с.

13. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. URL: www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=38836 (дата звернення: 17.10.2021).

14. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – URL: www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C99D4491C0171ACCAD297E1?art_id=38934&cat_id=38836 (дата звернення: 17.10.2021).

15. Как внедрить ISO 27001: инструкция по применению. URL: https://habr.com/ru/post/448568/ (дата звернення: 17.10.2021).

16. Комазов П. В., Рожко П. М. Методи забезпечення інформаційної безпеки. Європейський вектор модернізації інженерної та економіко-управлінської освіти в умовах сталого розвитку промислового регіону : матеріали Міжнародної науково- практичної конференції (27-28 травня

2021 року, м. Запоріжжя). – Запоріжжя : Наук. ред. Н. Г. Метеленко. ЗНУ Інженерний навчально-науковий інститут, 2021. С. 118-121

17. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наукового ступеня д-ра юрид. наук. : 12.00.07. Харків, 2004.

18. Кузьменко Б. В. Захист інформації : навч. посіб. – Ч. 2. Київ : Видавничий відділ КНУКіМ, 2009. 69 с.

19. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf (дата звернення: 17.10.2021).

20. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції. URL: www.pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi (дата звернення: 17.10.2021).

21. Ліпкан В. А. Національна безпека України. URL: www.pidruchniki.ws/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi (дата звернення: 17.10.2021).

22. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наукового ступеня кандидата юридичних наук : 12.00.07. Київ, 2005. 223 с.

23. Макарова М. В. Електронна комерція : посібник для студентів вищ. навч. закладів. Київ : Видавничий центр «Академия», 2002. 272 с.

24. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук.: 12.00.01. Київ, 2007. 22 с.

25. Марущак А. І. Пріоритети розвитку інформаційного права України. *Інформація і право*. 2011. № 1. С. 20-24.

26. Международный научный журнал «Символ науки» №10/2018 URL: https://os-russia.com/sn (дата звернення: 17.10.2021).

27. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) ДСТУ ISO/IEC 27001:2015 URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення: 17.10.2021).

28. Методика определения угроз безопасности информации в информационных системах. URL: https://fstec.ru/component/attachments/download/812 (дата звернення: 17.10.2021).

29. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології. Технології безпеки. Система керування інформаційною безпекою. Вимоги» URL: http://www.ni.din.de/sc27.html. (дата звернення: 17.10.2021).

30. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07. Київ, 2006. 20 с.

31. Ожегов С. И. Словарь русского языка. Москва, 1963 URL: https://search.rsl.ru/ru/record/01001596547 (дата звернення: 17.10.2021).

32. Соціально-правові основи інформаційної безпеки : навч. посібник за ред. В.В. Остроухова. Київ : Росава, 2007. 496 с.

33. Стандарты ITIL, MOF, ITSM, COBIT. URL: https://koptelov.info/publikatsii/standarty-itil-mof-itsm-cobit/ (дата звернення: 17.10.2021).

34. Пилипчук В. Г. Системні проблеми розвитку правової науки в інформаційній сфері. *Вісник Академії правових наук України*. 2011. №3. С. 16-27.

35. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

36. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. №373. *Офіційний вісник України*. 2006. №13.

37. Про основи національної безпеки України : Закон України : від 19.06.03 р. No 964-IV. *Відомості Верховної Ради України*. 2003. №39.

38. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки : Закон України : від 09.01.07 р. No 537-V. *Відомості Верховної Ради України*. 2007. №12. Ст. 102.

39. Стандарт ISO 27001. URL: https://sites.google.com/site/iso27com/standart27001 (дата звернення: 17.10.2021).

40. COBIT® 5 – the framework for the governance of enterprise IT. URL: https://www.itgovernance.co.uk/cobit (дата звернення: 17.10.2021).

41. ISO 27000 – Международные стандарты управления информационной безопасностью URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1

42. 87. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Київ : ДП«УкрНДНЦ», 2005. 60 с.