Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи магістра

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Оцінка ризиків інформаційної безпеки для підприємств роздрібної торгівлі»

Виконавець: студент ІІ курсу, групи КБм-21

Андрій ЖУРАВЛЬОВ
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Сергій ТОЛЮПА	
Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача КБм-21 (група) Журавльова Андрія Єгоровича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Оцінка ризиків інформаційної безпеки для підприємств роздрібної торгівлі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	процес оцінки ризиків підприємств роздрібної торгівлі
Предмет досліджень	оцінка ризиків підприємств роздрібної торгівлі
Мета	підвищення ефективності засобів захисту інформаційних систем підприємств роздрібної торгівлі, шляхом ранньої ідентифікації можливих ризиків інформаційної безпеки з урахуванням особливостей даної індустрії
Вихідні дані для проведення роботи	підприємство роздрібної торгівлі, корпоративна інформаційна система на підприємстві.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна полягає у адаптації методів управління ризиками інформаційної безпеки для визначення оптимального підходу до оцінки ризиків для підприємств роздрібної торгівлі.

Практична цінність можливості використання даного підходу для побудови системи управління інформаційною безпекою, яка базується на процесі управління ризиками інформаційної безпеки.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	24.10.2022 – 23.01.2023
Аналіз літературних джерел	24.01.2023 – 14.02.2023
Розробка плану оцінки ризиків на прикладі конкретного підприємства	15.02.2023 – 24.04.2023
Оформлення і друк пояснювальної записки	25.04.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект полягає у зменшенні витрат від кіберзагроз

Соціальний ефект полягає у оптимізації роботі з персоналом, інформування їх про загрози та засоби їх мінімізації.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Сергій ТОЛЮПА
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Андрій ЖУРАВЛЬОВ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Оцінка ризиків інформаційної безпеки для підприємств роздрібної торгівлі»: загальний обсяг роботи складає 80 сторінок, 12 рисунків, 9 таблиць та 25 літературних джерел.

Актуальність роботи зумовлюється тим, що в ній висвітлюються проблеми підприємств роздрібної торгівлі, які займають вагому нішу в індустрії як України, так і у всьому світі. Підприємства роздрібної торгівлі, першими впроваджують інноваційні рішення, отримують безсумнівні конкурентні переваги, але при цьому нові технології вимагають нових підходів до СУІБ, яка базується на управлінні ризиками.

Метою даної роботи є підвищення ефективності засобів захисту інформаційних систем підприємств роздрібної торгівлі, шляхом ранньої ідентифікації можливих ризиків інформаційної безпеки з урахуванням особливостей даної індустрії.

Об’єктом дослідження є інформаційна безпека підприємств роздрібної торгівлі.

Предмет досліджень – методи і підходи до оцінки ризиків інформаційної безпеки підприємств роздрібної торгівлі.

Методами дослідження було обрано: опрацювання літератури за даною темою, аналіз документації міжнародних стандартів та їх порівняння.

Практичне значення результатів роботи випливає з можливості використання даного підходу для побудови системи управління інформаційною безпекою, яка базується на процесі управління ризиками інформаційної безпеки, а також на основі використання даного підходу для оцінки ризиків інформаційної безпеки реального підприємства провести обробку ризиків для зменшення їх до прийнятного рівня.

Ключові слова: інформаційна безпека, оцінка ризиків, роздрібна торгівля, вразливість, загроза, збитки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АР	–	Аналіз ризику
SEI	–	Software Engineering Institute
ПЗ	–	Програмне забезпечення
ЦОД	–	Центр обробки даних
(D)DoS	–	(Distributed) Denial-of-Service
VPN	–	Virtual Private Network
ІКТ	–	Інформаційно-комунікаційні технології
ІБ	–	Інформаційна безпека
СУІБ	–	Система управління інформаційною безпекою
ІТ	–	Information Technology
ОН	–	Оцінка небезпеки
ЕОМ	–	Електронно обчислювальна машина
СЕД	–	Система електронного документообігу
РТ	–	Роздрібна торгівля

ВСТУП

Сьогодні зростає значення охорони інформації. В будь-якій сфері діяльності правильне планування ІБ є пріоритетним заходом для реалізації захисту даних.

Створення сильної корпоративної системи ІБ Є критично важливим критичним фактором розвитку будь-якого підприємства. Інформація є ключовим елементом в бізнесі, тому її безпека має велике значення. Під інформацією ми розуміємо не тільки статичні інформаційні ресурси, такі як бази даних і поточні налаштування обладнання, але і динамічні процеси обробки даних.

Аналіз ризиків є одним з основних і найскладніших етапів побудови системи захисту інформації, оскільки він базується на даних, отриманих під час оцінки безпеки підприємства. Сьогодні аналіз ризиків інформаційної безпеки отримує все більше уваги. Це пояснюється постійним зростанням використання інформаційних технологій у сучасному бізнесі, збільшенням цінності інформації, що обробляється та генерується підприємством, а також потребою інтегрувати різні інформаційні продукти для задоволення всіх потреб компанії.

Роздрібна торгівля неперервно зростає і вдосконалюється завдяки використанню різноманітних інновацій для бізнесу. Це ще більше ускладнює проблему забезпечення надійного захисту інформації і призводить до того, що інформаційна безпека стає ключовим фактором для забезпечення довіри споживачів і збереження конкурентоспроможності.

Актуальність даної роботи пояснюється фактом, що вона розглядає проблеми, що існують у підприємствах торгівельної галузі. Ці підприємства є піонерами у впровадженні інноваційних рішень та отриманні вагомих конкурентних переваг.

Метою даної роботи є оптимізація ефективності засобів захисту ІС підприємств роздрібної торгівлі, шляхом ранньої ідентифікації можливих ризиків інформаційної безпеки з урахуванням особливостей даної індустрії.

Для досягнення даної мети було поставлено такі **завдання**:

1. Аналіз проблем інформаційної безпеки підприємств роздрібної торгівлі;

2. Огляд існуючих методологій та стандартів з управління ризиками інформаційної безпеки, порівняльний аналіз, виявлення недоліків та переваг;

3. Визначення релевантного для підприємств роздрібної торгівлі підходу до оцінки ризиків інформаційної безпеки;

4. Оцінка ризиків інформаційної безпеки для реального підприємства, що належить до роздрібної торгівлі;

5. Визначення місць зберігання та обробки інформації, які мають ризики високого рівня

6. Визначення рекомендацій щодо зменшення ризиків високого рівня.

Методами дослідження обрано: опрацювання літератури за даною темою, аналіз документації міжнародних стандартів.

Наукова новизна даної роботи полягає у адаптації методів управління ризиками інформаційної безпеки для визначення оптимального підходу до оцінки ризиків для підприємств роздрібної торгівлі. Визначення такого підходу припускає більш успішну протидію сучасним кібер-зловмисникам, забезпечення безпеки, орієнтованої на захист від загроз шляхом впровадження превентивних засобів захисту.

Практичне значення результатів роботи випливає з можливості використання даного підходу для побудови системи управління інформаційною безпекою, яка базується на процесі управління ризиками інформаційної безпеки, а також на основі використання даного підходу для оцінки ризиків інформаційної безпеки підприємства провести обробку ризиків для зменшення їх до прийнятного рівня.

Таким чином **об’єктом дослідження** є інформаційна безпека підприємств роздрібної торгівлі.

Предмет досліджень – методи і підходи до оцінки ризиків інформаційної безпеки підприємств роздрібної торгівлі.

РОЗДІЛ 1
ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ РОЗДРІБНОЇ ТОРГІВЛІ

1.1 Використання IT в сучасному ритейлі

Діяльність у сфері торгівлі в новому тисячолітті є складним і динамічним сектором бізнесу, який охоплює як високорозвинені, так і розвиваючіся країни.. Сучасний ритейл переживає швидкі зміни, існують основні тренди, які впливають на способи ведення бізнесу в цій галузі.

Останнім часом роздрібна торгівля значно активізувалась у використанні інформаційних технологій, особливо в мобілізації бізнес-процесів. Це призвело до зростання важливості продуктів і послуг в галузі інформаційної безпеки роздрібної торгівлі.

Забезпечення безпеки стало одним з основних викликів управління підприємством. Зростаюча кількість загроз створює ризик не лише для матеріальних цінностей, але й для здоров'я та життя людей, а також для розвитку бізнесу.

1.2 Атаки у сфері роздрібної торгівлі

У 2018 році половина атак у сфері роздрібної торгівлі (52%) була спрямована на веб-додатки, зокрема на онлайн-магазини. Під час таких атак зловмисники отримували несанкціонований доступ до облікових даних клієнтів, викрадали інформацію про їх платіжні картки та порушували роботу веб-додатків. Крім того, майже кожна четверта атака (25%) передбачала впровадження шкідливого програмного забезпечення.

Ці виклики ставлять роздрібну торгівлю перед необхідністю забезпечити ефективні заходи інформаційної безпеки. Підприємства повинні активно вдосконалювати свої системи захисту, включаючи захист від кібератак, витоків даних та інших загроз. Вони повинні вдосконалювати свої інформаційні технології,

встановлювати сучасні антивірусні програми, міцні паролі та шифрування даних.

Також важливо навчити персонал правилам кібербезпеки та проводити регулярну підготовку щодо виявлення та реагування на можливі загрози. Підприємства можуть співпрацювати зі спеціалізованими компаніями з інформаційної безпеки для отримання консультацій та підтримки у цій сфері.

Забезпечення інформаційної безпеки стає необхідністю для роздрібної торгівлі в новому тисячолітті. Тільки шляхом прийняття належних заходів захисту та усвідомленням ризиків, підприємства зможуть забезпечити безпеку своїх клієнтів, зберегти довіру споживачів і збалансувати конкуренцію у цьому швидкозмінному секторі роздрібної торгівлі [5] (Рисунок 1.1).

Рисунок 1.1 – Поширені методи атак на підприємства роздрібної торгівлі

Великі підприємства роздрібної торгівлі, обробляючи тисячі транзакцій щодня через свої POS-термінали, стають привабливою мішенню для кіберзлочинців, оскільки існує процвітаючий ринок для викрадених даних кредитних карт. З цього випливає необхідність забезпечення безпеки POS-терміналів [6].

Все більше усвідомлюється, що інформаційна безпека впливає на ширший спектр бізнес-ризиків і вимагає більш комплексного підходу, що переходить до лідерів бізнесу. Звертається більше уваги на співробітників, впроваджуються «чесність», оскільки значна частина атак відбувається зсередини [7]. Також необхідно враховувати ризики, пов'язані з третіми сторонами (Рисунок 1.2).

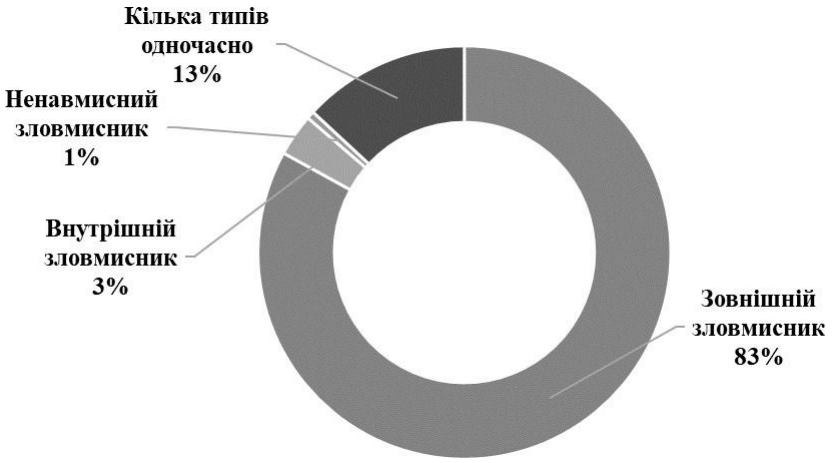

Рисунок 1.2 – Типи зловмисників, що здійснюють атаки на підприємства роздрібної торгівлі

Ефективне зниження втрат від факторів небезпеки є важливою конкурентною перевагою в роздрібній торгівлі. Актуальність питань безпеки в цій галузі є безсумнівною. Однак, для забезпечення належного рівня захисту потрібен комплексний підхід, який ефективно і економічно вирішить ці завдання.

Система безпеки включає різні організаційні, технічні і управлінські заходи, які взаємопов’язані. Побудова такої системи є унікальним продуктом, який швидко окупить витрати і приноситиме прибуток. Тому в роздрібній торгівлі рекомендується впроваджувати системи безпеки, спрямовані на потреби сучасного ринку і спрощення операційної діяльності, що підвищує рентабельність та ефективність.

Для зниження ризику інцидентів інформаційної безпеки, мають враховувати наступні аспекти [8]:

1. Створення стратегії інформаційної безпеки, що базується на визначенні об'єктів, які потребують захисту.
2. Встановлення пріоритетів щодо захисту,.
3. Визначення ролей та обов'язків з метою забезпечення інформаційної безпеки.
4. Впровадження заходів інформаційної безпеки у всі бізнес-процеси.

Висновки до розділу 1

Торговельні підприємства мають значну конкурентну перевагу як на внутрішньому ринку України, так і на міжнародній арені. Цей сектор продовжує активно впроваджувати інновації, які ускладнюють забезпечення надійного захисту та підкреслюють важливість інформаційної безпеки як ключового фактору, що сприяє довірі споживачів.

Ті підприємства роздрібної торгівлі, які першими впровадять інноваційні рішення, отримають явну перевагу у конкурентній боротьбі. Проте важливо пам'ятати, що нові технології вимагають нових підходів до забезпечення інформаційної безпеки.

Сучасне кіберсередовище потребує постійного перегляду заходів безпеки для протидії загрозам. Історія показує, що абсолютно непроникного захисту від зловмисників не існує. Кіберзлочинці постійно розробляють нові методи обходу існуючих захисних механізмів та проникнення в мережі. Після отримання доступу вони володіють здатністю зламати внутрішні ресурси підприємства з метою пошуку цінної інформації.

Для успішної боротьби з такими кіберзлочинцями необхідно забезпечити безпеку інформаційного середовища, що орієнтована на захист від загроз протягом усього циклу атаки - від початку, протягом розвитку та після завершення атаки. Ключовим елементом є впровадження процесу управління ризиками інформаційної безпеки.

Управління ризиками інформаційної безпеки означає систематичний підхід до ідентифікації, аналізу, оцінки та керування ризиками, пов'язаними з безпекою даних та інформаційними системами. Воно передбачає розробку та впровадження політик, процедур, технологій та практик, спрямованих на забезпечення належного рівня захисту.

Підприємства роздрібної торгівлі повинні зосередитися на декількох областях для зниження ризиків інцидентів і забезпечення ефективної інформаційної безпеки.

Серед них важливо забезпечити безпеку мережі та комунікацій, використовувати захист від вторгнень, контролювати доступ до систем та даних, регулярно оновлювати програмне забезпечення та відстежувати загрози безпеки.

Також важливо проводити навчання та свідомості співробітників стосовно інформаційної безпеки, встановлювати політику використання паролів та контролювати фізичний доступ до приміщень та обладнання. Регулярні аудити та аналізи безпеки допоможуть виявити потенційні вразливості та прийняти відповідні заходи для їх усунення.

Всі ці заходи допоможуть підприємствам роздрібної торгівлі забезпечити належний рівень інформаційної безпеки, що буде сприяти збереженню довіри споживачів, захисту цінної інформації та зниженню ризиків втрат. Розуміння важливості інформаційної безпеки та впровадження від дії соціальних інженерів, фішингових атак та інших видів кіберзагроз.

Підприємства роздрібної торгівлі повинні приділяти особливу увагу забезпеченню безпеки своїх інформаційних систем та даних. Це може включати застосування міцних паролів, шифрування даних, використання багаторівневої аутентифікації та систем контролю доступу. Крім того, необхідно регулярно оновлювати програмне забезпечення, встановлювати захисні патчі та використовувати антивірусне програмне забезпечення для виявлення та запобігання шкідливим програмам. Важливо також забезпечити резервне копіювання даних, щоб у разі інциденту була можливість відновлення інформації.

Навчання та підготовка співробітників також є ключовим аспектом інформаційної безпеки. Працівники повинні бути ознайомлені з основними правилами безпеки, уміти впізнавати підозрілі електронні повідомлення та посилання, а також знати процедури повідомлення про можливі інциденти безпеки.

Важливим елементом є також співпраця з експертами з інформаційної безпеки та партнерами, які можуть надати спеціалізовані рішення та консультації. Встановлення партнерських відносин з провідними постачальниками безпеки та впровадження передових технологій допоможуть забезпечити ефективну інформаційну безпеку на підприємстві.

РОЗДІЛ 2
ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ УПРАВЛІННЯ РИЗИКАМИ

2.1 Стандарти, орієнтовані на управління ризиками ІБ

Сьогодні у нас є достатній спектр методологій захисту від загроз. Деякі з них стали застарілими та не розвиваються, а інші можуть бути складними для вивчення через відсутність актуальних перекладів на англійську мову.

Однак, у даній роботі розглядаються саме ті методики, які використовують розгорнутий підхід. Вибір конкретної методики залежатиме від рівня вимог, які підприємство ставить перед собою щодо забезпечення безпеки інформації, характеру розглядуваних загроз та ефективності контрольних заходів з протидії інформаційним загрозам.

Оцінка ризиків інформаційної безпеки є важливим етапом для будь-якого підприємства. Ці методики допомагають оцінити потенційні загрози, визначити найбільш вразливі місця та розробити ефективні заходи контролю та захисту інформації. Їх використання допомагає забезпечити належний рівень безпеки інформації, знизити ризик втрати даних та недоступності систем, а також забезпечити довіру клієнтів і споживачів.

Кожна з наведених методик має свої особливості і підходи до оцінки ризиків ІБ. Наприклад, ISO 27005 є міжнародним стандартом, який надає систематичний підхід до оцінки ризиків ІБ, включаючи ідентифікацію загроз, вразливостей та можливих наслідків.

OCTAVE зосереджується на ідентифікації критичних активів та оцінці загроз, пов'язаних з ними. Існують також методики, специфічні для конкретних країн або галузей, наприклад, MAGERIT, що розроблена для оцінки ризиків в інформаційних системах урядових організацій Іспанії.

Важливим аспектом вибору методики є її актуальність і доступність. Деякі з методик можуть бути вже застарілими або не мати адекватних перекладів на англійську мову, що ускладнює їх використання та розуміння. Тому обрані методики повинні відповідати сучасним вимогам безпеки і мати належну підтримку та документацію.

Оцінка ризиків інформаційної безпеки є процесом, що потребує спеціалізованих знань і експертизи. Тому, для використання обраної методики, може бути корисним залучення фахівців з інформаційної безпеки, які володіють необхідними знаннями та досвідом. Вони зможуть допомогти підприємству зрозуміти та застосувати обрану методику ефективно і з максимальною користю.

При виборі методики оцінки ризиків інформаційної безпеки слід враховувати рівень вимог підприємства щодо безпеки даних і систем. Кожна методика може мати свої особливості та підходити для певного контексту. Наприклад, якщо підприємство працює в урядовому секторі, то методика MAGERIT може бути більш підходящою, оскільки вона спеціально розроблена для таких організацій. У разі, коли підприємство має міжнародну присутність, ISO 27005 може бути корисною завдяки своїй міжнародній визнаності.

Використання відповідної методики дозволить підприємству ідентифікувати потенційні загрози, визначити вразливості і прийняти відповідні заходи для забезпечення безпеки інформації. Результати оцінки ризиків допоможуть виявити найбільш критичні області, де необхідно зосередити увагу та розробити ефективні стратегії захисту.

2.1.1 ДСТУ ISO/IEC 27005:2015

Стандарт ISO 27005 належить до серії 2700x і пропонує підхід до організації процесу управління ризиками інформаційної безпеки. Хоча ця методика оцінки є класичною, вона має свої недоліки, такі як виключно академічний підхід та загальність формулювань. Однак стандарт ISO 27005 містить настанови та рекомендації, тому його вивчення рекомендується для отримання загального

досвідууправління ризиками інформаційної безпеки [1].

У цьому стандарті, термін "ризик" визначається як наслідок невизначеності відносно досягнення цілей. Ефект ризику може мати як позитивні, так і негативні наслідки та представляє собою відхилення від очікуваного результату. Зазвичай ризик виражається через комбінацію наслідків подій інформаційної безпеки та ймовірності їх виникнення. Невизначеність відноситься до недостатньої (навіть часткової) інформації та знаннями про її наслідки або можливість її виникнення.

Процес управління ризиками інформаційної безпеки включає такі етапи, як визначення обставин, оцінку ризиків, обробку ризиків, прийняття рішень щодо ризиків, обмін інформацією про ризики, а також моніторинг та перегляд ризиків. Метою цього процесу є ідентифікація потенційних загроз, оцінка їх впливу, визначення необхідних заходів для зниження ризиків та постійний контроль над ними.

Стандарт ISO 27005 надає структуровану методику для розуміння та управління ризиками інформаційної безпеки. Його основні етапи включають:

Визначення обставин: Цей етап передбачає збір і аналіз інформації про організацію, її активи, загрози та вразливості. На цьому етапі важливо зрозуміти контекст організації і її специфічні потреби щодо інформаційної безпеки.

Оцінка ризику: Цей етап включає оцінку впливу загроз на активи організації та визначення ймовірності виникнення цих загроз. Використовуються різні методи інформаційного аналізу та оцінки, щоб встановити рівень ризику для кожної загрози.

Обробка ризику: Після оцінки ризику необхідно прийняти рішення про подальші дії. Цей етап включає ідентифікацію можливих контролів та заходів, які можна впровадити для зменшення ризику. Важливо врахувати ефективність та вартість цих заходів.

Прийняття ризику: На цьому етапі організація приймає рішення про прийняття залишкового ризику. Враховуючи фінансові, технічні та стратегічні фактори, вона вирішує, чи буде здійснювати додаткові заходи зі зменшення ризику, чи приймає ризик на себе.

Обмін інформацією про ризик: Цей етап передбачає взаємодію зі

стейкхолдерами та іншими зацікавленими сторонами, щоб обмінюватися інформацією про ризики. Це допомагає покращити спільне розуміння ризиків та сприяє ефективному управлінню ними.

Моніторинг та перегляд ризику: Останній етап включає постійний моніторинг і оновлення оцінки ризику. Організація повинна встановити систему контролю, яка дозволяє відстежувати зміни в загрозах, вразливостях та ефективності заходів зі зменшення ризику. Результати моніторингу допомагають виявляти нові ризики та вчасно реагувати на них, забезпечуючи постійну безпеку інформації.

Хоча стандарт ISO 27005 є цінним інструментом для оцінки ризиків інформаційної безпеки, важливо пам'ятати, що кожна організація має свої унікальні потреби та контекст (Рисунок 2.1).

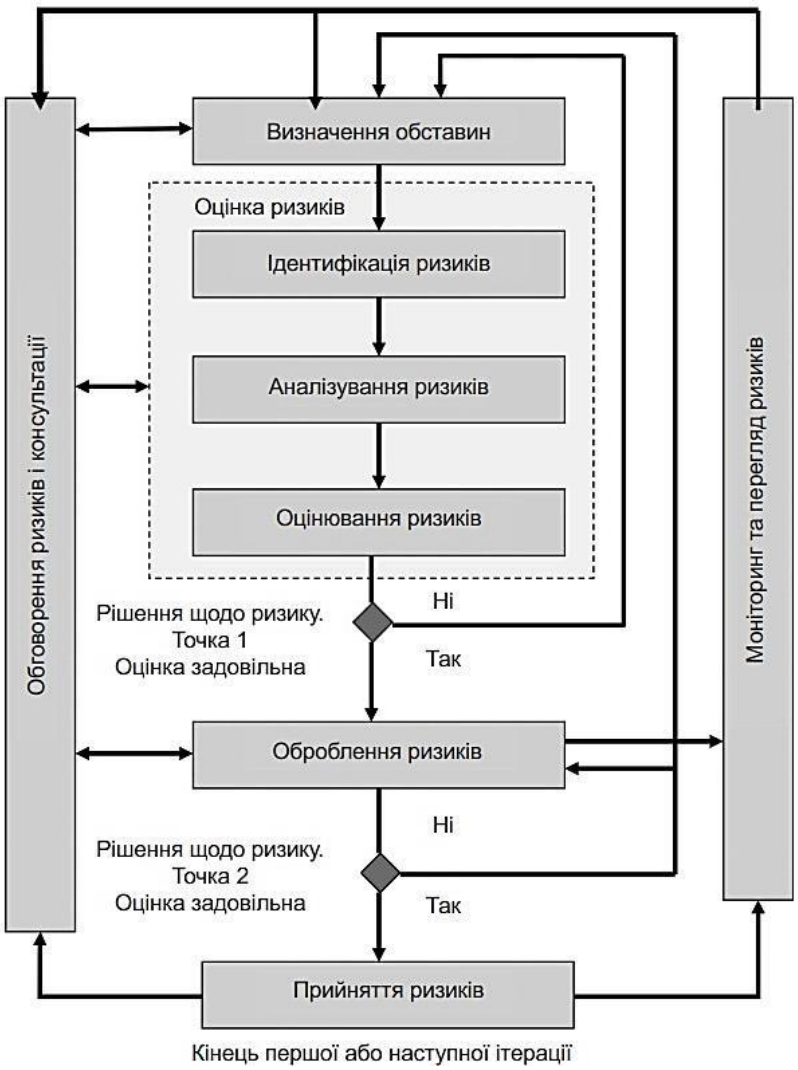

Рисунок 2.1 - Ілюстрація процесу управління ризиками ІБ за стандартом ISO 27005

На етапі визначення обставин в управлінні ризиками інформаційної безпеки (ІБ), встановлюються основні критерії, необхідні для ефективного управління ризиками. Цей етап включає визначення зовнішніх і внутрішніх обставин, встановлення сфери застосування та її меж, а також забезпечення функціонування системи управління ризиками ІБ в організації.

Базові критерії включають:

- Критерії зіставлення ризиків - використовуються для порівняння різних ризиків між собою.
- Критерії впливу - допомагають визначити потенційні наслідки ризиків.
- Критерії прийняття ризиків - використовуються для визначення того, які ризики можуть бути прийняті організацією.

Оцінка ризиків складається з таких дій:

- Ідентифікація ризику - цей етап має на меті визначення можливих подій, які можуть призвести до потенційних втрат і отримання уявлення про те, як, де і чому ці втрати можуть виникати.
- Аналіз ризиків - включає в себе детальне дослідження і оцінку ризиків, виявлених на попередньому етапі.
- Зіставлення ризиків - цей крок полягає в порівнянні виявлених ризиків з критеріями, встановленими на попередньому етапі.

Метою ідентифікації ризику є визначення можливих подій, які можуть спричинити потенційні втрати і отримання уявлення про те, як, де і чому ці втрати можуть виникати. Ідентифікація ризику включає наступні етапи, які збирають вхідні дані для подальшого аналізу ризику:

Ідентифікація активів СУІБ - цей крок включає визначення активів, які мають цінність для організації і потребують захисту. Це можуть бути інформаційні ресурси, системи, даних або фізичні об'єкти.

Ідентифікація загроз - на цьому етапі визначаються потенційні загрози, які можуть спричинити втрати або пошкодження активів СУІБ. Загрози можуть бути технічними, природними, людськими чинниками або їх комбінацією.

Ідентифікація існуючих засобів контролю - на цьому етапі визначаються заходи

контролю, які вже впроваджені в організації для запобігання або зменшення ризиків. Це можуть бути політики, процедури, технологічні рішення або відповідні стандарти.

Ідентифікація вразливостей - цей крок включає визначення слабких місць в системі, які можуть бути використані загрозами для атаки або злому. Вразливості можуть бути пов'язані з технічними аспектами, недостатніми процедурами безпеки, недоліками в системному адмініструванні тощо.

Ідентифікація наслідків - на цьому етапі визначаються можливі наслідки випадкових подій або атак на активи СУІБ. Це можуть бути фінансові втрати, порушення конфіденційності, порушення доступності, пошкодження репутації організації тощо.

В результаті ідентифікації ризику збираються всі необхідні дані, які стануть основою для подальшого аналізу ризиків. Ці дані використовуються для аналізу ризиків, розробки стратегій управління ризиками і прийняття відповідних заходів контролю.

На етапі ідентифікації ризиків збираються і систематизуються інформація про активи СУІБ, загрози, існуючі заходи контролю, вразливості та наслідки. Це дозволяє організації отримати повний обсяг інформації про потенційні ризики і їх вплив на інформаційну безпеку.

Після ідентифікації ризиків можна переходити до наступних етапів управління ризиками, таких як аналіз ризиків, розробка стратегій управління та прийняття рішень щодо контролю ризиків. Важливо продовжувати моніторити ризики та вносити відповідні зміни до стратегій управління ризиками, оскільки загрози та умови можуть змінюватися з часом.

Метою ідентифікації ризику є визначення можливих втрат та отримання уявлення про те, як, де і чому ці втрати можуть статися. Ідентифікація ризиків включає ідентифікацію активів системи управління інформаційною безпекою, загроз, існуючих засобів контролю, вразливостей та наслідків.

Аналіз ризиків може бути якісним або кількісним, або поєднанням обох методів, залежно від обставин. Рівні ризиків порівнюються з критеріями оцінювання ризику та критеріями прийняття ризику.

Обробка ризиків передбачає чотири варіанти: модифікацію ризику, прийняття ризику, усунення ризику та розподілення ризику. Ці варіанти надають організації можливість зменшити, прийняти, усунути або розподілити ризики відповідно до її потреб та можливостей.

2.1.2 NIST SP800-30

NIST SP800-30, в свою чергу, пропонує різноманітні методики оцінки ризиків та організації управління ризиками інформаційної безпеки на різних рівнях. Особливістю цього документа є детальні описи кожного елемента і рекомендації щодо їх практичного застосування у різних ситуаціях.

Розробка стратегій та політик є важливим елементом управління ризиками інформаційної безпеки, оскільки вони визначають підходи до управління ризиками і встановлюють принципи і правила для всіх зацікавлених сторін. Методика NIST SP800-30 враховує різні аспекти управління ризиками, починаючи від стратегічного рівня до конкретних застосувань в інформаційних системах. Цей підхід дозволяє організаціям більш гнучко і ефективно управляти ризиками, враховуючи їх контекст та особливості.

Оцінка ризиків за допомогою методики NIST SP800-30 передбачає аналіз потенційного збитку, який може виникнути внаслідок реалізації загрози, а також ймовірності виникнення цієї загрози. Ця двохпараметрична оцінка дозволяє отримати уявлення про ризики, з якими стикається організація, та визначити пріоритетні напрямки зменшення ризиків.

Однією з важливих особливостей методики NIST SP800-30 є її орієнтація на практичне застосування. У документі наведено детальні пояснення процесу оцінки ризиків і рекомендації щодо їх практичної реалізації. Це дозволяє організаціям впроваджувати ефективні та налагоджені на їх потреби підходи до управління ризиками інформаційної безпеки.

Мета виконання процесів управління ризиком полягає у забезпеченні можливості підприємству досягти своєї місії шляхом зміцнення безпеки IT-систем,

підвищення рівня інформованості та обізнаності керівництва та надання допомоги при прийнятті рішень щодо авторизації ІТ-систем на підставі результатів управління ризиком.

Управління ризиками є ітеративним процесом, що відбувається на всіх етапах життєвого циклу розвитку ІТ-системи. Його головною метою є зменшення негативного впливу на організацію та надання потрібної бази для прийняття рішень щодо управління ризиком ІТ-систем.

Методологія оцінки ризику включає дев'ять головних кроків, які допомагають організаціям систематично та структуровано оцінити ризики та прийняти необхідні заходи для зниження ризику інформаційної безпеки.

Виконання процесів управління ризиком має значення для підприємств, оскільки це дозволяє їм підвищити безпеку ІТ-систем, отримати обґрунтовані обсяги витрат із заходів управління ризиком та забезпечити авторизацію ІТ-систем на основі результатів оцінки ризику.

2.1.3 OCTAVE

OCTAVE є методологією, розробленою Software Engineering Institute (SEI) при університеті Карнегі Меллон, для оцінки ризиків в організаціях. Цей підхід сприяє ідентифікації та оцінці ризиків інформаційних систем, а також поліпшенню їхньої безпеки та захисту.

Особливістю даної методології є те, що процес аналізу здійснюється внутрішніми співробітниками організації, без залучення зовнішніх консультантів. Для цього формується спільна група, в яку входять технічні експерти та керівники різних рівнів, що дозволяє здійснити комплексну оцінку можливих наслідків безпекових інцидентів для бізнесу та розробити відповідні заходи протидії [3].

Методика OCTAVE включає такі фази аналізу:

Встановлення критеріїв оцінки ризику: на цьому етапі визначаються параметри та критерії, за якими буде проводитися оцінка ризиків.

Розробка профілю загроз: проводиться ідентифікація потенційних загроз,

пов'язаних з активами та місцями їх зберігання.

Ідентифікація інфраструктурних вразливостей: аналізуються вразливості, які можуть бути використані загрозами для атаки на систему.

Розробка стратегії та планів безпеки: на цьому етапі розробляються стратегії та плани заходів щодо забезпечення безпеки, які допоможуть запобігти або зменшити вплив ідентифікованих ризиків.

Методика OCTAVE надає організації систематичний підхід до оцінки ризиків і розробки планів безпеки. Вона спрямована на забезпечення більшої самостійності організації в процесі виявлення і вирішення проблем безпеки інформаційних систем [15].

На першому етапі - встановлення критеріїв оцінки ризику - визначаються важливі фактори, які впливають на безпеку системи. Це можуть бути втрати даних, вплив на бізнес-процеси, витрати на відновлення та інші.

Другий етап - розробка профілю загроз - передбачає ідентифікацію потенційних загроз для активів організації та їх місць зберігання. Це можуть бути технічні загрози, які виникають в результаті вразливостей системи, а також соціальні або природні загрози.

Третій етап – знаходження вразливостей - спрямований на виявлення слабких місць в системі, які можуть бути використані загрозами. Це можуть бути недостатні заходи безпеки, відсутність контролю доступу або недостатня свідомість співробітників.

Четвертий етап - розробка стратегії та планів безпеки - передбачає розробку конкретних заходів для запобігання або зменшення ризиків. Це можуть бути технічні заходи, які включають в себе захист мережі, шифрування даних, резервне копіювання тощо, а також організаційні заходи, інформування персоналу та впровадження політик безпеки (Рисунок 2.2).

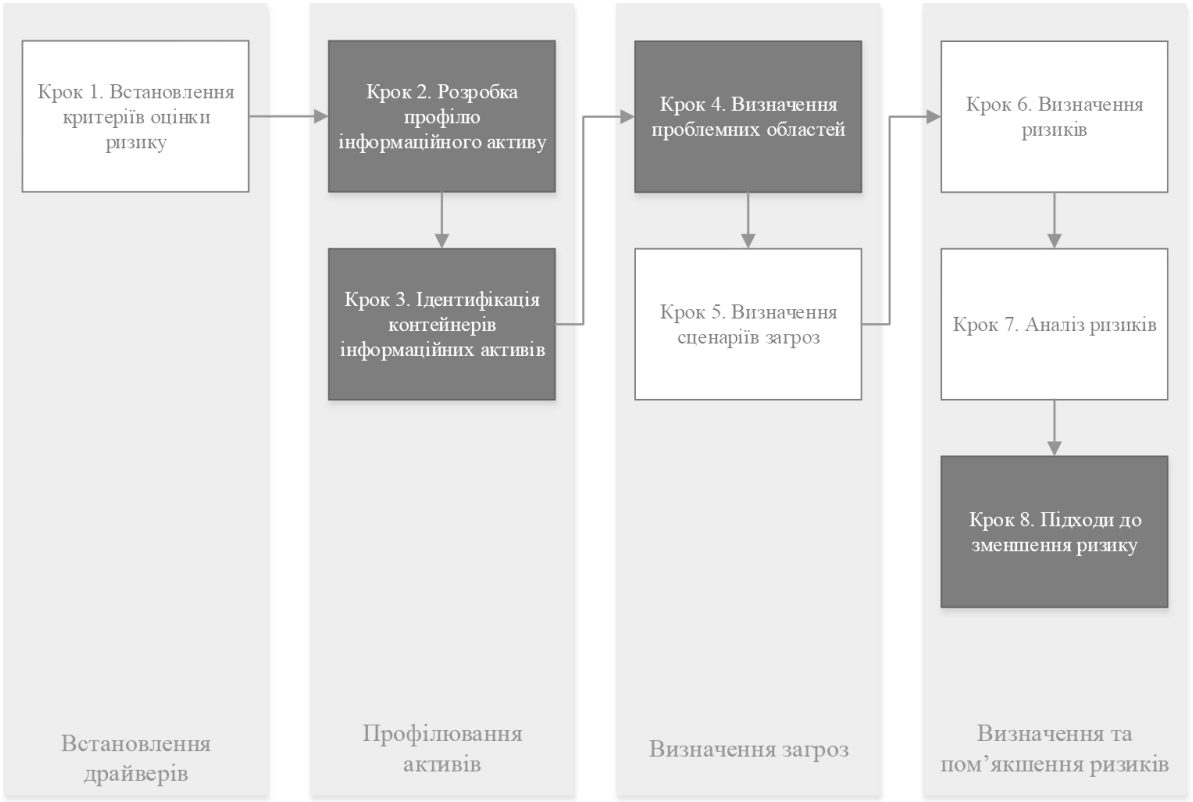

Рисунок 2.2 - Модель OCTAVE

Методика OCTAVE включає в свою структуру профіль загрози, який містить інформацію про актора, тип доступу, джерело загрози, мотивацію та можливі наслідки. Крім того, профіль містить посилання на загальнодоступні каталоги, де можна знайти описи цих загроз. У методиці OCTAVE загрози класифікуються залежно від джерела наступним чином:

- Загрози, спричинені людиною-порушником через мережу передачі даних.
- Загрози, спричинені людиною-порушником, який має фізичний доступ.
- Загрози, пов'язані з відмовами в роботі системи.
- Інші загрози.

Такі загрози можуть призвести до розкриття, модифікації, втрати або руйнування інформаційного ресурсу, а також до відключення або відмови в обслуговуванні. У методиці OCTAVE рекомендується використовувати "дерево варіантів" для опису профілю загрози (приклад такого дерева для загроз типу 1 показано на Рисунку 2.3). Це дерево допомагає систематизувати та структурувати загрози. На першому етапі дослідження головним завданням є стандартизований опис

зв'язку між загрозою та ресурсом, тому рекомендується уникати надмірної кількості технічних деталей. Детальний аналіз технічних аспектів виконується на наступних етапах дослідження.

Застосування методики OCTAVE дозволяє організаціям систематично і структуровано оцінювати загрози та розробляти ефективні стратегії забезпечення безпеки [14].

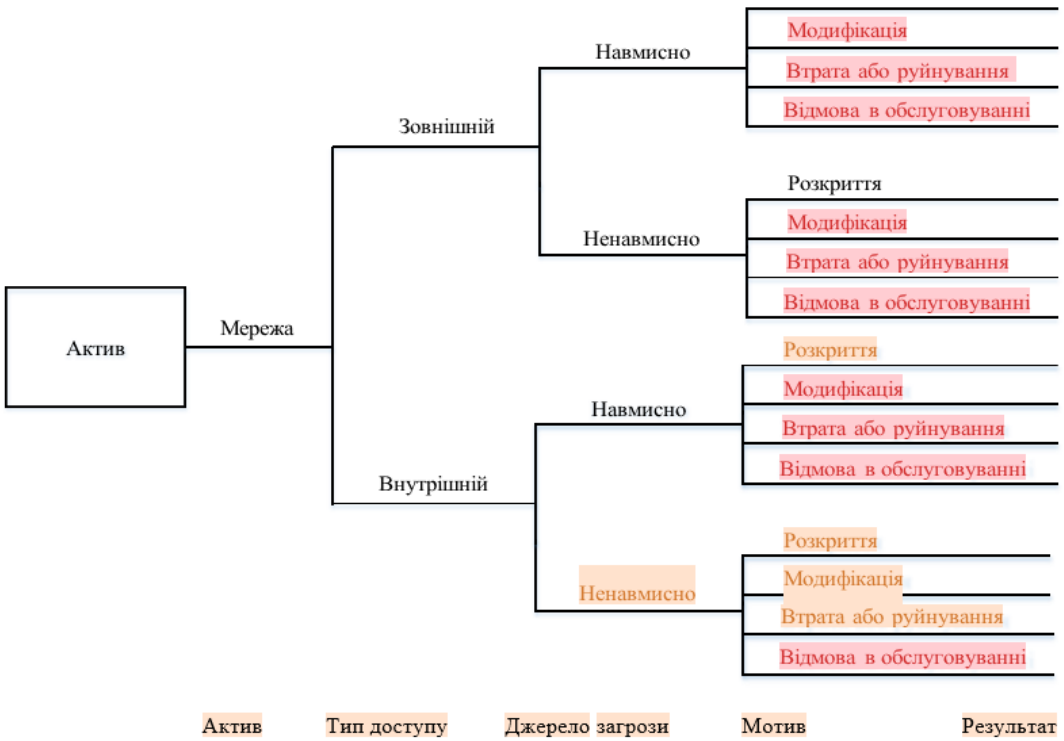

Рисунок 2.3 – Дерево варіантів, що використовується при описі профілю

Ідентифікація інфраструктурних вразливостей є важливим етапом другої фази дослідження системи з використанням методики OCTAVE. Під час цього етапу проводиться визначення інфраструктури, яка забезпечує функціонування активів, а також середовища, що може стати джерелом доступу до них. Наприклад, для бази даних відділу кадрів інфраструктура може включати сервер, на якому розташована база даних, а також робочі станції співробітників цього відділу. Під час цієї фази аналізуються компоненти різних класів, такі як сервери, мережеве обладнання, системи зберігання, персональні комп'ютери, мобільні комп'ютери, бездротові пристрої та інші.

Група, що проводить аналіз, вказує, які компоненти в кожному сегменті мережі

перевіряються на наявність вразливостей. Перевірка вразливостей здійснюється за допомогою сканерів безпеки, які використовуються для операційних систем, мережевих сканерів безпеки, спеціалізованих сканерів для конкретних веб-серверів, систем управління базами даних та інших компонентів. Після перевірки вразливостей для кожного компонента визначаються списки вразливостей, які потребують негайного усунення, ті, які потребують усунення найближчим часом, та ті, до яких не потрібно негайних дій [23].

Отримані дані цієї фази підготовлюються у звіт, в якому вказуються виявлені вразливості, їх потенційний вплив на активи та запропоновані заходи щодо усунення вразливостей.

Третя фаза методики OCTAVE - розробка стратегії і планів безпеки - є ключовою стадією в дослідженні системи. Після оцінки ризиків на попередніх етапах визначається відповідна стратегія та плани зниження ризиків.

При оцінці ризику в OCTAVE надається оцінка очікуваного збитку, не залучаючи оцінку ймовірності. Використовується шкала, яка включає категорії високий, середній і низький ризик. Ризики оцінюються з урахуванням фінансових збитків, впливу на репутацію компанії, а також на життя та здоров'я клієнтів та співробітників. Крім того, враховується можливість спровокувати службове розслідування внаслідок виникнення певного інциденту. Для кожної градації ризику встановлюються відповідні значення, що відображають його рівень.

Після оцінки ризиків розробляються плани зниження ризиків різних типів, такі як довгострокові плани, плани на середню перспективу та список завдань на найближчий час. У планах зниження ризиків визначаються конкретні заходи та рекомендації щодо підвищення безпеки системи. Ці заходи можуть включати в себе вдосконалення процедур автентифікації та авторизації, встановлення додаткових захисних механізмів, шифрування даних, регулярні аудити та навчання персоналу щодо кібербезпек [11].

Відповідно до звіту, визначаються пріоритети усунення вразливостей та запровадження заходів безпеки. Стратегія безпеки включає в себе широкий спектр заходів, спрямованих на запобігання і виявлення потенційних загроз та забезпечення

безпеки активів організації.

Довгострокові плани зниження ризиків передбачають впровадження стратегічних ініціатив та системних змін у всій організації. Це можуть бути заходи щодо підвищення свідомості про кібербезпеку серед персоналу, вдосконалення політик та процедур безпеки, розвиток інформаційної безпеки як складової стратегії бізнесу, а також інвестиції в нові технології та рішення безпеки.

Плани на середню перспективу спрямовані на поетапне впровадження конкретних технічних рішень та механізмів безпеки. Наприклад, це може включати реалізацію системи моніторингу та виявлення вторгнень, встановлення ефективних фаєрволів та систем обмеження доступу, оновлення програмного забезпечення та регулярні апгрейди систем [19].

Списки завдань на найближчий час передбачають негайні дії та виправлення вразливостей з найвищим пріоритетом. Це можуть бути термінові патчі, усунення відомих проблем безпеки та виконання невідкладних заходів для запобігання потенційним атакам або втратам даних.

Висновки до розділу 2

Аналіз ризиків інформаційної безпеки є важливим етапом для ефективного управління безпекою інформації. Для досягнення успіху у цьому процесі необхідно мати можливість швидкого реагування для системи ІБ.

Такий підхід дозволяє використовувати найкращі практики з кожної методології і створює можливість для гнучкого та налагоджуваного управління ризиками ІБ. Це сприяє покращенню безпеки інформації, зниженню вразливостей та ризиків, а також забезпечує компанії надійний фундамент для захисту її активів та дотримання вимог законодавства щодо конфіденційності, повноти та доступності даних.

РОЗДІЛ 3
ОСНОВНІ ПІДХОДИ ДЛЯ ОЦІНКИ ІНФОРМАЦІЙНОЇ ЦІННОСТІ

Майно або активи можуть бути розділені на дві категорії: нематеріальну власність, яка включає знання, інформацію, дані і т.д., і матеріальне майно, таке як обладнання та інші фізичні активи (Рисунок 3.1).

Рисунок 3.1 – Співвідношення матеріальних та нематеріальних активів

Література не дає вичерпних відповідей на питання про оцінку інформаційної цінності. Вартість нематеріальних активів, які мають велике значення, часто ігнорується, що призводить до суб'єктивної оцінки і недостатньо надійних підстав для прийняття рішень. Література з даної теми не є достатньо розвиненою, оскільки важко знайти універсальний підхід до оцінки цінності активів [20].

Оцінка активів ускладнюється через відсутність чітко визначених значень для інформації, даних та знань, а також їх непередбачуваний вплив на бізнес-результати. Проблеми виникають тому, що неможливо виміряти інформацію за допомогою

конкретних фізичних доказів або об'єму.

Оцінка інформаційної цінності вимагає врахування багатьох аспектів, таких як потенційна користь, стратегічна вагомість, вплив на конкурентоспроможність та репутацію компанії. Однак, відсутність чіткого рамок і шкал оцінки створює складнощі при прийнятті об'єктивних рішень щодо цінності активів [19].

3.1 Вплив інформації на бізнес

У відмінність від інших матеріальних активів, інформація може приймати різноманітні форми і включати дизайн продукту, технічні дані, інструкції з управління, оперативні дані, знання співробітників, комп'ютерне програмне забезпечення, бізнес-результати, бази даних, документацію та багато іншого. У бізнесі інформація є стратегічним ресурсом, основним джерелом доходів та рушійною силою для створення нової цінності, підвищення продуктивності, досягнення успіху на ринку та підтримки робочих процесів.

Оцінка цінності інформації включає врахування різних аспектів, таких як потенційна користь, стратегічне значення та вплив на бізнес. Інформація має не лише фінансову цінність, але і інші, які необхідно враховувати. Оцінка цінності інформації може здійснюватись за допомогою якісного або кількісного підходу, або їх комбінації. Вибір підходу залежить від конкретних обставин і вимагає балансу між якісною і кількісною складовими.

Оцінка цінності інформації є складним завданням, оскільки інформація має багато вимірів і впливає на різні аспекти бізнесу. Підходи до оцінки цінності інформації розвиваються протягом останніх десятиліть.

Якісний підхід до оцінки цінності інформації базується на описі та ранжируванні. Він зосереджується на якісних характеристиках інформації, таких як її актуальність, достовірність, доступність та сприятливість для прийняття рішень. Цей підхід особливо актуальний у випадках, коли інформація має важливе стратегічне значення, але її фінансова цінність складно виміряти.

Кількісний підхід, натомість, базується на чисельному розрахунку цінності

інформації. Цей підхід використовує фінансові моделі, методи оцінки ризику та інші кількісні параметри для визначення цінності інформації. Наприклад, можна використовувати метод дисконтованої грошової вартості, щоб визначити чисту поточну вартість інформаційного активу [16].

Комбінація якісного та кількісного підходів є також популярним варіантом для оцінки цінності інформації. Вона дозволяє поєднати переваги обох підходів і забезпечити більш об'єктивну оцінку. Наприклад, можна використовувати якісний підхід для опису важливості інформації і кількісний підхід для розрахунку її фінансової цінності. Результати оцінки цінності інформації залежать від вибору підходу та методології, що використовується. Оцінка цінності інформації може допомогти бізнес-організаціям приймати обґрунтовані рішення щодо управління інформаційними активами та ресурсами.

Оцінка кількості вартості активів, таких як ліцензії, патенти та знання, доступні на ринку, може бути здійснена досить просто. Ці активи мають конкретну фінансову вартість, яку можна визначити на основі їх вартості придбання або виробництва. Однак, визначення цінності інформації, яка не має прямого фінансового еквівалента або виникає під час бізнес-процесів, є складнішою задачею. В такому випадку, якісна оцінка стає цінним інструментом для аналізу . У Таблиці 3.2 наведено метрики, які використовуються для обох типів [21].

Таблиця 3.2

Метрики оцінки вартості інформації

Метрика	Значення
Фінансова вартість	Виражає відношення вартість / прибуток в числах; Використовує математичні та статистичні розрахунки Може зробити оцінку більш важкою
Один, два, три, чотири, п’ять (1, 2, 3, 4, 5); ключова, критична, важлива, загальна, не важлива	Метрика зрозуміла, повинна бути розроблена група правил для категоризації рівнів цінності Успішність метрики залежить від суб’єктивності визначення критеріїв Корисна, якщо фінансова вартість активів не важлива або невідома Може застосовуватися до всіх елементів ризику Не вимагає багато часу Розрахунки прості Аналіз витрат / прибутку не підтримується

3.2 Підходи до оцінки вартості інформації

Аналіз визначенням фінансової вартості інформації виходячи з двох методів. Перший метод передбачає фінансову оцінку, що може бути застосована до інформації , які визначаються в основному через суму коштів на їх створення).

У такому випадку можна визначити цінність інформації на основі втрат або витрат, пов'язаних з відновленням або втратою цієї інформації.

Один з методів якісної оцінки полягає у використанні "матриці цінностей", що зображено на Рисунку 3.2. Результати оцінки відображаються у вигляді матриці, що надає корисну інформацію для подальших рішень та управлінських стратегій. Використовуючи якісний підхід, можна збагатити оцінку інформації, дозволяючи краще розуміти її цінність у контексті бізнес-процесів та приймати обґрунтовані рішення.

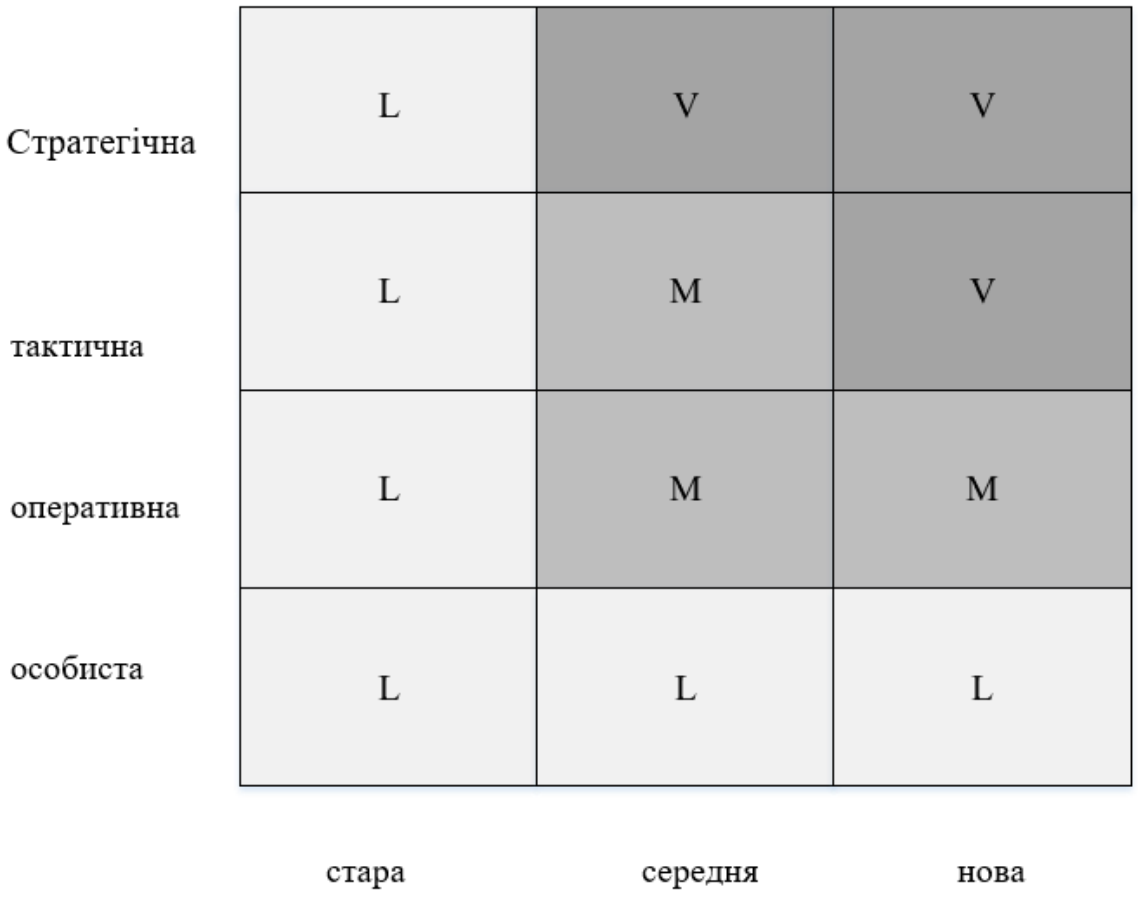

Рисунок 3.2 – Матриця співвідношення важливості інформації та її вік

Висновки до розділу 3

В даному розділі робиться акцент на проблемі визначення інформаційної цінності та критеріїв, які використовуються для оцінки інформації. Оцінка цінності інформації вирішується шляхом перегляду ролі інформації в бізнесі. Для більш якісної оцінки важливо визначити критерії, які реально описують процеси в компанії, та за допомогою яких легко оцінити цінність інформації.

Існують два домінуючих метода оцінки та пов’язані з ними метрики: кількісний та якісний. Сама оцінка визначається обраною методологією і вона залежить від характеристик інформації, що оцінюється (чи можливо оцінити в грошовому еквіваленті чи ні). У кожному випадку обрана методологія та діапазон значень критеріїв повинні бути спрямовані на вибір найбільш ефективної оцінки і відповідно подальшого захисту інформації.

Враховуючи складність оцінки вартості розмаїття підходів до оцінки, важливо враховувати специфіку конкретного бізнесу та контексту, у якому використовується інформація. Здійснення об'єктивної та збалансованої оцінки допоможе компанії зрозуміти цінність своїх інформаційних ресурсів і прийняти обґрунтовані рішення щодо їх захисту та оптимального використання.

РОЗДІЛ 4
ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПІДПРИЄМСТВА РОЗДРІБНОЇ ТОРГІВЛІ

4.1 Особливості підприємств роздрібної торгівлі як об’єкта дослідження

Для торговельних підприємств велика кількість взаємопов'язаних бізнес-процесів потребує ефективного управління. Це призводить до накопичення значної кількості інформації та даних, які необхідні для функціонування компанії. Організація мають велику кількість співробітників, що вимагає контролю інформаційних систем, а також уваги до ризиків, пов'язаних зі співробітниками [22].

Важливо визначити, яку інформацію та інформаційні системи ми вважаємо пріоритетною. Для цього потрібно враховувати фінансову цінність, вплив на бізнес-процеси, конкурентоспроможність та інші фактори. Аналіз можливих ризиків, пов'язаних з конфіденційністю, цілісністю та доступністю інформації, також допоможе визначити найбільш вразливі області і прийняти необхідні заходи безпеки.

Для успішного захисту цінної інформації та уникнення можливих наслідків втрати чи розголошення необхідно розробити комплексну стратегію інформаційної безпеки. Ця стратегія повинна включати оцінку цінності інформації, контроль доступу, навчання персоналу та використання технологічних рішень для захисту.

Щоб вирішити цю проблему, потрібно встановити чіткі критерії, які відображатимуть значущість інформації для підприємства. Розгляд фінансової цінності, впливу на бізнес-процеси, конкурентоздатності та інших факторів може допомогти визначити, яка інформація має найвищий пріоритет у захисті. Крім того, важливо провести аналіз можливих ризиків, пов'язаних з конфіденційністю, цілісністю та доступністю інформації, щоб визначити найбільш вразливі області і прийняти необхідні заходи безпеки [22].

З урахуванням особливостей торговельної галузі, важливо розробити

комплексну стратегію інформаційної безпеки, яка включатиме оцінку цінності інформації, контроль доступу, навчання персоналу та впровадження технологічних рішень для захисту інформаційних систем. Тільки таким чином підприємство зможе ефективно забезпечити захист своєї цінної інформації та уникнути можливих наслідків втрати або розголошення.

Для ефективного захисту інформації у підприємствах роздрібної торгівлі також необхідно звернути увагу на навчання співробітників щодо інформаційної безпеки, внутрішні політики та відповідальність за невиконання вимог безпеки. Це допоможе підвищити свідомість персоналу щодо ризиків і потенційних загроз інформаційній безпеці. Також важливо регулярно інформувати співробітників про актуальні методи атак та шахрайства, а також про процедури звітування і виявлення інцидентів.

При визначенні пріоритетів у захисті інформації слід також враховувати технологічні рішення, такі як використання шифрування даних, системи контролю доступу, моніторинг мережі та інші заходи для забезпечення безпеки інформаційних систем. Крім того, необхідно регулярно проводити аудит безпеки, оцінювати ефективність заходів безпеки та вживати коригувальних заходів для покращення системи інформаційної безпеки.

При цьому велике значення має систематичний підхід, який включає постійне оновлення оцінки ризиків, врахування нових тенденцій та загроз інформаційній безпеці, а також забезпечення достатніх ресурсів для впровадження заходів щодо забезпечення безпеки даних та ІА. Одним із важливих завдань керування загрозами інформаційної безпеки є визначення критичності і цінності інформації для підприємства. Необхідно провести детальний аналіз і ідентифікувати дані, які є найбільш цінними та вразливими. Це допоможе зосередити зусилля на захисті самої важливої інформації та визначити пріоритети в управлінні ризиками [23].

4.2 Підхід до оцінки ризиків ІБ

Керування загрозами комплексним процесом, який включає кілька етапів. Основною метою цього процесу зниження ризиків порушення безпеки та розуміння

причин, що зроблять інформаційні системи вразливими.

Перший етап – вибір підходів. На цьому етапі визначаються методи і інструменти, які будуть використовуватися для оцінки потенційних загроз інформаційній безпеці. Це може включати аналіз інформаційних активів, ідентифікацію потенційних загроз і визначення рівня вразливості системи.

Другий етап - оцінка ризику. На цьому етапі проводиться оцінка ймовірності виникнення загроз та потенційних наслідків порушення безпеки. Це допомагає визначити рівень ризику і встановити пріоритетність заходів щодо його зниження.

Третій етап - обробка ризику. На цьому етапі вживаються заходи для зниження ризику до прийнятного рівня. Це може включати впровадження технічних, організаційних та правових заходів, які спрямовані на запобігання або зменшення впливу потенційних загроз. Етапи зображені на Рисунку 4.1.

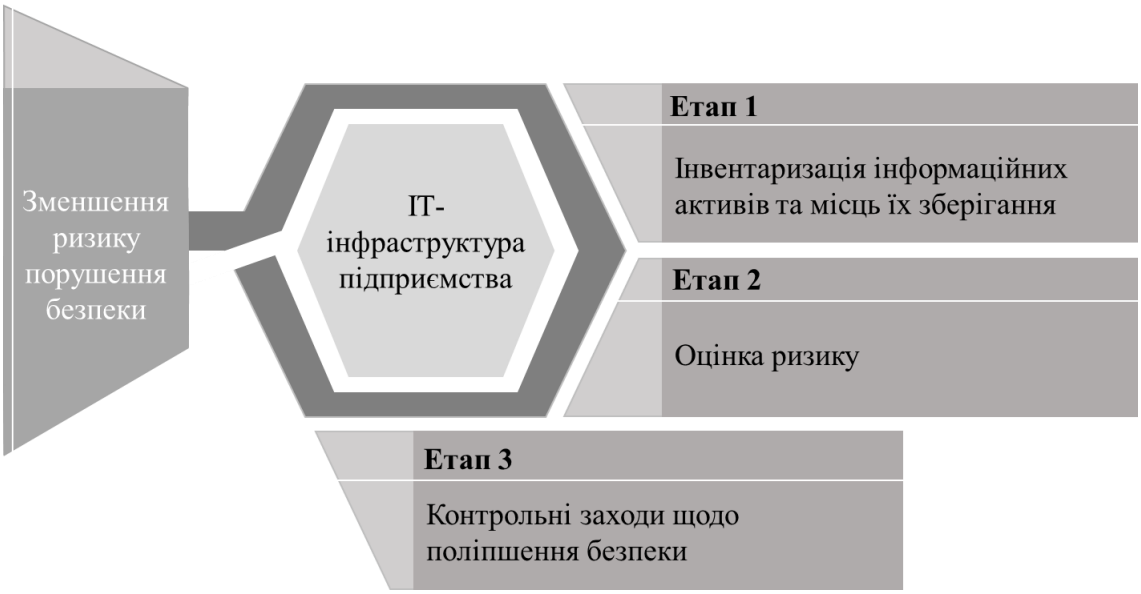

Рисунок 4.1 - Три етапи процесу управління ризиками інформаційної безпеки

Центральним елементом запропонованої моделі оцінки ризиків є оцінка IT-інфраструктури підприємства роздрібної торгівлі (Рисунок 4.2).

Створюється рекурсивний механізм, який збирає дані про уразливості і загрози, аналізує їх і визначає рівень ризику, що може бути виміряний та оброблений. Ця оцінка дозволяє виявити потенційні проблеми та слабкі місця в IT-інфраструктурі та прийняти відповідні заходи для зниження ризиків [20].

Важливо враховувати, що процес управління ризиками інформаційної безпеки

є постійним і динамічним. Підприємства роздрібної торгівлі повинні регулярно переглядати та оновлювати свої стратегії та заходи, оскільки загрози та уразливості можуть змінюватись з часом. Регулярні перегляди та вдосконалення процесу управління ризиками допоможуть підприємствам підтримувати високий рівень інформаційної безпеки та захищати свою інформацію від потенційних загроз.

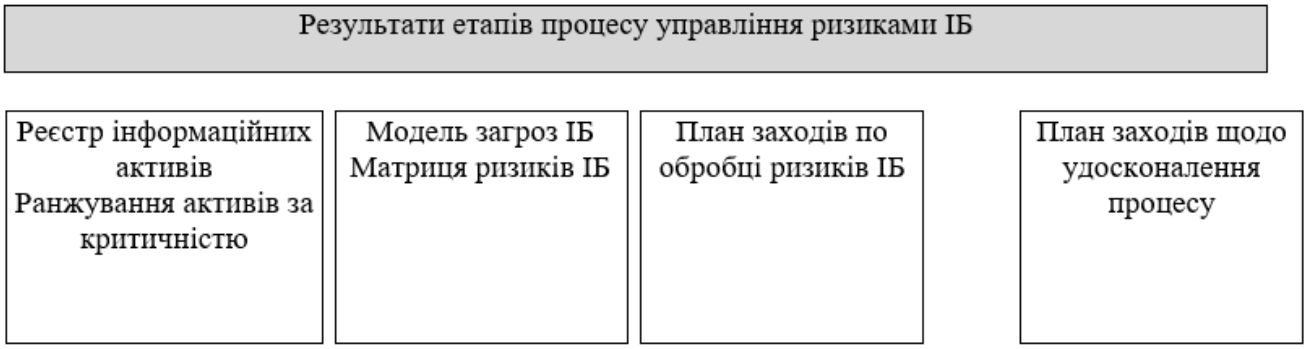

Рисунок 4.2 – Результати етапів процесу управління ризиками ІБ

4.3 Етап 1: Інвентаризація інформаційних активів та місць їх зберігання

Перед початком інвентаризації інформаційної безпеки, необхідно визначити область, в якій проводитиметься оцінка ризиків ІБ. Запропонована модель встановлює межі для оцінки ризиків ІБ шляхом визначення меж дії системи управління інформаційною безпекою (СУІБ).

Це означає, що оцінка ризиків ІБ виконується на рівні окремих структурних підрозділів і компонентів підприємства, враховуючи їх взаємодію та вплив на загальну інформаційну безпеку.

Визначення меж виконання процесу оцінки ризиків ІБ дозволяє зосередитись на конкретних областях підприємства, де інформаційна безпека є найбільш вразливою, і прийняти заходи для запобігання можливим загрозам. Цей підхід до управління інформаційною безпекою дозволяє зрозуміти, які частини організації мають найбільший потенціал ризику і вимагають найбільшої уваги та заходів з контролю.

Одним з ключових аспектів моделі є Система управління інформаційною безпекою (СУІБ), яка виступає як центральний організатор і контролер заходів і

процесів забезпечення безпеки інформації. СУІБ об'єднує різні організаційні одиниці, бізнес-підрозділи та інформаційні системи підприємства, забезпечуючи їх взаємодію і спільну мету - забезпечення конфіденційності, повноти та доступності інформації.

У межах СУІБ виконується процес оцінки ризиків інформаційної безпеки.

Процес аналізу загроз ІБ в межах СУІБ сприяє виробленню дієвих стратегій та планів контрольних заходів. Залучення організаційних одиниць, бізнес-підрозділів та інших складових підприємства у цей процес дозволяє виявити слабкі місця, визначити найвразливіші активи та розробити цілеспрямовані стратегії для забезпечення безпеки інформації (Рисунок 4.3).

• Конфіденційність означає, що інформація недоступна неавторизованим, і її зміст не розкривається.

• Цілісність, що інформація забезпечує точність і повноту.

• Доступність означає, що інформація доступна користувачу, коли вона йому потрібна.

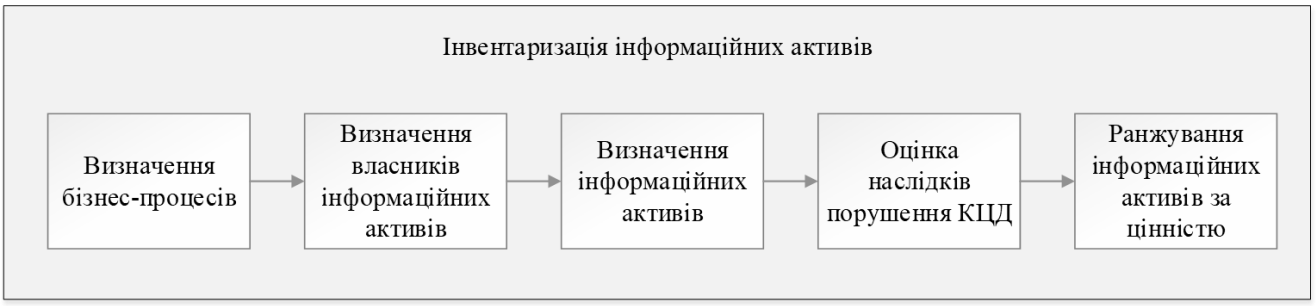

Рисунок 4.3 – Процес інвентаризації інформаційних активів

4.3.1 Визначення бізнес-процесів

Перш ніж проводити ідентифікацію інформаційних активів, слід спочатку встановити бізнес-процеси, які функціонують у організації і де ці активи створюються. Для торговельної галузі ці бізнес-процеси можна визначити за допомогою служб адміністративного апарату. Деякі з таких служб включають в себе:

1. Служба управління ланцюгами поставок (логістика): ця служба відповідає за планування, координацію та контроль руху товарів від постачальників до клієнтів.

2. Служба безпеки: її завдання полягає у забезпеченні безпеки працівників, клієнтів та активів підприємства, включаючи захист інформації.

3. Служба IT: вона відповідає за планування, розробку, впровадження та підтримку інформаційних систем і технологій, що використовуються в організації.

4. Служба маркетингу: її завдання включає дослідження ринку, розробку маркетингових стратегій, просування товарів і послуг підприємства.

5. Юридична служба: вона забезпечує правову підтримку організації, включаючи укладання контрактів, врегулювання спорів і забезпечення дотримання законодавства.

6. Служба управління економікою та фінансами: вона відповідає за фінансове планування, бухгалтерський облік, управління ресурсами і фінансовий аналіз організації.

7. Служба закупок: її завданням є організація процесу закупівель необхідних матеріалів, товарів і послуг для підприємства, забезпечення оптимальних умов співпраці з постачальниками та контроль якості закуплених товарів.

8. Аналітична служба: ця служба відповідає за збір, аналіз та інтерпретацію даних для прийняття обґрунтованих рішень. Вона займається проведенням маркетингових досліджень, аналізом конкурентного середовища та прогнозуванням ринкових тенденцій.

9. Служба нерухомості: її завдання включає управління нерухомим майном підприємства, включаючи оренду, продаж та утримання приміщень і об'єктів нерухомості.

10. Проектно-технологічна служба: вона відповідає за розробку та впровадження нових технологій, проектування інфраструктури підприємства та вирішення технічних завдань.

11. Служба управління регіонами: ця служба займається координацією та управлінням діяльністю підприємств у різних регіонах, зокрема відкриттям нових філій, розвитком мережі та взаємодією з місцевими органами влади.

12. Технічна служба: її завданням є забезпечення технічної підтримки, обслуговування та ремонту технічного обладнання та інфраструктури підприємства.

13. Служба управління персоналом: вона відповідає за рекрутинг, навчання, мотивацію та управління персоналом підприємства, включаючи такі чинники, як укомплектованість, кар'єрний розвиток, оцінка працівників та управління трудовими відносинами.

4.3.2 Оцінка наслідків порушення КЦД активів

Для усіх ІА оцінюються можливі результати від отримання загроз порушення конфіденціальності, повноти, доступу (Таблиця 4.1).

У даному підході для активу визначається рівень наслідків по кожному типу для кожної властивості інформації.

Таблиця 4.1

Наслідки при порушенні конфіденційності, повноти та доступності активу

Рівень наслідків порушення КЦД	Наслідки комерційним інтересам організації	Наслідки операційної діяльності	Наслідки відносинам з клієнтами і партнерами	Наслідки лояльності співробітників
3	Комерційні інтереси або фінансове становище організації можуть бути істотно підірвані, втрата частки ринку	Критична втрата управлінського контролю, повна зупинка операційної діяльності, скасування поточних проектів	Серйозне погіршення іміджу організації, втрата довіри з боку значної частини клієнтів і партнерів, широка негативна популярність	Критичне зниження лояльності співробітників, масові звільнення
2	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 50 000 до 100 000 грн.	Середня втрата управлінського контролю, часткове зупинення операційної діяльності і труднощі в реалізації поточних проектів	Негативна інформація про підприємство поширюється в ЗМІ, втрата довіри з боку деякої частини клієнтів і партнерів	Значне зниження лояльності співробітників, погіршення клімату підприємстві і часті звільнення

1	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 10 до 50 000 грн.	Низька втрата управлінського контролю, незначні переривання операційної діяльності і незначні труднощі в реалізації поточних проектів	Втрата довіри деяких клієнтів або потенційних клієнтів, зниження довіри з боку деяких партнерів	Незначне зниження лояльності і скарги з боку співробітників
0	Порушення конфіденційності, повноти та доступності інформації не має відчутних наслідків. Дана інформація документується в реєстрі інформаційних активів, але не бере участь в оцінці ризиків ІБ			

4.3.3 Ранжування інформаційних активів за цінністю

У сучасних бізнес-системах інформація стала стратегічним ресурсом, ключовим для успішної діяльності підприємств. Вона виступає як одна з найважливіших бізнес-цінностей, є джерелом доходів та мотивацією для створення нових цінностей.

Оцінка інформаційної цінності в контексті підприємств роздрібної торгівлі здійснюється з урахуванням декількох аспектів:

- Значення для комерційних інтересів підприємства.
- Значення для операційної діяльності підприємства.
- Значення для відносин з клієнтами і партнерами.
- Значення для збереження лояльності співробітників.

Для визначення ступеня критичності інформації і ранжування її за важливістю необхідно оцінити наслідки порушення конфіденціальності, повноти та доступності інформації. Ця оцінка допоможе визначити її цінність для організації [25].

Проте, існує проблема відсутності універсального та зрозумілого методу оцінки інформаційної цінності, який би також враховував процес оцінки ризиків інформаційної безпеки. Це вимагає подальших досліджень і розробки відповідних підходів та інструментів для об'єктивної оцінки інформаційної цінності.

Для ранжування інформації необхідно використовувати запропоновану шкалу

з Таблиці 4.2.

Таблиця 4.2

Класифікація інформаційних активів за ступенем їх впливу на бізнес

Цінність інформації	**Рівень критичності інформації**
[8, 10]	К1 (особливо критична інформація)
[5, 8)	К2 (критична інформація)
[2, 5)	К3 (інформація середньої критичності)
< 2	К4 (некритична інформація)

В результаті проведення інвентаризації створюється список, що містить опис інформаційних активів, місця їх зберігання, а також користувачів, що мають доступ до цих активів у вигляді відділів та інших організаційних підрозділів.

Інвентаризація інформаційних активів - це неперервний процес, який потребує періодичного перегляду та оновлення власниками цих активів. При виявленні нового активу або зміні існуючих даних про актив, власник повинен повідомити співробітників з питань інформаційної безпеки в організації, які вносять відповідну інформацію до реєстру інформаційних активів. Після оновлення реєстру власник інформаційних активів має узгодити його з оновленими даними. Оновлений реєстр інформаційних активів ініціює проведення додаткової оцінки ризиків для нових або оновлених активів.

4.4 Оцінка ризиків ІБ

Ризик ІБ – рівень шкоди, яку зазнає компанія, у разі реалізації загрози з використанням уразливості місця зберігання та обробки інформації компанії

На Рисунку 4.4 показаний процес для оцінки ризиків інформаційної безпеки.

Рисунок 4.4 – Процес оцінки ризиків інформаційної безпеки

Оцінка ризиків необхідна для визначення критичної для функціонування бізнесу інформації та збитків від порушення конфіденціальності, повноти та доступності цієї інформації.

4.4.1 Оцінка рівня схильності активів та місць їх зберігання та обробки до впливу ризику

Підхід, запропонований, щоб захистити інформацію в конкретних місцях зберігання, вимагає оцінки рівня наслідків порушення конфіденціальності, повноти та доступності активів, що зберігаються в цих місцях.

Рівень схильності активів та місць їх зберігання та обробки до впливу ризику визначається за Таблицею 4.3.

Таблиця 4.3

Залежність рівня схильності активів та місць їх зберігання та обробки до впливу ризику від рівня наслідків порушення КЦД

Рівень наслідків порушення КЦД	**Рівень схильності активів та місць їх**

	зберігання та обробки до впливу ризику, %
3	100
2	80
1	60
0	20

4.4.2 Ідентифікація вразливостей місць зберігання і обробки інформаційних активів

Після створення та схвалення інвентаризаційного реєстру виконується процес визначення вразливостей місць зберігання та обробки інформаційних активів.

Для забезпечення інформаційної безпеки використовуються різноманітні засоби, включаючи:

- Управління доступом, що контролює права доступу користувачів до системи;
- Управління змінами, що керує процесом внесення змін до інформаційних систем;
- Управління резервним копіюванням, що забезпечує регулярне створення резервних копій даних;
- Управління задачами за розкладом, що планує і контролює виконання завдань згідно з графіком;
- Управління інцидентами, що реагує на випадки порушення безпеки і відновлює нормальну роботу системи;
- Управління вразливостями, що виявляє та аналізує вразливості в інформаційних системах.

Для забезпечення безпеки інформації також використовуються різні процеси, включаючи:

- Управління мобільними пристроями, що контролює використання мобільних пристроїв у робочих цілях;

- Управління знімними носіями інформації, що регламентує використання знімних носіїв даних;
- Управління доступом, що контролює права доступу користувачів до системи;
- Управління життєвим циклом інформаційних систем, що керує процесом розробки, експлуатації та виведення інформаційних систем з експлуатації;
- Моніторинг подій інформаційної безпеки, що виявляє та аналізує події, пов'язані з безпекою інформації;
- Управління вразливостями, що виявляє та аналізує потенційні вразливості в системах;
- Управління інцидентами, що реагує на випадки порушення безпеки і вживає заходів щодо їх вирішення;
- Управління ризиками інформаційної безпеки, що виявляє та оцінює ризики, пов'язані з безпекою інформації;
- Криптографічний захист інформації, що використовує шифрування для захисту конфіденціальності та повноти даних;
- Захист від зловмисного коду, що виявляє та запобігає впливу шкідливого програмного забезпечення;
- Управління резервним копіюванням, що забезпечує регулярне створення резервних копій даних;
- Контроль за установкою програмного забезпечення на комп'ютерах користувачів, що контролює процес встановлення програм на робочих станціях;
- Безпека мережі, що забезпечує захист мережевої інфраструктури від несанкціонованого доступу та атак;
- Управління сервісними організаціями, що встановлює процедури та контролює діяльність зовнішніх постачальників послуг з питань безпеки.
- Забезпечення високої кваліфікації та обізнаності персоналу, впровадження процедур адміністрування і механізмів контролю процесів, розподіл ролей і відповідальності.

- Застосування фізичних заходів захисту та створення відповідного фізичного оточення для зберігання інформації.
- Дотримання вимог законодавства, договорів, стандартів і інших нормативних документів щодо інформаційної безпеки.

Для кожного процесу та кожного місця зберігання інформації складається перелік виявлених вразливостей. Кожна вразливість потребує встановлення її рівня, який визначається в існуючому середовищі. Запропоновано наступні рівні вразливостей:

- Високий рівень вразливості - вказує на значну вразливість, яка може бути використана для вторгнення або порушення безпеки інформації.
- Середній рівень вразливості - вказує на помірну вразливість, яка потребує певних заходів для запобігання вторгненню або порушенню безпеки.
- Низький рівень вразливості - вказує на незначну вразливість, яка має незначний вплив на безпеку інформації і може бути вирішена з відносно малими зусиллями.

Рівень вразливості буде використаний в розділі 4.4.5 для оцінки ймовірності загрози.

4.4.3 Ідентифікація загроз направлених на місця зберігання активів

У Таблиці 4.4 наведено співвідношення між типовими загрозами та основними характеристиками інформації, спеціально для підприємств роздрібної торгівлі.

Таблиця 4.4

Типи загроз

Група загрози	**Тип загрози**	**Основні властивості інформації, на які впливає загроза**		
Зовнішні атаки		К	Ц	Д
	Атаки, що викликають відмову в обслуговуванні			×
	Злом ключів	×		
	Злом паролів	×		
	Несанкціонована спроба доступу	×	×	×
	Модифікація мережевого трафіку		×	×
	Перехоплення повідомлень	×		
	Поширення комп’ютерних вірусів		×	×
	Поширення спаму			×
	Впровадження шкідливого коду	×	×	
	Впровадження троянських програм	×	×	
	Соціальна інженерія	×		
	Виконання зловмисного сканування	×		
	Злом веб сайтів		×	
	Підміна веб сайтів	×		
	Підміна облікових записів користувачів	×		
Навмисна некоректна експлуатація		К	Ц	Д
	Отримання несанкціонованого доступу до системи / мережі	×		
	Використання системи з метою порушення роботи			×
	Використання системи з метою шахрайства	×	×	

	Розкриття інформації, що використовується для входу в систему	×		
	Розкриття бізнес інформації	×		
	Завантаження або відправка неадекватного вмісту		×	×
	Зміна або додавання транзакцій, файлів або баз даних		×	×
	Зміна системних привілеїв без авторизації		×	×
	Зміна або установка ПО без авторизації		×	×
	Установка недозволеного ПО		×	×
Крадіжка		К	Ц	Д
	Крадіжка бізнес інформації	×		×
	Крадіжка комп’ютерного обладнання			×
	Крадіжка ПО	×		×
	Порушення авторських прав на програмне забезпечення		×	
	Крадіжка інформації для аутентифікації	×		
	Крадіжка інформації для ідентифікації особистості	×		
Збої в роботі		К	Ц	Д
	Збій в роботі застосунків, розроблених всередині Компанії	×	×	×
	Збій в роботі застосунків, закуплених у сторонніх постачальників	×	×	×
	Збій в роботі системного ПО	×	×	×
	Збій в роботі комп’ютерного / мережевого обладнання		×	×
Порушення надання послуг		К	Ц	Д
	Пошкодження обчислювального центру, втрата обчислювальної техніки			×

	Пошкодження / втрата комунікаційних каналів / послуг			×
	Пошкодження / втрата допоміжного обладнання			×
	Втрата електроживлення			×
	Перевантаження системи			×
	Стихійні лиха			×
Ненавмисна неправильна експлуатація		К	Ц	Д
	Помилки користувачів		×	×
	Помилки адміністраторів / IT персоналу		×	×
Непередбачені наслідки змін		К	Ц	Д
	Непередбачені наслідки від зміни / впровадження нових бізнес-процесів	×	×	×
	Непередбачені наслідки від змін в ПЗ	×	×	×
	Непередбачені наслідки від змін в бізнес-інформації	×	×	×
	Непередбачені наслідки від змін в комп’ютерному / комунікаційному устаткуванні	×	×	×
	Непередбачені наслідки від змін в організації	×	×	×
	Непередбачені наслідки від змін в методах користувачів або засобах	×	×	×

Вразливість системи безпеки підприємства може виникнути внаслідок відсутності або недієвості контролів інформаційної безпеки. Зокрема, якщо контролі недостатні або неефективні, це може створити умови для реалізації загроз.

Натомість, наявність і ефективність показників рівня безпеки інформаційної інфраструктури сприяють зниженню ймовірності реалізації загроз. Тому важливо включити опис цих контролів у матрицю ризиків та враховувати їх при подальшому оцінюванні вірогідностей реалізації загроз.

4.4.4 Оцінка ймовірності та частоти реалізації загрози

Оцінка ймовірності виникнення загрози у випадках, пов'язаних з навмисними діями людей, такими як несанкціонований доступ, ускладнюється через залежність цих дій від наявної системи захисту інформації на підприємстві. Врахування системи захисту інформації є важливим фактором при оцінці ймовірності навмисної загрози.

Напрочуд неправильним підходом буде надавати оцінку виникнення навмисної загрози, ігноруючи систему захисту інформації. Зловмисники оцінюватимуть свої можливості, і в разі слабкого захисту організації вони можуть намагатися здійснити шкідливі дії, що може завдати шкоди організації. У той же час, в компанії із організованим захистом зі суворим контролем дій співробітників, зловмисники будуть утримуватись від таких спроб [18].

Розглянемо різні категорії зловмисників за декількома аспектами, зосередившись на класифікації їх мети, рівні доступу, ресурси, кваліфікації та ступені ризику.

Залученість зловмисників може мати різноманітні цілі, такі як завдання шкоди, фінансова вигода, доступ до інформації і багато інших. Наприклад, цілі промислових шпигунів можуть суттєво відрізнятися від цілей синдикату організованої злочинності. Тому контрзаходи, які ефективно протидіють першим, можуть не бути ефективними проти других. Розуміння мети потенційних зловмисників є першим кроком у визначенні ефективних контрзаходів.

Зловмисники мають різний рівень доступу. Наприклад, можливості, які мають члени організації, можуть бути значно більшими, ніж у звичайних осіб. Фінансові можливості зловмисників також значно варіюються: деякі мають значні ресурси, тоді як інші обмежені. Крім того, їх технічна кваліфікація також може значно розрізнятися.

Різні класи зловмисників по-різному сприймають ризик. Конкуренти, що втратили свою ринкову позицію, можуть бути готові пожертвувати всім, щоб знищити конкурента. Злочинці можуть бути готові взяти на себе ризик опинитися за ґратами, але, ймовірно, не хочуть ризикувати більшими наслідками, які можуть виникнути від реалізації загрози для підприємства.

Зловмисники, які мають бажання отримати славу, зазвичай уникають потрапляння до в'язниці, оскільки це може пошкодити їх репутацію та соціальний статус. Індивід, що займається незаконними діями та має практично необмежений бюджет, володіє найбільшими можливостями для прийняття рішень, оскільки він може використовувати свої фінансові ресурси в різних напрямках. Він може отримати

необхідну інформацію, підкупивши осіб з відповідним доступом. Крім того, він може покращити свої технічні навички, купуючи технології або наймаючи експертів (можливо, зацікавивши їх у своїх цілях або надавши неправдиву інформацію). Тим самим, він може знизити ризик, здійснюючи складніші та витратніші атаки [17].

Розумний зловмисник (що є більшістю) обере таку атаку, яка повністю компенсує його витрати: кваліфікацію, отримання доступу, використання ресурсів, час і ризик. Деякі атаки можуть вимагати високого рівня технічної кваліфікації, але не потребувати спеціального рівня доступу, наприклад, злам алгоритму шифрування. Кожен зловмисник намагатиметься використовувати набір атак, який він вважає оптимальним, відкидаючи ті, що не задовольняють його потребам. Він вибере таку атаку, яка зменшує витрати і збільшує його вигоду.

Імовірність загрози збільшується, якщо отримана вигода від отримання ІА перевищує суму коштів на її отримання. При значному зростанні прибутку до ресурсів на її отримання (Cinf / Cg), імовірність загрози різко зростає.

Рівень захищеності інформації визначається витратами на отримання цієї інформації. Чим більше витрати на отримання, тим менше відношення Cinf / Cg і, отже, менша ймовірність загрози.

Ймовірність виникнення загрози залежить від кількох факторів, включаючи:

Ціну інформації, яка захищається;

Рівень ІБ організації;

Кваліфікацію та ресурси зловмисника, а також витрати на отримання інформації;

Криміногенну обстановку в організації, зокрема наявність співробітників, які можуть продати інформацію.

Необхідно визначити, чи існує вразливість у даній організації, яка може стати джерелом загрози. Якщо є джерело загрози, то ця загроза може мати місце [15].

4.4.5 Визначення рівня ризику ІБ

Для встановлення ступінь ризику, необхідно розрахувати величину можливих

збитків, які виникнуть внаслідок реалізації загрози, щодо збереження та роботи з ІА. Існують різні методи оцінки цих збитків. У даній роботі запропоновано оцінювати фінансовий ризик, пов'язаний з порушенням конфіденціальної, повноти та доступу ІА.

На основі певних факторів може бути сформована вартість інформації Cinf. Ці фактори включають:

- Дисконтована вартість ІА, яка визначається як вартість повної переробки або реоновлення активу.
- Вартість утримання активу, пов'язана з витратами на підтримку та обслуговування активу.
- Витрати, що виникають у випадку втрати доступу до активу.
- Збитки репутаційні.
- Спад грошового потоку.
- Втрата конкурентних переваг.
- Зменшення ефективності внутрішніх бізнес-процесів організації.

Для організації буде вибраний певний рівень результатів діяльності як матеріальна величина. Запропонований підхід передбачає, що цей рівень буде визначено як 5% від чистого прибутку організації за рік. Цей рівень відповідатиме небезпек ІА, які мають велику значимість для організації. Аналіз небезпек, пов'язаних з втратою активів низької і середньої значущості, будуть нижче встановленого порога матеріальності (Таблиця 4.5).

Таблиця 4.5

Визначення шкали матеріальних збитків та відповідного рівня збитку

Матеріальна величина збитку	Рівень ризику
≥ 5% від чистого прибутку за рік	Високий
від 1% до 5% від чистого прибутку за рік	Середній
≤ 1% від чистого прибутку за рік	Низький

У підприємства рівень обробки ризиків залежить від їх ступеня. Ризики з

низьким рівнем не піддаються обробці. Середні ризики можуть бути прийнятними залежно від згоди власників ІА.

4.5 Етап 3: Контрольні заходи щодо поліпшення безпеки

Підвищення рівня контрольованості ІА підприємства вимагає аналізу загроз інформаційної безпеки. Існує кілька загальних методів обробки ризиків ІБ, які можуть бути використані:

1. Прийняття ризику: Цей підхід базується на оцінці потенційних збитків від отримання фактору загрози, його очікуваної частоти та політики організації. Якщо ризик вважається прийнятним, а його контроль є простим, можна прийняти рішення не вживати додаткових заходів.

2. Зниження об’єму загрози: Цей метод передбачає мінімізацію вірогідності афекту загрози або використання вразливості. Це може бути досягнуто за допомогою захисних заходів, які зменшують можливість виникнення інциденту, або заходів, які знижують можливий збиток у разі реалізації ризику.

3. Передача ризику: Якщо зниження ризику до допустимого рівня складне або неекономічне, ризик можна передати третій стороні, наприклад, шляхом укладення страхового договору. Це може зменшити вплив ризику на підприємство з економічної точки зору.

4. Уникнення ризику: Цей спосіб передбачає зміну бізнес-процесів або дій для уникнення здійснення ризику. Наприклад, підприємство може відмовитися від певних ризикованих бізнес-активностей або перемістити ресурси з зони ризику. Уникнення ризику може також включати відмову від застосуванні ІА підприємства, а також будь-які інші дії, спрямовані на усунення можливості виникнення ризикованих ситуацій.

Важливо зауважити, що способи обробки ризиків ІБ не є взаємовиключними і можуть комбінуватися. Наприклад, після зниження рівня ризику за допомогою захисних заходів, залишковий ризик може бути застрахований. Також один спосіб обробки ризиків може відноситися до кількох ризиків ІБ одночасно.

Підприємствам необхідно ретельно аналізувати ризики і вибирати оптимальні способи їх обробки, враховуючи конкретні особливості організації. Крім того, важливо постійно моніторити ризики та переглядати заходи забезпечення безпеки, оскільки загрози та уразливості можуть змінюватися з часом.

Вироблення ефективної стратегії обробки ризиків ІБ сприятиме поліпшенню ІБ підприємства. Запобігання можливим загрозам та зменшення можливого збитку при реалізації ризиків є важливими кроками у забезпеченні стійкої та надійної інформаційної безпеки підприємства [14].

4.5.1 Зниження рівня ризиків ІБ

Працівники відділу інформаційної безпеки (ІБ) підприємства грають важливу роль у розробці заходів для зниження ризиків, пов'язаних із інформаційною безпекою.

При розробці цих заходів необхідно враховувати наступні аспекти: ідентифікацію ризиків, необхідні дії для зниження рівня ризиків, очікувані результати від впровадження цих дій, критерії успішного виконання, необхідні ресурси для реалізації заходів та остаточний рівень ризику після впровадження.

Розроблені заходи повинні бути економічно обґрунтованими, тобто вартість впровадження заходів не повинна перевищувати можливі збитки. Якщо зниження рівня ризику не є економічно доцільним або неможливим, можуть бути розглянуті варіанти передачі ризику третім сторонам або відмови від ризикових операцій.

Підприємство також повинно визначити свій ризик-апетит, тобто припустимий рівень залишкового ризику. Якщо залишковий ризик перевищує ризик-апетит підприємства, необхідно розробити додаткові заходи для

зниження рівня ризику до прийнятного рівня. Для цього важливо скласти план впровадження розроблених заходів, який включатиме графік впровадження, відповідальних осіб за виконання заходів та терміни їх реалізації.

При визначенні пріоритету впровадження заходів використовується систематичний підхід. Заходи класифікуються за рівнем ризику, який вони мають знизити. Найвищий пріоритет надається заходам, спрямованим на зниження

найвищого ризику. У межах кожної групи заходів першочерговими вважаються ті, які можна реалізувати швидше та простіше, приносячи найбільший ефект.

Також пріоритетність заходів визначається їх взаємозалежністю. Заходи, від яких залежить успішність інших, отримують вищий пріоритет. Крім того, інші фактори, такі як наявність ресурсів, законодавчі вимоги, фінансові обмеження та тимчасові фактори, можуть впливати на вибір пріоритетних заходів.

Враховуючи всі ці аспекти, співробітники відділу ІБ підприємства розробляють комплексні та адаптовані заходи для зниження ризиків інформаційної безпеки. Це може включати впровадження нових технологій, політик безпеки, тренінгів для персоналу, регулярних оглядів та аудитів систем безпеки.

4.5.2 Передача ризику ІБ

Передача загроз третій стороні може стати вигідним, якщо цей спосіб є економічно доцільнішим, ніж реалізація мір для зниження рівня ризику. Така передача може здійснюватися через страхову компанію або шляхом аутсорсингу певних процесів компанії.

Витрати, пов'язані з втратою конфіденціальності інформації, такі як крадіжка клієнтських або фінансових даних зловмисником. Ці витрати можуть охоплювати розслідування, сплата регуляторних штрафів, розгляд цивільних позовів та інформування заінтересованих сторін.

Кіберстрахування охоплює не лише хакерські атаки, але й природні катастрофи, такі як землетруси та повені, а також збої в роботі фізичних приміщень та сервісів, наприклад, електропостачання або водопостачання. Крім того, це враховує інші випадки, коли порушується нормальне функціонування організації, що призводить до порушення КЦД інформації.

Передача ризику третім сторонам, таким як страхові компанії або фірми, що надають послуги аутсорсингу, може мати певні переваги. Вона дозволяє підприємству зосередитися на своїй основній діяльності, перекладаючи відповідальність за управління ризиками на спеціалізовані організації. Крім того,

передача ризику може бути фінансово вигідною, оскільки вартість страхових премій або послуг аутсорсингу може бути меншою, ніж загальні витрати на розробку та впровадження власних заходів зі зниження ризику.

Проте, перед прийняттям рішення про передачу ризику третім сторонам, необхідно ретельно оцінити всі фактори, включаючи фінансові витрати, репутаційні наслідки та можливості управління самостійно. Також важливо узгодити деталі та обсяг покриття страхування або обсяг послуг аутсорсингу, щоб впевнитися, що вони відповідають потребам підприємства [14].

4.5.3 Уникнення ризику ІБ

Адміністративний апарат підприємства повинно прийняти рішення щодо припинення бізнес-процесів, яка може створити загрозу інформаційній безпеці, або заміни її менш ризикованою альтернативою. У даному випадку користь від проведення цієї бізнес-діяльності значно нижча, ніж розмір збитків, пов'язані з реалізацією ризиків інформаційної безпеки. Уникнення ризику передбачає відмову від певних напрямків діяльності, переміщення ресурсів з зони ризику, відмову від обробки критичної інформації або інші заходи [14].

4.5.4 Прийняття ризику ІБ

Якщо попередні підходи не підходять до загрози або економічно недоцільними, керівництво підприємства може зробити вибір на користь прийняття деяких ризиків ІБ, які перевищують рівень ризик-апетиту. На Рисунку 4.5 зображені результати оцінки ризиків підприємства А.

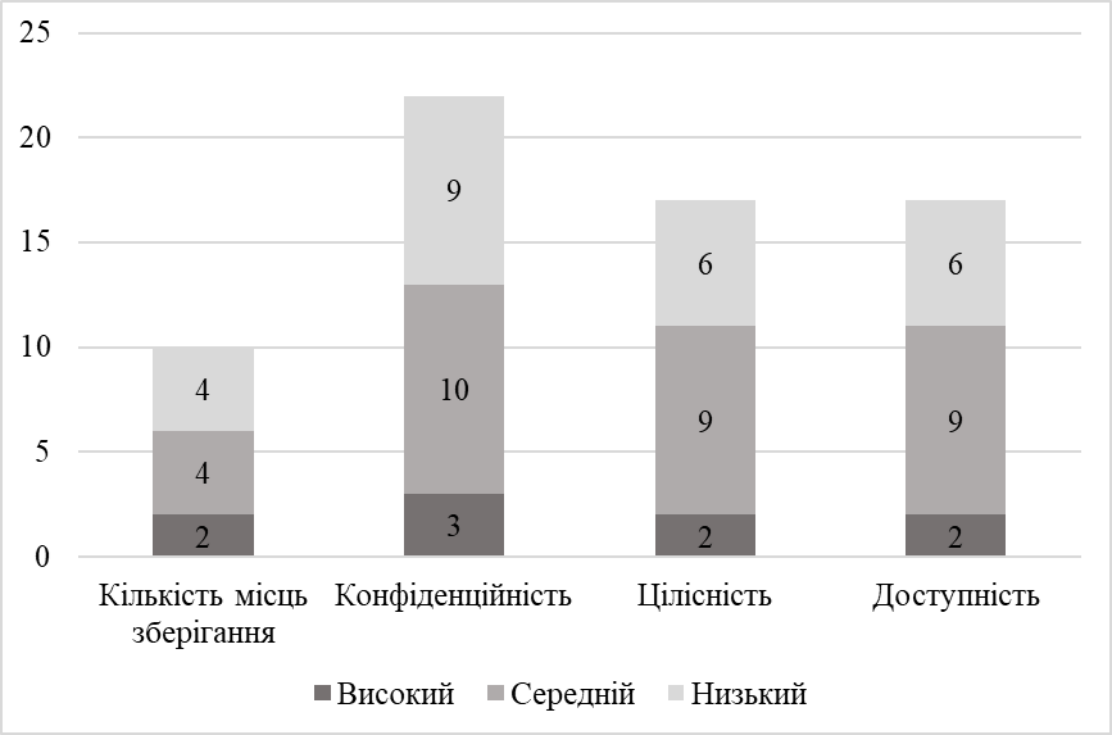

Рисунок 4.5 – Результати оцінки ризиків інформаційної безпеки для підприємства А роздрібної торгівлі

Високий ступінь загроз отримали:

1. ЕОМ генерального директора;
2. Система електронного документообігу.

На дані ризики слід звернути увагу в першу чергу, провести обробку ризиків та зменшити їх рівень до прийнятного – низького.

Середній ступінь небезпеки отримали:

1. Електронна пошта;
2. Паперові документи.

Висновки до розділу 4

У цьому розділі був запропонований новий підхід до оцінки ризиків інформаційної безпеки, специфічний для підприємств роздрібної торгівлі. Цей підхід включає особливості, які є властивими цьому виду діяльності. Кількісна оцінка ризиків сприятиме визначенню найкритичніших точок зберігання, обробки та

передачі інформації в компанії [12].

Розроблений підхід був випробуваний на підприємстві А. Оцінка ризиків показала наявність двох критичних точок зберігання ІА, які мали високий рівень ризику і можуть призвести до значних збитків (понад 5% від річного прибутку підприємства). Чотири точки зберігання показали помірний рівень ризику, який також потребує уваги після високоризикових областей [13].

ВИСНОВКИ

В рамках даного дослідження було проведено аналіз можливих загроз і атак, що стикаються підприємства роздрібної торгівлі. Результати аналізу виявили, що різноманітні атаки на підприємства відбуваються щороку, і вони можуть бути здійснені як внутрішніми, так і зовнішніми загрозами. Особливо велика частина атак стається ззовні, оскільки підприємства роздрібної торгівлі співпрацюють з багатьма постачальниками та підрядниками, що робить їх вразливими перед зловмисниками, включаючи конкурентів. Однак найбільші збитки для таких підприємств виникають внаслідок внутрішніх атак. Найпоширенішими з них є впровадження шкідливого програмного забезпечення, що свідчить про неефективність наявної системи безпеки та недостатню інформованість співробітників щодо інформаційної безпеки.

Одним з ключових етапів впровадження системи управління інформаційною безпекою є створення ефективного механізму управління ризиками, який дозволяє приймати обґрунтовані рішення в цій сфері. У роботі було проведений огляд існуючих методів оцінки ризиків, які широко використовуються в Україні. Проте детальний аналіз таких методів виявив необхідність розробки більш гнучкого та ефективного підходу до управління ризиками інформаційної безпеки для підприємств роздрібної торгівлі. Існуючі підходи мають свої недоліки, такі як загальність підходу, використання якісних методів для визначення ризиків та потребу у значних ресурсах для їх впровадження.

Розроблений підхід до управління ризиками інформаційної безпеки для підприємств роздрібної торгівлі пропонує кількісну оцінку ризиків, класифікацію їх та своєчасне зниження високих ризиків з метою зменшення можливих збитків і збереження коштів, пов'язаних з відновленням або відновленням роботи місць зберігання та обробки інформації компанії. Крім того, розроблений підхід надає рекомендації щодо забезпечення (підвищення) рівня інформаційної безпеки.

Особливістю цього підходу є врахування специфіки роздрібної торгівлі, що

впливає на визначення впливу ризиків на інформаційні активи. Наслідки ризиків можуть впливати на комерційні інтереси, операційну діяльність, відношення клієнтів та постачальників, а також на лояльність співробітників. Крім того, ризики класифікуються залежно від їхнього рівня, де високі ризики вказують на можливі матеріальні збитки у розмірі більше 5% від чистого прибутку підприємства за рік.

Протягом проведення досліджень було підтверджено висока ефективність запропонованого підходу на реальному підприємстві. Однак, існує потенціал для подальшого розширення та розвитку підходу, наприклад, шляхом включення нових методів обробки ризиків, оцінці важливості та пріоритетності ризиків залежно від контексту підприємства та постійного моніторингу змін у загрозах і технологічному середовищі. Також можна додати аналіз специфічних сценаріїв загроз та розробку відповідних заходів управління ризиками:

Високий ступінь загрози отримали такі сегменти підприємства зберігання інформації:

ЕОМ генерального директора;

Система електронного документообігу.

Середній ступінь небезпеки отримали:

Електронна пошта;

Паперові документи.

Серед важливих причин високого рівня загроз мала ефективність наявних контрольних заходів, які б пом’якшували ризики.

21% загроз від їх загальної кількості пов’язані з неналежним застосуваннння нормативних документів, що регламентують безпечне підключення окремих компонентів. 79% загроз від їх загальної кількості пов’язані з порушенням нормативних документів компанії.

Таким чином, запропонувавши власний підхід до оцінки ризиків інформаційної безпеки, який враховує особливості індустрії роздрібної торгівлі, видає кількісний результат, визначає на які існуючі вразливості та недоліки контрольних заходів слід звернути увагу в першу чергу, дозволяє досягти підвищенню ефективності засобів захисту інформаційних систем підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.

2. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology) [Текст]. – Gaithersburg: National Institute of Standards and Technology, 200.332.– 95 с.

3. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст] / R. A.Caralli, J. F. Stevens, L. R. Young, L. R. Wilson.– Бостон: Університет Карнегі-Меллон, 2007. – 0.3354 с.

4. Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust [Електронний ресурс] // Symantec White Paper. 200.335. Режим доступу: https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf.

5. Cyber risk in retail: Protecting the retail business to secure tomorrow’s growth [Електронний ресурс]. – 200.337 – Режим доступу: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/us-risk- 200.337-retail-cyber-risk-report-04070.335.pdf

6. Інформаційна безпека та роздрібна торгівля [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/about/press/press-releases/200.335/08-20.33d.html

7. Security trends in the retail industry [Електронний ресурс]. – 200.336 – Режим доступу: https://www.ibm.com/downloads/cas/DO8MZRV9

8. Cyber security concerns in the retail sector [Електронний ресурс]. – 200.337 – Режим доступу: https://www.grantthornton.ie/globalassets/0.33.- member-firms/ireland/insights/factsheets/grant-thornton---cyber-security- concerns---retail.pdf

9. Скачек Л. М. ЦІННІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Текст] / Л. М. Скачек. // Інформаційна безпека. – 200.333. – №0.33(9). – С. 0.3352–0.3354.

10. "Information Security in Retail Enterprises: Risk Assessment and Mitigation Strategies" - автор John Smith. - Нью-Йорк: ACM, 2022. - ISBN 978-1-2345-6789-0

11. C. Meadows, “Applying the Dependability Paradigm to Computer Security,” Proc. Workshop on New Security Paradigms, Sep. 1995, pp. 75-81.

12. E. Jonsson et al., “On the Functional Relation Between Security and Dependability Impairments,” Proc. 1999 Workshop on New Security Paradigms, Sep. 1999, pp. 104-111.

13. G. Song et al., “CERIAS Classic Vulnerability Database User Manual,” Technical Report 2000-17, CERIAS, Purdue University, West Lafayette, IN, 2000.

14. N.R. Mead, R.J. Ellison, R.C. Linger, T. Longstaff, and J. McHugh, “Survivable Network Analysis Method,” Tech. Rep. CMU/SEI-2000-TR-013, Pittsburgh, PA, Sep. 2000.

15. P. Ammann, S. Jajodia, and P. Liu, “A Fault Tolerance Approach to Survivability,” in Computer Security, Dependability, and Assurance: From Needs to Solutions, IEEE Computer Society Press, Los Alamitos, CA, 1999.

16. Determining Key Risks for Modern Distributed Information Systems, Dmytro Palko, Hrygorii Hnatienko, Tetiana Babenko, Andrii Bigdan, Taras Shevchenko National University of Kyiv 64/13, Volodymyrska Street, Kyiv, 01601, Ukraine, 2021.

17. 2019 Global Cyber Risk Perception Survey // Marsh, Microsoft. - 2019. Access: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

18. "Information Security in Retail Enterprises: Risk Assessment and Mitigation Strategies" - John Smith. - Нью-Йорк: ACM, 2022. - ISBN 978-1-2345-6789-0

19. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment - A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY). - 2013. doi: 10.1109/ifuzzy.2013.6825462.

20. Xin Y. et al. Machine learning and deep learning methods for cybersecurity //IEEE access. – 2018.– Vol. 6. – P. 35365-35381.

21. "Assessing Information Security Risks in Retail Organizations" - автор Jennifer Davis. - Сан-Франциско: O'Reilly Media, 2017. - ISBN 978-1-8765-4321-0. – 228 с.

22. Шапорін, В.О. Моделі та методи аналізу ризиків безпеки

інформаційних систем: дис. канд. техн. наук : 05.13.06 — Інформаційні технології - Одеса, 2016. – 178 с.

23. ISO 31000 Risk Management. Brien Posey. Access: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management

24. Understanding the Differences between the COSO ERM Framework and ISO 31000 Risk Management Standards. Lisanne Sison, Jim Doran. Access: https://www.ajg.com/us/news-and-insights/2020/oct/coso-iso-3100-risk-management-plans/

25. What Is ISO 27001:2013? A Guide for Businesses. Adam Nunn. Access: https://auth0.com/blog/what-is-iso-27001-2013-a-guide-for-businesses/

Додаток А

Результати оцінки ризиків підприємства А

Таблиця А.1 – Результати інвентаризації інформаційних активів та місць їх зберігання

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
1	Директор служби економіки та фінансів	Звіт про динаміку основних ключових показників підприємства	2.5	- Генеральний директор	Н/З	Н/З	- Генеральний директор - Директор служби економіки та фінансів	Н/З	Н/З
2	Директори всіх служб в рамках бюджету своєї служби	Звіт про запланований бюджет в розрізі місяця, кварталу і року	1.5	- Генеральний директор	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	- Генеральний директор - Директор служби економіки та фінансів - Директори всіх служб (бюджет своєї служби)	Н/З	Н/З
3	Генеральний директор	Стратегічні плани розвитку	7.5	Н/З	- Генеральний директор - Рада директорів - Директори всіх служб	- Генеральний директор - Рада директорів - Директори всіх служб	- Генеральний директор - Рада директорів - Директори всіх служб	Н/З	Н/З
4	Директор служби розвитку роздрібної торгівлі	Картка об'єкта	4.25	Н/З	- Н/З	- Н/З	- Генеральний директор - Директор служби розвитку роздрібної торгівлі	Н/З	Н/З

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
5	Генеральний директор	Рішення ради директорів про покупку нового об'єкта	5	Н/З	Н/З	Н/З	- Генеральний директор - Рада директорів	Н/З	Н/З
6	Генеральний директор	Звіт про прибутки і збитки Компанії в динаміці	6.25	Н/З	Н/З	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З
7	Директор аналітичної служба	Аналітика продажів	3.25	Н/З	Н/З	Н/З	- Генеральний директор - Директор служби економіки та фінансів - Директор аналітичної служби	- Директор аналітичної служба	Н/З
8	Директор аналітичної служба	Дані про виконання плану по товарообігу магазинами за минулий день	2.25	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок
9	Директор аналітичної служба	Звіт про дотримання плану по нормам запасів на розподільних центрах і магазинах	0.75	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
10	Директор аналітичної служба	Звіт про виконання плану товарообігу по акціях	1.25	Н/З	Н/З	Н/З	Н/З	- Аналітична служба	- Генеральний директор - Директор служби управління ланцюгами поставок
11	Директори всіх служб в рамках своєї служби	Дані по форс-мажорних ситуацій	0.5	Н/З	Н/З	Н/З	Н/З	Н/З	- Генеральний директор - Директор служб
12	Директор служби маркетингу	Дані про відкриття нових магазинів	0.002	- Генеральний директор	Н/З	Н/З	- Генеральний директор - Директор служби маркетингу	Н/З	Н/З
13	Директор аналітичної служба	Звіт про рентабельність магазинів	1.75	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служб економіки та фінансів	Н/З	Н/З	Н/З	Н/З
14	Директор служби управління регіонами	Звіт за основними ключовими показниками регіонів	1.25	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служби управління регіонами	Н/З	- Генеральний директор - Директор аналітичної служби - Директор служби управління регіонами	Н/З	Н/З

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
15	Директор служби управління персоналом	Звіт про плинність кадрів і некомплекту штату	0.25	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	Н/З
16	Директор аналітичної служба	Звіт про втрати нормованих груп товарів	0.5	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	Н/З
17	Директор служби комерційної нерухомості	Дані по нерухомості Компанії	0.25	Н/З	Н/З	Н/З	- Генеральний директор - Директор служби комерційної нерухомості	Н/З	Н/З
18	Генеральний директор	Концепція магазино-будування	0.75	- Генеральний директор	Н/З	- Підрядні організації	- Директори служб	Н/З	Н/З
19	Генеральний директор	Картка проекту з даними по плановаим інноваціям, експериментам, покупкам нового обладнання	3.75	Н/З	- Генеральний директор - Директори всіх служб	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З
20	Директори всіх служб в рамках своєї служби	Комерційні умови роботи з постачальниками, тендерна документація	5	Н/З	Н/З	Н/З	- Генеральний директор - Директори всіх служб	Н/З	Н/З

№	Власник ІА	Найменування ІА	Вартість ІА, млн грн	Місця зберігання ІА					
				ПК	Електронна пошта	Паперовий документ	СЕД	Business Intelligence	Мобільний телефон
21	Директор служби управління регіонами	Кадрові дані	1.25	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	- Генеральний директор - Директор служби управління персоналом	Н/З	Н/З
22	Директор аналітичної служба	Звіти з продажу власної торгової марки	1.75	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	- Генеральний директор - Директор аналітичної служби	Н/З	Н/З

Таблиця А.2 – Наслідки при порушенні конфіденційності, цілісності та доступності активу

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
1	Звіт про динаміку основних ключових показників підприємства	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
2	Звіт про запланований бюджет в розрізі місяця, кварталу і року	3	0	0	0	2	2	0	0	0	0	2	2	3	2	2

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
3	Стратегічні плани розвитку	3	0	0	0	3	3	2	0	0	0	0	0	3	3	2
4	Картка об'єкта	3	0	0	0	3	2	0	2	2	0	0	0	3	3	2
5	Рішення ради директорів про покупку нового об'єкта	3	0	0	0	1	1	0	0	0	0	0	0	3	1	1
6	Звіт про прибутки і збитки Компанії в динаміці	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
7	Аналітика продажів	3	0	0	0	2	2	1	0	0	0	0	0	3	2	2
8	Дані про виконання плану по товарообігу магазинами за минулий день	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
9	Звіт про дотримання плану по нормам запасів на розподільних центрах і магазинах	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
10	Звіт про виконання плану товарообігу по акціях	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1
11	Дані по форс-мажорних ситуацій	2	0	0	0	1	1	2	0	0	0	1	1	2	1	1
12	Дані про відкриття нових магазинів	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	Звіт про рентабельність магазинів	2	0	0	0	2	2	0	0	0	0	0	0	2	2	2

№	Найменування ІА	Наслідки комерційним інтересам організації			Наслідки операційної діяльності			Наслідки відносинам з клієнтами і партнерами			Наслідки лояльності співробітників			Рівень наслідків порушення К	Рівень наслідків порушення Ц	Рівень наслідків порушення Д
		К	Ц	Д	К	Ц	Д	К	Ц	Д	К	Ц	Д			
14	Звіт за основними ключовими показниками регіонів	3	0	0	0	2	2	0	0	0	0	0	0	3	2	2
15	Звіт про плинність кадрів і некомплекту штату	2	0	0	0	1	1	0	0	0	1	0	0	2	1	1
16	Звіт про втрати нормованих груп товарів	2	0	0	0	1	1	0	0	0	0	0	0	1	1	1
17	Дані по нерухомості Компанії	2	0	0	0	2	2	1	0	0	0	0	0	2	2	2
18	Концепція магазино-будування	2	0	0	0	2	2	0	0	0	0	0	0	2	2	2
19	Картка проекту з даними по плановим інноваціям, експериментам, покупкам нового обладнання	2	0	0	0	2	2	1	1	1	1	0	0	2	2	2
20	Комерційні умови роботи з постачальниками, тендерна документація	3	0	0	0	2	2	1	1	1	1	0	0	3	2	2
21	Кадрові дані	2	0	0	0	1	1	1	0	0	1	0	0	2	1	1
22	Звіти з продажу власної торгової марки	2	0	0	0	1	1	0	0	0	0	0	0	2	1	1

Таблиця А.3 – Оцінки ризиків активів генерального директора підприємства та місць їх зберігання та обробки

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	∑ □□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Крадіжка / втрата місць зберігання інформації (мобільних пристроїв, комп'ютерного обладнання і паперових документів)	×	×	×	ПК	Відсутність / недоліки процесу шифрування конфіденційної інформації на пристроях. Кінцеві користувачі відповідальні за шифрування інформації	Отримання несанкціонованого доступу до конфіденційної інформації компанії, в разі крадіжки ІТ-обладнання з конфіденційною інформацією, через відсутність / недоліків процесу та інструментів шифрування інформації	70.752	100%	0.99	70.04448
				Паперовий документ	Відсутність / недоліки відповідальності і контролю за фізичним захистом паперових документів при їх пересилці. У компанії не використовується одна кур'єрська служба для пересилки конфіденційних документів, з якої був би укладений договір і зафіксована відповідальність за фізичний захист документів при пересилці, в тому числі за нерозголошення конфіденційної інформації	Крадіжка паперових документів, на яких зберігається конфіденційна інформація, представниками кур'єрської служби або іншими зловмисниками, через відсутність контролю за пересиланням документів і відповідальності за фізичний захист документів при їх пересилці	9.75	100%	5	48.75
				Паперовий документ	Відсутність / недоліки політики чистого столу компанії при роботі з конфіденційною інформацією	Крадіжка паперових документів, на яких зберігається конфіденційна інформація, через відсутність / недоліків контролю за паперовими документами на робочих місцях співробітників	9.75	100%	3	29.25
				Мобільний телефон	Недоліки процесу і інструментів з управління мобільними пристроями (смартфони і планшети), за допомогою яких співробітники отримують доступ до конфіденційної інформації компанії. Відсутність політики щодо безпечного поводження з мобільними пристроями, налаштування безпеки пристроїв, контролю і моніторингу їх використання	Крадіжка / втрата мобільних пристроїв, через відсутність вимог до співробітників щодо безпечного поводження з мобільними пристроями, а також з-за недоліків процесу управління мобільними пристроями з боку компанії	4.75	80%	0.33	1.254

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	∑ □□□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Ненавмисне розкриття конфіденційної інформації співробітником компанії / представником зовнішньої організації	×			ПК	Відсутність / недоліки політики чистого екрану в приміщеннях компанії при роботі з конфіденційною інформацією на ІТ-обладнанні	Розголошення конфіденційної інформації зловмиснику, який отримав доступ до екрану мобільного пристрою, на якому відображається конфіденційна інформація	70.752	100%	3	212.256
				Електронна пошта	Відсутність контролю за відправкою листів по електронній пошті, що містять конфіденційну інформацію	Розголошення конфіденційної інформації при відправці електронного листа помилковому адресату	19.5	100%	0.99	19.305
Ненавмисне розкриття конфіденційної інформації співробітником компанії / представником зовнішньої організації	×			Паперовий документ	Відсутність процесу щодо безпечного використання, поширення та знищення інформаційних активів в паперовому вигляді. Немає обов'язкових вимог до маркування документів в залежності від їх рівня конфіденційності співробітниками компанії.	Розголошення конфіденційної інформації, через відсутність процесу безпечного поводження з конфіденційною інформацією, в тому числі маркування місця зберігання конфіденційної інформації	9.75	100%	0.99	9.6525
				Паперовий документ	Друк на мережевих принтерах не захищений паролем. Не виконується перевірка місць, де розташовані принтери, на предмет зберігання документів з конфіденційною інформацією і їх використання в якості чернеток	Розголошення конфіденційної інформації при отриманні доступу до паперового документу, який залишений без нагляду на принтері після друку або використовується в якості чернетки	9.75	100%	7	68.25
Умисне розкриття конфіденційної інформації співробітниками	×			Електронна пошта	Відсутність можливості контролювати відправку конфіденційної інформації по електронній пошті, якщо інформація була попередньо зашифрована засобами шифрування	Розголошення конфіденційної інформації, за допомогою її відправки по електронній пошті, через відсутність функціональності системи запобігання витоків інформації з аналізу зашифрованої інформації	19.5	100%	3	58.5
				Мобільні телефони	Відсутність / недоліки контролю за копіюванням інформації з ІС, в тому числі електронної пошти, на приватний пристрій. Відсутність формалізованого підходу до управління мобільними пристроями, а також вимог до співробітників щодо безпечного використання мобільних пристроїв	Розголошення конфіденційної інформації співробітниками, через відсутність контролю доступу користувачів і їх діями при роботі з конфіденційною інформацією компанії за допомогою особистих пристроїв	4.75	80%	5	19

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	∑ □□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Непередбачені наслідки змін: впровадження нових бізнес-процесів, зміни в ПЗ, зміни в комп'ютерному / комунікаційному устаткуванні	×	×	×	ВІ	Недоліки в процесі управління змінами ІС, які можуть привести до неправомірного доступу до конфіденційної інформації. У компанії відсутній контроль за доступом розробників на продуктивне середовище, дотримання розробником вимог безпечної інсталяції та конфігурування застосунків	Розголошення конфіденційної інформації при отриманні несанкціонованого доступу до інформації в процесі розробки, тестування і установки змін ІС, через відсутність контролю доступу розробників на продуктивне середовище і відсутності стандарту безпечної інсталяції та конфігурування додатків	7.5	100%	0.99	7.425
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	ВІ	Відсутність / недоліки контролю доступу до інформаційних активів в хмарному середовищі, орендованій у хмарного провайдера, як внутрішніх користувачів, так і інших орендарів хмари і адміністраторів хмарних сервісів	Крадіжка конфіденційної інформації через недоліки в управлінні доступом до конфіденційної інформації компанії, яка зберігається і обробляється в хмарних сервісах	7.5	100%	0.33	2.475
				ПК	У компанії відсутня політика управління ліцензіями ПО, а також контроль за використанням неліцензійного ПЗ, яке може містити велику кількість вразливостей безпеки застосунків	Витік конфіденційної інформації, відмова в обслуговуванні ПК з використанням вразливостей неліцензійного ПЗ, встановленого на ІТ-обладнанні компанії, установка якого на ІТ-обладнання не контролюється	70.752	100%	0.99	70.04448
				Електронна пошта	Відсутність / недоліки контролю за масовими розсилками, визначенням і обробкою спам-листів, виявлення і видалення вірусного ПЗ в електронних листах	Крадіжка конфіденційної інформації, порушення працездатності ІС за допомогою шкідливого ПО або соціальної інженерії, що розсилаються по електронній пошті співробітникам компанії, з причини відсутності / недоліків засобів і механізмів контролю за масовими розсилками, визначенням і обробкою спам-листів, виявлення і видалення вірусного ПЗ в електронних листах	19.5	100%	0.99	19.305

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	$\sum$ □□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	Система електронного документо-обігу	Для адміністрування застосунку співробітниками СІТ застосовуються вбудовані облікові записи 'sa' і 'Administrator', які призначені для первинного розгортання ІС. Пароль до цих облікових записів відомий всім співробітникам зазначеного підрозділу. Згідно «Процедурі управління правами доступу» назви адміністративних облікових записів повинні однозначно ідентифікувати користувача, не даючи при цьому зайвої інформації про призначення облікового запису. Політика ІБ також встановлює вимогу, відповідно до якого будь-який доступ має здійснюватися із застосуванням персоналізованої облікового запису	Інформація про вбудовані облікові записи застосунків є загальнодоступною. Комбінація загальновідомих «логінів» і можливих варіантів пароля використовуються для реалізації атаки «brute force». Використання неперсоніфікованих адміністративних облікових записів, доступ до яких має велика кількість співробітників, істотно збільшує ризик компрометації таких облікових записів, а також ускладнює виявлення і розслідування пов'язаних з ними інцидентів ІБ	45.002	100%	0.99	44.55198
	×	×	×	Система електронного документо-обігу	Для окремих облікових записів застосунку застосовується внутрішня аутентифікація (наприклад, 'sa' і 'Administrator'). Для таких облікових записів на рівні програми не активований параметр «Застосовувати політику паролів», який приводить парольні налаштування програми у відповідність з парольними настройками на рівні ОС сервера БД. Поточні парольні настройки на рівні ОС не відповідають вимогам ІБ, які визначені в «Процедурі управління правами доступу», «Стандарті безпечної настройки операційних систем Windows Server»: Мінімальна довжина пароля - 7 символів. Рахунок не блокується після невдалих спроб входу в систему.	Використання слабких паролів або паролів, які легко визначити, в сукупності з відсутністю обмежень по числу вводів невірних паролів облікових записів істотно спрощують підбір паролів за допомогою застосування загальнодоступних утиліт («brute force»). У свою чергу, отримання зловмисником несанкціонованого доступу до застосунку може призвести до модифікації знищення і розкриттю критичних даних ІС, порушення її працездатності та інших несприятливих наслідків для Компанії	45.002	100%	0.99	44.55198

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	∑ □□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	ПК	Неконтрольована установка ПО на стаціонарні робочі станції. Відсутність актуального білого списку ПО, яке може бути встановлено на робочі станції співробітників без узгодження співробітниками ІБ. Відсутність контролю того, що співробітники СІТ використовують файли ПО, перевірені та узгоджені співробітниками ІБ	Крадіжка або модифікація конфіденційної інформації, порушення працездатності ІС з використанням шкідливого ПО або ПО з уразливими безпеки, яке можна встановити на робочі станції без перевірки і узгодження співробітниками ІБ	70.752	100%	3	212.256
				ВІ	Використання ІС з вразливостями, уразливими конфігураціями, обліковими записами та паролями за замовчуванням. Відсутність формальної політики з управління вразливостями. У компанії відсутній процес за визначенням критичних оновлень ПО, в тому числі ОС, і процес їх швидкого встановлення на робочі станції і серверне обладнання. У компанії відсутній стандарт безпечної настройки ІС і мережевого устаткування, що включає список дозволених портів, протоколів, сервісів і необхідних заходів захисту для забезпечення безпечного функціонування. Відсутня процес по скануванню коду ПО на наявність вразливостей безпеки при установці оновлень	Крадіжка конфіденційної інформації з використанням вразливостей ІС і мережевого устаткування компанії, через відсутність процесу управління уразливими і стандартів безпечної настройки ІС і мережевого устаткування	7.5	100%	0.99	7.425
	×	×	×	ВІ	Відсутність / недоліки аутентифікації користувачів в корпоративну мережу, ІС на всіх інфраструктурних рівнях (ОС, СУБД, застосунок)	Крадіжка конфіденційної інформації, порушення працездатності ІС, доступ до якої був отриманий з використанням вразливостей механізму аутентифікації	7.5	100%	0.99	7.425
				ПК	Недоліки в роботі антивірусного захисту, в тому числі несвоєчасне оновлення сигнатурних баз, непроведення сканування комп'ютерів	Крадіжка або модифікація конфіденційної інформації, порушення працездатності ІС з використанням шкідливого ПО, установка і запуск якого не контролюється засобами антивірусного захисту через її відсутність, застарілої сигнатурної бази або можливості її відключення	70.752	100%	0.99	70.04448

Продовження Таблиці А.3

Загроза	Основні властивості інформації, на які впливає загроза			Місце зберігання та обробки ІА	Вразливість	Ризик	∑ □□□, млн грн	L_R, %	F_e	R, млн грн
	К	Ц	Д							
Проникнення зловмисника в ІС, з метою отримати доступ до конфіденційної інформації, порушення працездатності ІС і інших несприятливих наслідків	×	×	×	Система електронного документо-обігу	Видача неузгоджених і / або некоректних прав доступу до ІС, недоліки механізму авторизації. Існуючі нормативні документи щодо процесу давно не актуалізувалися. Співробітники запитують права доступу виходячи із загального розуміння функціональності в системі. Матриці прав доступу не використовуються для видачі доступу в ІС. Права визначають відповідальні адміністратори на підставі свого досвіду або раніше наданих прав співробітникам. Відсутні формалізовані вимоги до проведення перевірок виданого доступу фахівцями ІБ.	Розголошення конфіденційної інформації при отриманні несанкціонованого доступу до інформаційних активів компанії, через недоліки процесу управління доступом	45.002	100%	3	135.006
				Система електронного документо-обігу	Недоліки процесу обмеження доступу до ІС при звільненні працівника. Доступ співробітників обмежується вручну фахівцем СІТ на підставі щоденного аналізу HR-системи, з метою визначити звільнених і переведених на нову посаду співробітників. Блокування доступу - відповідальність співробітників СІТ, у яких відсутні формалізовані вимоги до блокування даного доступу. Відсутня формалізований підхід до перевірки своєчасності блокування доступу співробітниками ІБ. Результати перевірок формально не документуються.	Розголошення конфіденційно інформації ї, порушення працездатності системи співробітниками, доступ яких до ІС не своєчасно заблокований	45.002	100%	0.99	44.55198

Контроль	Впровадження процесу управління доступом до ІС
Рекомендації	1. Розробити «Процедуру управління доступом до ІС», яка визначає вимоги до процесу надання, зміни і блокування доступу до інформаційних активів в ІС 2. Організаційно та технічно реалізувати доступ до ІС відповідно до вимог Процедури управління доступом 3. Впровадити вимоги процедури управління доступу до ІС, керуючись такими принципами: • Мінімальної достатності прав доступу - користувач повинен мати доступ в системі мінімально необхідний для виконання службових обов'язків; • Видача прав повинна базуватися на формальних вимогах, які визначають, які посади і відділи співробітників можуть запитувати які права по роботі з ІА в ІС, файлових сховищах або ІТ-сервісах. По можливості, створити матриці прав доступу в ІС, а в самих ІС реалізувати групи і / або ролі, за допомогою яких видавати доступ користувачам; • "Чотирьох очей" (залучення декількох співробітників) для розмежування повноважень при здійсненні операцій з конфіденційною інформацією. 4. Впровадити вимоги до процесу аутентифікації користувачів в ІС: • Вимоги до облікових записів користувачів: o Кожному співробітнику повинен бути привласнений унікальний ідентифікатор в ІС; o Всі системні і технічні облікові записи, які використовуються адміністраторами або іншими системами повинні бути визначені і формально задокументовані, а також визначені співробітники, які мають право використовувати дані облікові записи та / або відповідають за їх підтримку. • Вимоги до парольних налаштувань: o Паролі користувачів повинні бути унікальними для різних ІС або повинен використовуватися механізм однієї точки входу в усі системи; o Паролі повинні відповідати заданим рівнем складності, змінюватися на періодичній основі, не повторюватися з раніше використовуваними (мінімум з 5 останніми); o Блокування облікового запису користувача в разі 3-х невдалих спроб введення для звичайних користувачів і 5 спроб для адміністративних облікових записів (період блокування не менше 30 хв); o Час неактивності користувача до блокування його робочого ПК повинна складати не менше 7 хвилин. • Визначити вимоги до додаткових засобів аутентифікації користувачів. Для перевірки справжності користувача для доступу до високо-конфіденційної інформації повинні застосовуватися додаткові параметри: біометричні дані, смарт-карти співробітника

	5. Провести повну перевірку прав доступу всіх співробітників компанії до ІА на предмет необхідності фактичного доступу користувачів. Після цього виконувати контроль коректності наданих прав доступу до ІА Компанії на періодичній основі, не рідше ніж раз у квартал.		
Пріоритет	Високий	**Складність**	Середня
Тривалість	2 місці		
Фінансові інвестиції	Впровадження рекомендацій не потребує фінансових інвестицій		
Контроль	**Впровадження політики чистого екрану в приміщеннях компанії при роботі з конфіденційною інформацією на ІТ-обладнанні**		
Рекомендації	1. Створити та забезпечити процедуру контролю за дотриманням правил «чистого стола та чистого екрана», яка буде включати (але не обмежуватися) наступними вимогами: • Документи і ІТ-обладнання, яке не використовується, слід прибирати з робочих столів і ховати в сейфи і інші шафи або приміщення, які обмежують доступ сторонніх осіб; • Вихід з систем або автоматичне блокування екрану ПК і ноутбука при закінченні роботи користувача; • Розміщення моніторів ПК і ноутбуків далеко від місць, де їх можуть побачити люди, у яких не повинно бути доступу до інформації (наприклад, далеко від вікон і прохідних ділянок приміщень). 2. Визначити та інформувати співробітників про дисциплінарні заходи, які можуть бути застосовані до співробітників компанії, в разі порушення прийнятих правил поводження з конфіденційною інформацією; 3. Співробітники ІБ повинні виконувати на періодичній основі контроль дотримання вимог процедури щодо безпечного поводження з конфіденційною інформацією; 4. Розробити Програму підвищення обізнаності в області ІБ, яка регламентує наступні аспекти: • Опис комплексної програми підвищення обізнаності співробітників та представників зовнішніх організацій, яка повинна включати (але не обмежуватися): o Зведену інформацію про існуючі нормативно-довідкові документи компанії в області ІБ, що регламентують захист конфіденційної інформації; o Порядок поводження з паперовими і електронними документами (зберігання / транспортування / знищення, політика чистого стола та чистого екрана);		

	○ Визначення відповідальності співробітників і представників зовнішніх організацій в разі недотримання вимог ІБ, в тому числі дисциплінарні заходи, які можуть бути застосовані до співробітників і представників зовнішніх організацій. 5. Впровадити Програму підвищення обізнаності персоналу та представників зовнішніх організацій в області ІБ: • Співробітники компанії, які в ході своєї робочої діяльності мають доступ до конфіденційної інформації, повинні щорічно проходити навчання в області ІБ, організоване працівниками ІБ.		
Пріоритет	Високий	**Складність**	Середня
Тривалість	3 місяці		
Фінансові інвестиції	30000-35000 $ Інвестиції складаються з: 1. 5000-10000 $ - створення силами підрядника онлайн порталу для розміщення матеріалів ІБ для вивчення співробітниками і оцінювання їх знань; 2. Від 25'000 $ - аутсорсинг створення і проведення тренінгів із загальних питань ІБ для 700 співробітників компанії, в розрахунку 1 тренінг триває до 3 год;		
Рекомендації	1. Розробити та впровадити «Стандарт використання ПЗ на робочих станціях, серверному і мережевому обладнанні», включаючи наступне: • Створення та підтримка в актуальному стані списку стандартного ПЗ, дозволеного для установки на робочих ПК всіх співробітників; списку нестандартного ПЗ, яке можуть використовувати певні відділи і посади в рамках своєї роботи (наприклад, утиліти, які дозволено використовувати адміністраторам систем і користувачами з привілейованими правами для отримання доступу до баз даних); • Формалізувати вимоги заборони самостійної установки і зміни конфігурацій програмного забезпечення співробітниками (не з служби підтримки) на робочих ПК; • Формалізувати вимоги до перевірки безпеки ПЗ перед узгодженням установки ПЗ на робочі ПК / ноутбуки по заявці користувача; • Формалізувати розподіл ролей і обов'язків за впровадження і контроль установки і використання ПЗ на робочих станціях, серверному і мережевому обладнанні компанії; • Визначити та задокументувати дисциплінарні заходи, які застосовуються для співробітників, які встановили та використовували неузгоджене і / або заборонене ПЗ; • Формалізувати процес управління ліцензіями використовуваного ПЗ, включаючи контроль		

	дотримання термінів і кількості ліцензій, а також заборона використання неліцензійного ПЗ; • Формалізувати процес управління оновленнями ПЗ, встановленого на робочих ПК; • Вести журнал аудиту змін ПЗ на робочих ПК, серверному і мережевому обладнанні; • Періодично перевіряти встановлене ПЗ на робочих ПК, серверному і мережевому обладнанні, і порівнювати його зі списком стандартних програм і зі затвердженими заявками співробітників на установку нестандартного ПЗ; документувати результати перевірки та усувати виявлені порушення. 2. Перевірити, що ніхто з користувачів не має прав на установку неавторизованого ПЗ на робочих ПК. Для цього необхідно перевірити, що забезпечено наступне: • Відсутність у користувача прав адміністратора на робочому ПК; • Обмеження доступу до виконуваних файлів недозволених для запуску і установки застосунків на рівні файлової системи; • Відсутність доступу користувача до мережевих ресурсів, на яких можуть зберігатися файли застосунків, невстановлених на робочому ПК; • Обмеження на використання зовнішніх носіїв інформації; • Обмеження доступу в мережу Інтернет.